ESET PROTECT On-Prem

Guía de administración

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

ESET PROTECT On-Prem está 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

Bienvenido a ESET PROTECT On-Prem, versión 11.0. ESET PROTECT On-Prem Le permite administrar productos de ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central. Con ESET PROTECT Web Console, podrá implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o detecciones que se produzcan en ordenadores 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	Nuevo nombre	Versión en la que se ha cambiado el nombre
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

- ESET PROTECT Server: puede instalar ESET PROTECT Server en servidores Windows y Linux, así como implementarlo como un dispositivo virtual preconfigurado. Se ocupa de la comunicación con los agentes y recopila y almacena datos de aplicaciones en la base de datos.

- ESET PROTECT Web Console: ESET PROTECT Web Console es la interfaz principal que le permite administrar los ordenadores cliente de su entorno. Muestra información general del estado de los clientes de su red y le permite implementar de forma remota soluciones de ESET en ordenadores no administrados. Después de instalar ESET PROTECT Server, puede acceder a Web Console desde un navegador web. Si decide hacer que el servidor web esté disponible desde Internet, puede utilizar ESET PROTECT On-Prem desde cualquier lugar o dispositivo en el que disponga de conexión a Internet. Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server. Consulte también Introducción a ESET PROTECT Web Console.

- ESET Management Agent: ESET Management facilita la comunicación entre ESET PROTECT Server y los ordenadores cliente. El agente debe instalarse en el ordenador cliente para establecer comunicación entre ese ordenador y ESET PROTECT Server. Como está en el ordenador cliente y puede almacenar varios contextos de seguridad, el uso de ESET Management Agent reduce considerablemente el tiempo de reacción a las nuevas detecciones. Con la Consola web de ESET PROTECT, puede implementar ESET Management Agent en ordenadores no administrados que se hayan identificado a través de Active Directory o el Sensor de RD de ESET. También puede instalar manualmente ESET Management Agent en los ordenadores cliente.

- Rogue Detection Sensor: ESET PROTECT On-Prem Rogue Detection Sensor (RD) detecta los ordenadores no administrados presentes en su red y envía su información a ESET PROTECT Server. Puede agregar fácilmente nuevos ordenadores cliente a su red protegida. RD Sensor recuerda los ordenadores que se han detectado y no envía la misma información dos veces.

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

  - Descarga y almacena en caché: actualizaciones de los módulos de ESET, paquetes de instalación y

actualización enviados por ESET PROTECT On-Prem (por ejemplo, ESET Endpoint Security MSI Installer), actualizaciones de productos de seguridad de ESET (actualizaciones de componentes y productos), resultados de ESET LiveGuard.

- Reenviar comunicación desde las instancias de ESET Management Agent a ESET PROTECT On-Prem.

- Conector del dispositivo móvil: es un componente que permite la administración de dispositivos móviles con ESET PROTECT On-Prem, gracias a la que puede administrar dispositivos móviles (Android e iOS) y ESET Endpoint Security para Android.

⚠ El componente ESET PROTECT Mobile Device Management/Connector (MDM/MDC) (solo local) llega al fin de la vida útil en enero de 2024. Más información. Le recomendamos migrar a Cloud MDM.

Consulte también Información general sobre los elementos de la infraestructura de ESET PROTECT On-Prem.

ESET PROTECT On-Prem herramientas independientes

- Herramienta Mirror: la herramienta Mirror es necesaria para las actualizaciones de módulos sin conexión. Si los ordenadores cliente no tienen conexión a Internet, puede utilizar la herramienta Mirror para descargar archivos de actualización de servidores de actualizaciones de ESET y almacenarlos localmente.

- ESET Remote Deployment Tool: esta herramienta le permite implementar paquetes todo en uno creados en la Consola web de ESET PROTECT. Puede distribuir ESET Management Agent con un producto de ESET en los ordenadores de una red según le convenga.

Soluciones adicionales de ESET

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 complementaria nativa de ESET PROTECT Web Console y ofrece la administración del cifrado de disco completo de estaciones de trabajo Windows y macOS administradas con una capa adicional de seguridad en el inicio de sesión previo al arranque.

- ESET LiveGuard Advanced – ESET LiveGuard Advanced (entorno de pruebas en la nube) es un servicio de pago que proporciona ESET. Su finalidad es agregar una capa de protección diseñada específicamente para paliar las amenazas nuevas.

- ESET Inspect On-Prem: un completo sistema Endpoint de detección y respuesta que incluye funciones como las siguientes: detección de incidentes, administración de incidentes y respuesta, recopilación de datos, indicadores de detección de riesgo, detección de anomalías, detección de comportamientos e incumplimientos de políticas.

Sincronizar licencias

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

- ESET Business Account: el portal de licencias para 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 la ayuda

La Guía de administración se escribió para ayudarle a familiarizarse con ESET PROTECT On-Prem y contiene instrucciones sobre cómo utilizarlo.

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

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

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

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

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

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

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

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

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

Leyenda de los iconos

Esta es una colección de iconos utilizados en ESET PROTECT Web Console con su descripción. Algunos de los iconos describen acciones, tipos de elementos o el estado actual. La mayoría de los iconos se muestran en uno de los tres colores para indicar la accesibilidad de un elemento:

Icono predeterminado: acción disponible

Icono azul: elemento resaltado cuando pasa sobre él el puntero del ratón

Icono gris: acción no disponible

Icono de estado	Descripciones
	Detalles sobre el dispositivo cliente.
	Agregar dispositivo: agregue nuevos dispositivos. **Nueva tarea**: para agregar una nueva tarea. **Nueva notificación**: para agregar una nueva notificación. **Nuevos grupos estáticos/dinámicos**: para agregar nuevos grupos
	Modificar: puede modificar las tareas, notificaciones, plantillas de informes, grupos, políticas, etc. que cree.
	Duplicar : le permite crear un nueva directiva basada en la directiva existente que ha seleccionado, se requiere un nuevo nombre para el duplicado.
	Mover: ordenadores, políticas o grupos estáticos o dinámicos. **Grupo de acceso** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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, etc. seleccionados por completo.
	Cambiar nombre de varios elementos: si selecciona varios elementos, puede cambiarles el nombre uno a uno en una lista o utilizar la búsqueda de expresiones regulares (Regex) y sustituir varios elementos a la vez.
	Análisis: al utilizar esta opción se ejecutará la tarea Análisis a petición en el cliente que haya notificado la detección.
	Actualizaciones > **Actualizar módulos**: al utilizar esta opción se ejecutará la tarea Actualización de módulos (activa una actualización de forma manual). **Actualizar** > **Actualizar productos de ESET**: se actualizan los productos de ESET instalados en el dispositivo seleccionado. **Actualizar** > **Actualizar sistema operativo**: se actualiza el sistema operativo del dispositivo seleccionado.
	Registro de auditoría - Permite ver el Registro de auditoría del elemento seleccionado.
	Ejecutar tarea para dispositivos móviles.
	Inscribir de nuevo: vuelva a inscribir un dispositivo móvil.
	Desbloquear: el dispositivo se desbloqueará.
	Bloquear: el dispositivo se bloqueará cuando se detecte actividad sospechosa o esté marcado como desaparecido.
	Buscar: si desea solicitar las coordenadas GPS de su dispositivo móvil.
	Modo sirena/perdido: activa una potente sirena de forma remota, la sirena sonará aunque el dispositivo esté en silencio.
	Restablecimiento de fábrica: todos los datos almacenados en el dispositivo se borrarán de forma permanente.
	Inicio/Apagado: haga clic en un ordenador y seleccione **Inicio/Apagado** > **Reiniciar** para reiniciar el dispositivo. Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste. **Restaurar**: para restaurar un archivo en cuarentena en su ubicación original.
	Apagar: haga clic en un ordenador y seleccione **Inicio/Apagado** > **Apagar** para apagar el dispositivo. Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste. Desactivar productos
	Cerrar sesión: haga clic en un ordenador y seleccione **Inicio/Apagado** > **Cerrar sesión** para cerrar la sesión de todos los usuarios del ordenador.
	Ejecutar tarea: seleccione una tarea y configure el desencadenador y la aceleración (opcional) de esta tarea. La tarea se pone en la cola de acuerdo con los parámetros de la tarea. Esta opción desencadena inmediatamente una tarea existente que usted selecciona de una lista de tareas disponibles.
	Tareas recientes: muestra las tareas recientes. Haga clic en una tarea para volver a ejecutarla.
	Asignar usuario: para asignar un usuario a un dispositivo. Puede administrar los usuarios en Usuarios del ordenador.
	Administrar políticas: una política también se puede asignar directamente a uno o varios clientes, no solo a un grupo. Seleccione esta opción para asignar la política a los clientes seleccionados.
	Enviar llamada de activación: ESET PROTECT Server ejecuta la replicación instantánea de ESET Management Agent en un equipo cliente a través de EPNS. Esto es útil cuando no quiere esperar al intervalo regular en el que el ESET Management Agent se conecta al ESET PROTECT Server. Por ejemplo cuando desea ejecutar una tarea del cliente de inmediato en los clientes o si desea aplicar de inmediato una política.
	Implementar el agente: cree un instalador de ESET Management Agent para implementarlo 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.
	Silencio: si selecciona un ordenador y pulsa **Silencio**, el agente de este cliente dejará de informar a ESET PROTECT On-Prem; solo agregará la información. En la columna Silenciado se muestra un icono de silencio junto al nombre del ordenador. Cuando se desactiva el silencio haciendo clic en **Quitar silencio**, el ordenador que estaba silenciado volverá a informar y se restaura la comunicación entre ESET PROTECT On-Prem y el cliente.
	Desactivar: para desactivar o quitar el ajuste o la selección.
	Asignar: asigne una política a clientes o grupos.
	Importar: seleccione en Informes/Políticas/Clave pública lo que desea importar.
	Exportar: seleccione en Informes/Políticas/Certificado de iguales lo que desea exportar.
	Etiquetas - Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
	Grupo estático
	Grupo dinámico
	No aplicar el indicador de política
	Aplicar el indicador de política
	Forzar el indicador de política
	Desencadenadores: consulte la lista de Desencadenadores para la tarea del cliente seleccionada.
	Escritorio
	Móvil
	Servidor
	Servidor de archivos

Icono de estado	Descripciones
	Servidor de correo
	Servidor de puerta de enlace
	Servidor de colaboración
	ESET Management Agent
	Conector del dispositivo móvil
	Rogue Detection Sensor
	ESET PROTECT Server
	ESET Inspect Server
	ESET Bridge
	Tipo de detección de **antivirus**. Consulte todos los tipos de detección en Detecciones. Haga clic en un ordenador y seleccione **Soluciones** > **Implementar producto de seguridad** para implementar un producto de seguridad ESET en el ordenador.
	Haga clic en un ordenador o en el icono del engranaje situado junto a un grupo estático y seleccione **Soluciones** > **Activar ESET LiveGuard** para activar ESET LiveGuard Advanced.
	ESET Inspect Connector Haga clic en **Ordenadores** > seleccione uno o más ordenadores y haga clic en **Ordenador** > **Soluciones** > **Activar ESET Inspect On-Prem** para implementar ESET Inspect Connector en los ordenadores Windows/Linux/macOS administrados. El ESET Inspect On-Prem solo está disponible cuando tiene la licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de ESET Inspect**.
	Haga clic en un ordenador y seleccione **Soluciones** > **Activar cifrado** para activar ESET Full Disk Encryption en el ordenador seleccionado.
	El ordenador tiene ESET Full Disk Encryption activado.

Ayuda sin conexión

La ayuda sin conexión de ESET PROTECT On-Prem no se instala de forma predeterminada. Si necesita ayuda de ESET PROTECT On-Prem que pueda utilizar sin conexión (si no tiene acceso a Internet en ocasiones o nunca), siga los pasos que se indican a continuación para agregar la ayuda sin conexión.

> La actualización de Web Console y Apache Tomcat borra los archivos de la Ayuda sin conexión. Si usó la ayuda sin conexión con una versión más antigua de ESET PROTECT On-Prem, vuelva a crearla para ESET PROTECT On-Prem 11.0 tras la actualización. De esta forma se asegura de que tiene la ayuda sin conexión más reciente que coincide con la versión de ESET PROTECT On-Prem.

Haga clic en el código de idioma para descargar la ayuda sin conexión para su ESET PROTECT On-Prem en el idioma deseado. Incluso puede instalar la ayuda sin conexión en varios idiomas.

Instrucciones de configuración de la ayuda sin conexión para Windows

1. Descargue un archivo *.zip* haciendo clic en un código de idioma en la siguiente tabla para descargar la ayuda sin conexión para su ESET PROTECT On-Prem en el idioma deseado.
2. Guarde el archivo *.zip* (por ejemplo, en una unidad flash USB).
3. Cree una nueva carpeta llamada *help* en el ordenador que ejecute ESET PROTECT Web Console en la siguiente ubicación: *%ProgramFiles%\Apache Software Foundation\[carpeta Tomcat]\webapps\era\webconsole*.
4. Copie el archivo *.zip* en la carpeta *help*.
5. Extraiga el contenido del archivo *.zip* , por ejemplo *en-US.zip*, en una carpeta con el mismo nombre, en este caso, **en-US**, de modo que la estructura de carpetas tenga este aspecto: *%ProgramFiles%\Apache Software Foundation\[Tomcat folder]\webapps\era\webconsole\help\en-US*

Ya puede abrir su ESET PROTECT Web Console, seleccionar el idioma e iniciar sesión. La ayuda sin conexión de ESET PROTECT On-Prem se abrirá cada vez que haga clic en el icono **Ayuda** situado en la esquina superior derecha y haga clic en **Tema correspondiente** - **Ayuda**.

> Puede agregar la ayuda sin conexión en varios idiomas si es necesario, siguiendo los pasos anteriores.

> Si el ordenador o el dispositivo móvil desde los que accede a ESET PROTECT Web Console no tienen conexión a Internet, tendrá que cambiar la configuración de ESET PROTECT Web Console para **obligar a la ayuda sin conexión de ERAESET PROTECT On-Prem** a abrirse de forma predeterminada (en vez de la ayuda en línea). Para hacerlo, siga las instrucciones que se indican a continuación de la tabla.

Instrucciones de configuración de la ayuda sin conexión para Linux

1. Descargue un archivo *.tar* haciendo clic en un código de idioma en la siguiente tabla para descargar la ayuda sin conexión para su ESET PROTECT On-Prem en el idioma deseado.
2. Guarde el archivo *.tar* (por ejemplo, en una unidad flash USB).
3. Abra una ventana del terminal y vaya a */usr/share/tomcat/webapps/era/webconsole*
4. Cree una nueva carpeta llamada *ayuda* ejecutando el 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` para el 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, mediante la ejecución del comando `tar -xvf en-US.tar`.

Ya puede abrir su ESET PROTECT Web Console, seleccionar el idioma e iniciar sesión. La ayuda sin conexión de ESET PROTECT On-Prem se abrirá cada vez que haga clic en el icono **Ayuda** situado en la esquina superior derecha y haga clic en **Tema correspondiente** - **Ayuda**.

Para actualizar la ayuda sin conexión tras 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 mostrado anteriormente. Tras sustituir la carpeta, continúe de la forma normal.

Puede agregar la ayuda sin conexión en varios idiomas si es necesario, siguiendo los pasos anteriores.

Si el ordenador o el dispositivo móvil desde los que accede a ESET PROTECT Web Console no tienen conexión a Internet, tendrá que cambiar la configuración de ESET PROTECT Web Console para **obligar a la ayuda sin conexión de ERAESET PROTECT On-Prem** a abrirse de forma predeterminada (en vez de la ayuda en línea). Para hacerlo, siga las instrucciones que se indican a continuación de la tabla.

Idioma compatible	Ayuda HTML sin conexión .zip	Ayuda HTML sin conexión .tar
Inglés	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 de 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 brasileño	pt-BR.zip	pt-BR.tar
Ruso	ru-RU.zip	ru-RU.tar
Español	es-ES.zip	es-ES.tar
Español de Latinoamérica	es-CL.zip	es-CL.tar
Eslovaco	sk-SK.zip	sk-SK.tar
Turco	tr-TR.zip	tr-TR.tar
Ucraniano	uk-UA.zip	uk-UA.tar

Forzar ayuda sin conexión 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. **Busque** la línea `help_show_online=true`, cambie el valor de este ajuste a `false` y guarde los cambios.
3. **Reinicie** el servicio Tomcat en los servicios o a través de la línea de comandos.

La ayuda sin conexión de ESET PROTECT On-Prem se abrirá cada vez que haga clic en el icono **Ayuda** situado en la esquina superior derecha y haga clic en **Tema correspondiente - Ayuda**. Se mostrará la ventana de ayuda correspondiente para la página actual.

Forzar ayuda sin conexión 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. **Busque** la línea `help_show_online=true`, cambie el valor de este ajuste 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`.

La ayuda sin conexión de ESET PROTECT On-Prem se abrirá cada vez que haga clic en el icono **Ayuda** situado en la esquina superior derecha y haga clic en **Tema correspondiente - Ayuda**. Se mostrará la ventana de ayuda correspondiente para la página actual.

Nuevas funciones de ESET PROTECT On-Prem

ESET LiveGuard Advanced informe de comportamiento

Como preparación para ofrecer nuevos informes de comportamiento más completos a los clientes que usan EDR, hemos agregado la opción de descargar informes de comportamiento generados por ESET LiveGuard Advanced. 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. Más información

Reglas de tiempo para grupos dinámicos

Hemos agregado la opción de incluir reglas de tiempo como criterios adicionales para las plantillas de grupo dinámico. Al configurar reglas de tiempo, los ordenadores solo se incluirán en los grupos dinámicos durante el periodo especificado. Más información

Cambio de nombre del producto

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

Otras mejoras y correcciones de errores

Descubra en el registro de cambios qué otras mejoras se han implementado.

Registro de cambios

Consulte también:

- La lista de todas las versiones de los componentes de ESET PROTECT
- problemas conocidos de ESET PROTECT On-Prem
- Política sobre el fin de la vida útil 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)

Consulte 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 de ESET e idiomas compatibles

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

- Windows, Linux y macOS

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

Navegador web
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

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

Versiones más recientes de productos de ESET que se pueden administrar con ESET PROTECT On-Prem 11.0

Las versiones del producto de seguridad de ESET que se enumeran a continuación se pueden administrar con ESET Management Agent versión 11.0 y posteriores.
Se recomienda utilizar la versión más reciente de ESET Management Agent para administrar por completo la última versión de los productos de seguridad de ESET y sus funciones. Si utiliza una versión de ESET Management Agent anterior a la versión de ESET PROTECT Server, es posible que algunas de las funciones de administración más recientes no estén disponibles.
Las versiones de los productos de seguridad de ESET que son anteriores a las que se muestran en la tabla siguiente no pueden gestionarse con ESET PROTECT On-Prem 11.0.
Si desea obtener más información sobre la compatibilidad, visite la política sobre el fin de la vida útil de los productos de ESET para empresas.

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	Superiores a 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 en 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 a través de la licencia de suscripción

Producto de ESET	Disponible desde la versión
ESET Endpoint Antivirus/Security para Windows	7.0
ESET Endpoint Antivirus/Security para macOS	6.8.x
ESET Endpoint Security para Android	2.0.158
Administración de dispositivos móviles de ESET para Apple iOS	7.0
ESET File Security para Microsoft Windows Server	7.0
ESET Mail Security para Microsoft Exchange	7.0
ESET File Security para Windows Server	7.0
ESET Mail Security para IBM Domino	7.0
ESET Security para Microsoft SharePoint Server	7.0
ESET File Security en Linux	7.0
ESET Endpoint Antivirus en Linux	7.0
ESET Server Security para Windows	8.0
ESET Server Security para Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect 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
Indonesio (Indonesia)*	id-ID
Italiano (Italia)	it-IT
Japonés (Japón)	ja-JP
Coreano (Corea)	ko-KR
Polaco (Polonia)	pl-PL
Portugués (Brasil)	pt-BR
Ruso (Rusia)	ru-RU
Español (Chile)	es-CL
Español (España)	es-ES
Eslovaco (Eslovaquia)	sk-SK
Turco (Turquía)	tr-TR
Ucraniano (Ucrania)	uk-UA

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

Introducción a ESET PROTECT On-Prem

ESET PROTECT On-Prem puede configurarse y administrarse mediante ESET PROTECT Web Console. Tras instalar ESET PROTECT On-Prem o implementar el dispositivo virtual de ESET PROTECT correctamente, puede conectarse a ESET PROTECT Server desde ESET PROTECT Web Console.

Puede comenzar la configuración después de haber instalado con éxito ESET PROTECT On-Prem.

Primeros pasos después de la implementación de ESET PROTECT Server

1.Abra ESET PROTECT Web Console en el navegador web e inicie sesión.

2.Agregue sus licencias a ESET PROTECT On-Prem.

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

4.Asigne la política integrada **Informe de aplicaciones: informa de todas las aplicaciones instaladas** a todos los ordenadores.

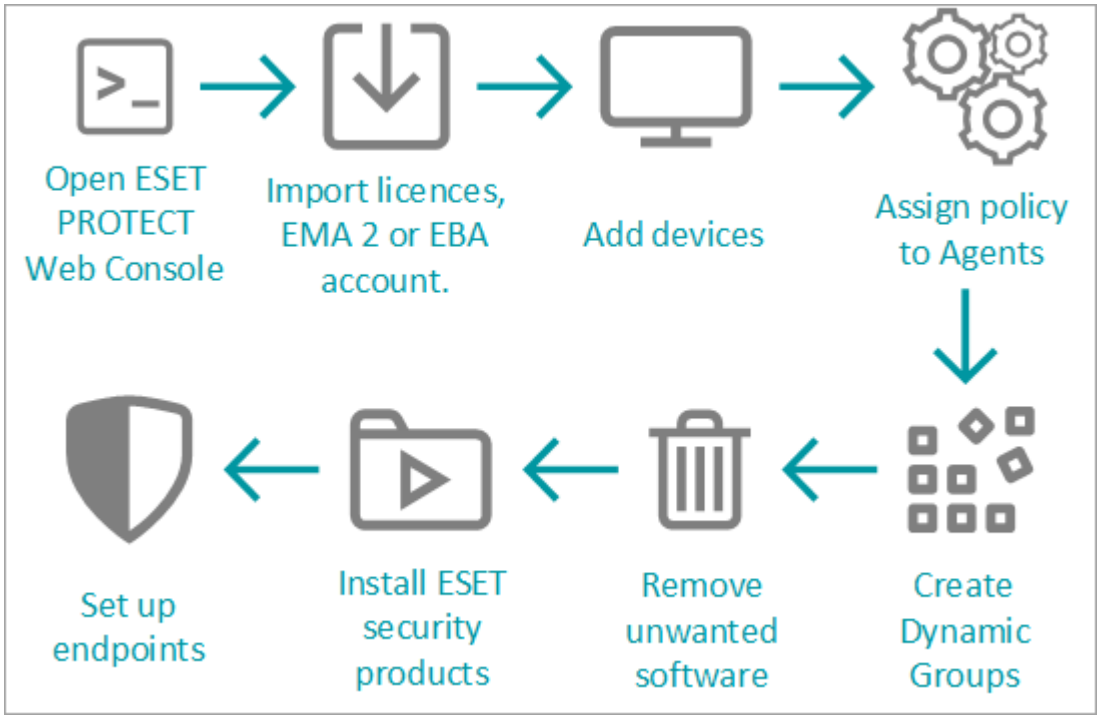
5.Cree un grupo dinámico para ordenadores con productos domésticos de ESET.

6.Elimine las aplicaciones antivirus de terceros con la tarea Desinstalación de software.

7.Instale los productos de seguridad de ESET con la tarea Instalación de software (a menos que haya instalado el agente con el instalador todo en uno).

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

seguridad de ESET. Por ejemplo, en equipos Windows con ESET Endpoint, asigne la política integrada **Antivirus: seguridad máxima, opción recomendada**. Consulte también Cómo administrar productos Endpoint desde ESET PROTECT On-Prem.



Pasos adicionales recomendados

• Familiarícese con ESET PROTECT Web Console, ya que es la interfaz que utilizará para administrar los productos de seguridad de ESET.

• Durante la instalación ha creado la cuenta de administrador predeterminada. Se recomienda guardar las credenciales de la cuenta de administrador en un lugar seguro y crear una nueva cuenta para administrar los clientes y configurar sus permisos.

No recomendamos utilizar la cuenta de **administrador** de ESET PROTECT On-Prem predeterminada como cuenta de usuario normal. Sirve como copia de seguridad si le sucede algo a las cuentas de usuario normales o si se queda bloqueado. Puede iniciar sesión con la cuenta de administrador para resolver esos problemas.

• Utilice notificaciones e informes para supervisar el estado de los ordenadores cliente de su entorno. Por ejemplo, si desea recibir una notificación cuando se produzca un evento específico o si desea ver o descargar un informe.

• Realice una copia de seguridad de su base de datos con regularidad para evitar la pérdida de datos.

• Le recomendamos que exporte la autoridad certificadora del servidor y los certificados de iguales. Si necesita volver a instalar ESET PROTECT Server, puede usar la autoridad certificadora y los certificados de iguales del ESET PROTECT Server original y no tendrá que volver a instalar los ESET Management Agent en los ordenadores cliente.

Apertura de ESET PROTECT Web Console

ESET PROTECT Web Console es la interfaz principal que se utiliza para comunicarse con ESET PROTECT Server. Puede pensar en ella como en un panel de control, un lugar central desde el que administrar todas las soluciones de seguridad de ESET. Es una interfaz web a la que se puede acceder con un navegador desde cualquier lugar y desde cualquier dispositivo con acceso a Internet. Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server.

Hay varias formas de abrir ESET PROTECT Web Console:

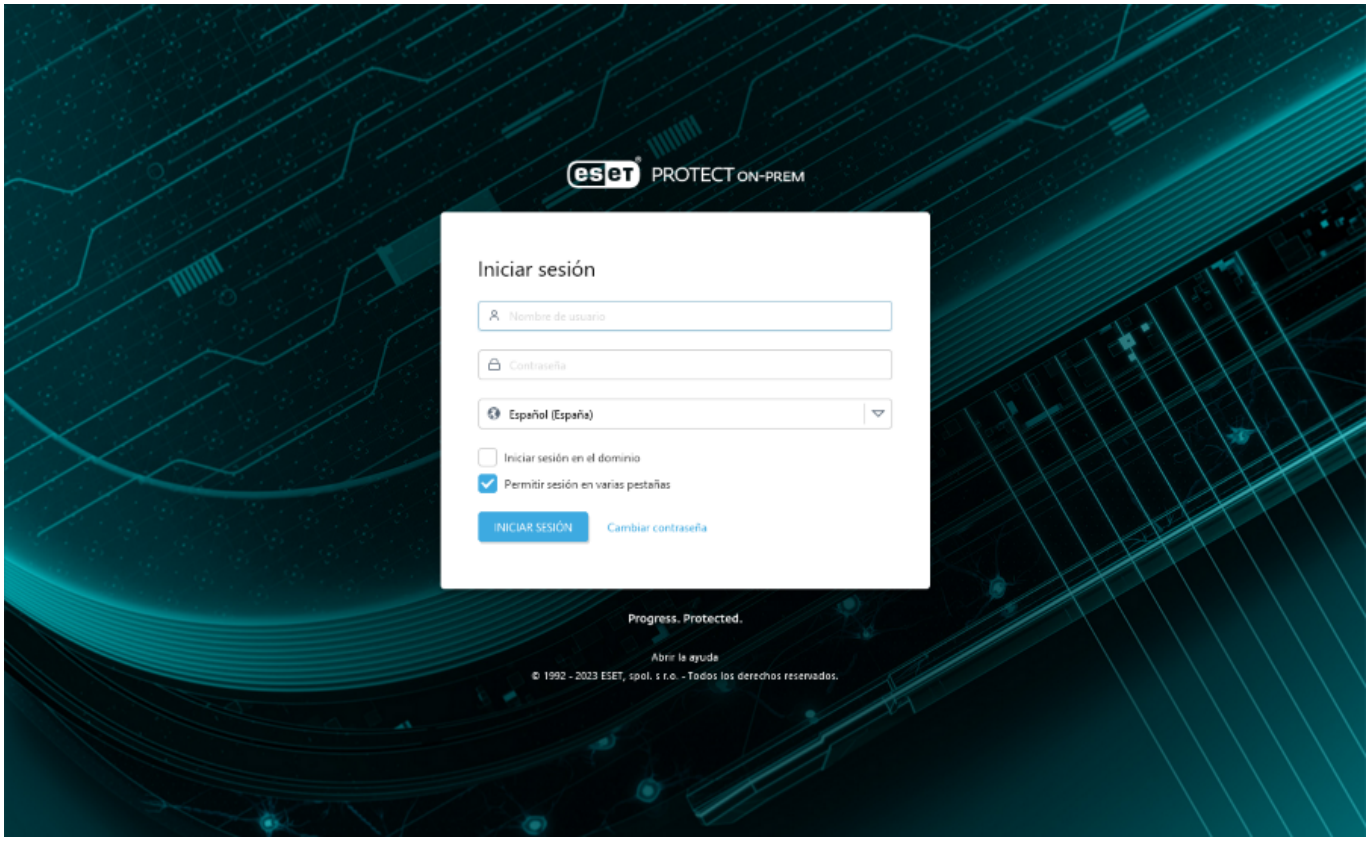
- En su **servidor local** (la máquina que aloja su Web Console), escriba esta URL en el navegador web: https://localhost/era/

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

- Para iniciar sesión en el **dispositivo virtual de ESET PROTECT On-Prem**, utilice la siguiente URL:
https://[Dirección IP]/
Reemplace "[dirección IP]" por la dirección IP de su máquina virtual de ESET PROTECT On-Prem.

- En su servidor local (el ordenador que aloja su Web Console), haga clic en **Inicio** > **Todos los programas** > **ESET** > **ESET PROTECT On-Prem** >**ESET PROTECT Web Console** y aparecerá una pantalla de inicio de sesión en su navegador web predeterminado. Esto no se aplica al dispositivo virtual de ESET PROTECT.

Cuando el servidor web (que ejecuta ESET PROTECT Web Console) esté conectado, se mostrará la siguiente pantalla de inicio de sesión.



Si es la primera vez que inicia sesión, proporcione las credenciales que ha introducido durante el proceso de instalación (seleccione su situación de instalación: Instalador todo en uno en Windows, implementación de dispositivo virtual, otras situaciones de instalación).

El usuario predeterminado de Web Console es **Administrator**. Para más detalles sobre esta pantalla, consulte pantalla de inicio de sesión de Web Console.

Si tiene problemas para iniciar sesión o recibe mensajes de error al intentar iniciar sesión, consulte la sección Solución de problemas de Web Console.

ESET PROTECT Web Console

ESET PROTECT Web Console es la interfaz principal que se utiliza para comunicarse con ESET PROTECT Server. Puede pensar en ella como en un panel de control, un lugar central desde el que administrar todas sus soluciones de seguridad de ESET. Es web y se puede acceder a ella con un navegador (ver Navegadores web compatibles) desde cualquier lugar y en cualquier dispositivo con acceso a Internet. Cuando inicie sesión en Web Console por primera vez, aparecerá ESET PROTECT On-PremRecorrido por ***.

En el diseño estándar de ESET PROTECT Web Console:

- El usuario actualmente conectado siempre se muestra en la esquina superior derecha, junto con la cuenta atrás del tiempo de espera para su sesión. Puede hacer clic en **Cerrar sesión** para cerrar sesión en cualquier momento. Cuando se agote el tiempo de espera de la sesión (debido a la inactividad del usuario), deberá iniciar sesión de nuevo. Para cambiar la configuración del usuario, haga clic en su nombre de usuario en la esquina superior derecha de ESET PROTECT Web Console.

- El Menú principalestá accesible a la izquierda en todo momento, excepto cuando está utilizando un asistente. Haga clic en para desplegar el menú de la parte izquierda de la pantalla; puede contraerlo

haciendo clic en **Contraer**.

- Si necesita ayuda para trabajar con ESET PROTECT On-Prem, haga clic en el icono **Ayuda** situado en la esquina superior derecha y, a continuación, haga clic en **Tema correspondiente - Ayuda**. Se mostrará la ventana de ayuda de la página actual. Haga clic en **Ayuda** > Acerca de para ver la versión de ESET PROTECT On-Prem y otros detalles.

- Puede utilizar la herramienta Buscar en la parte superior de ESET PROTECT Web Console. Escriba al menos 3 y un máximo de 30 caracteres en el campo de búsqueda para buscar estas categorías: **Nombre del ordenador**, **Descripción del ordenador**, **Dirección IP del ordenador**, **Nombre del grupo estático**, **Causa de la detección**, **Usuarios del ordenador**, **Nombre de usuario nativo** y **Nombre de usuario del 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 Web Console con el filtro de categoría aplicado.

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

Vínculos rápidos
Configurar ordenadores
• Agregar ordenador
• Agregar dispositivo móvil
• Implementación de Agent
• Agregar usuario del ordenador
Administrar ordenadores
• Crear tarea del cliente
• Crear nueva directiva
• Asignar directiva
Revisar estado
• Generar informe
• Componentes del servidor

- En la esquina superior izquierda de la pantalla, junto al nombre de ESET PROTECT On-Prem, encontrará el icono de navegación del producto que le ayudará a desplazarse entre ESET PROTECT On-Prem y otros productos: ESET Inspect On-Prem, ESET Business Account, ESET MSP Administrator (puede ver los respectivos productos en función de sus derechos de acceso y licencia).

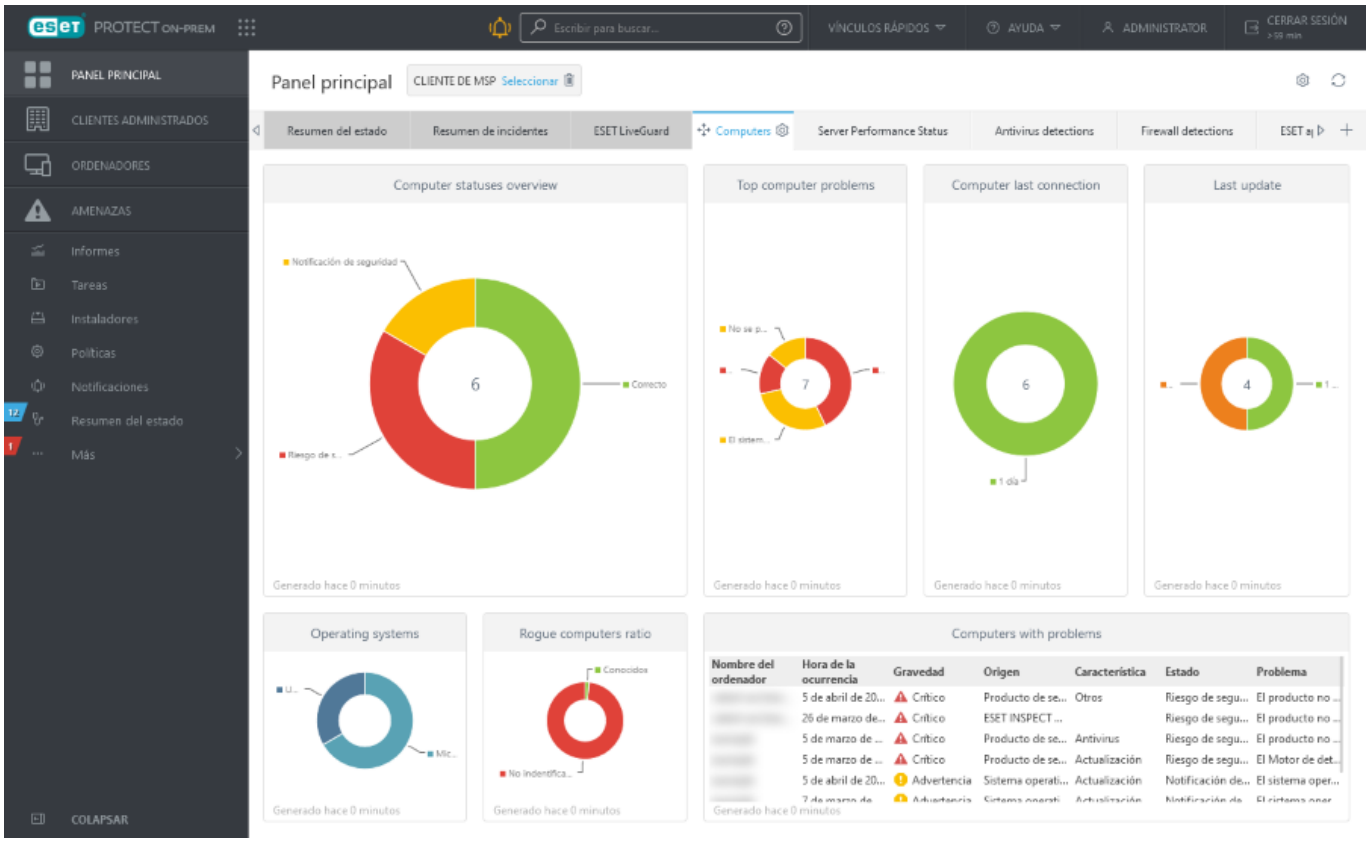
- El icono de **engranaje** siempre denota un menú contextual

- Haga clic en **Actualizar** para actualizar la información que se muestra.

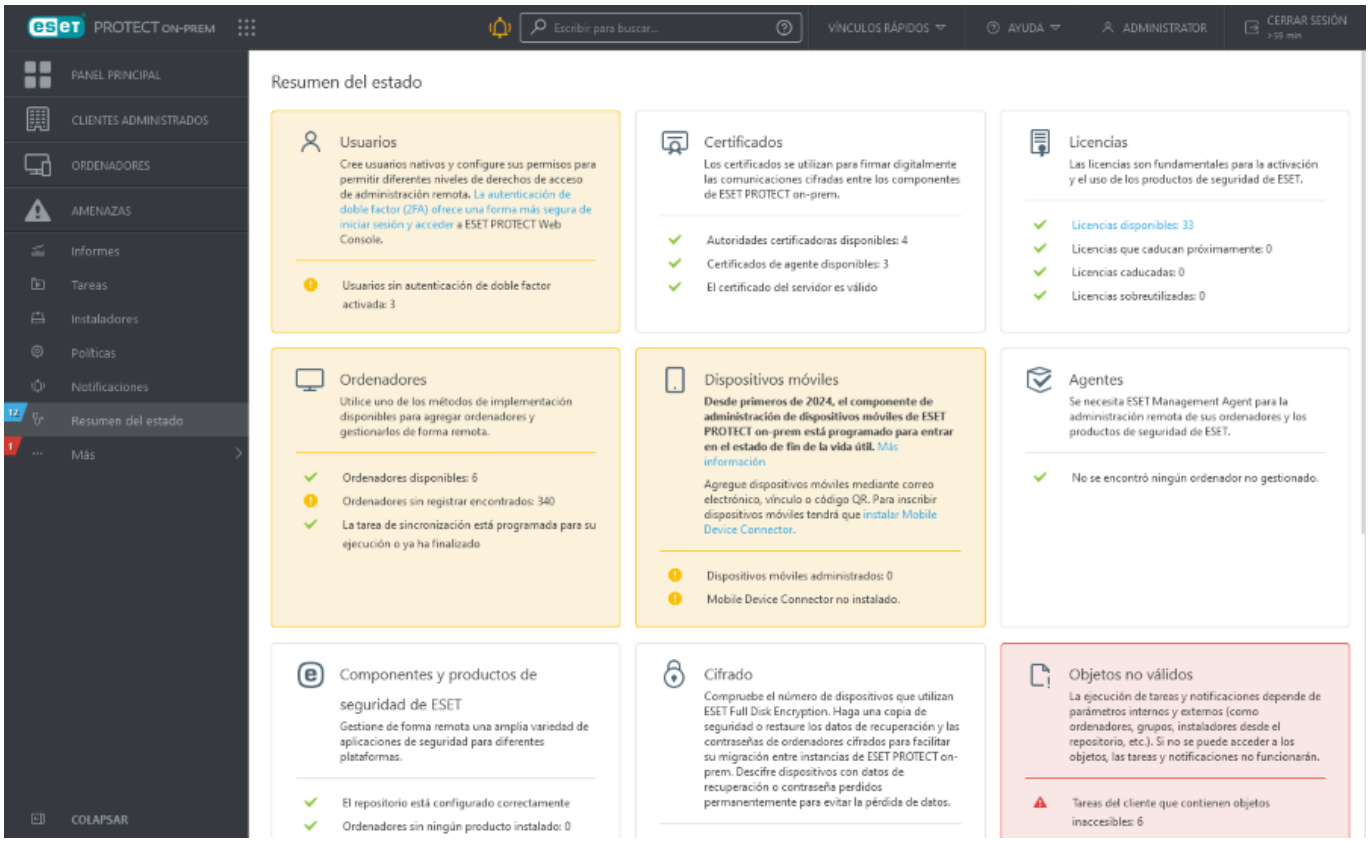
- Los botones de la parte inferior de la página son únicos para cada sección y función, y se describen en detalle en sus respectivos capítulos.

- ESET PROTECT Web Console 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.

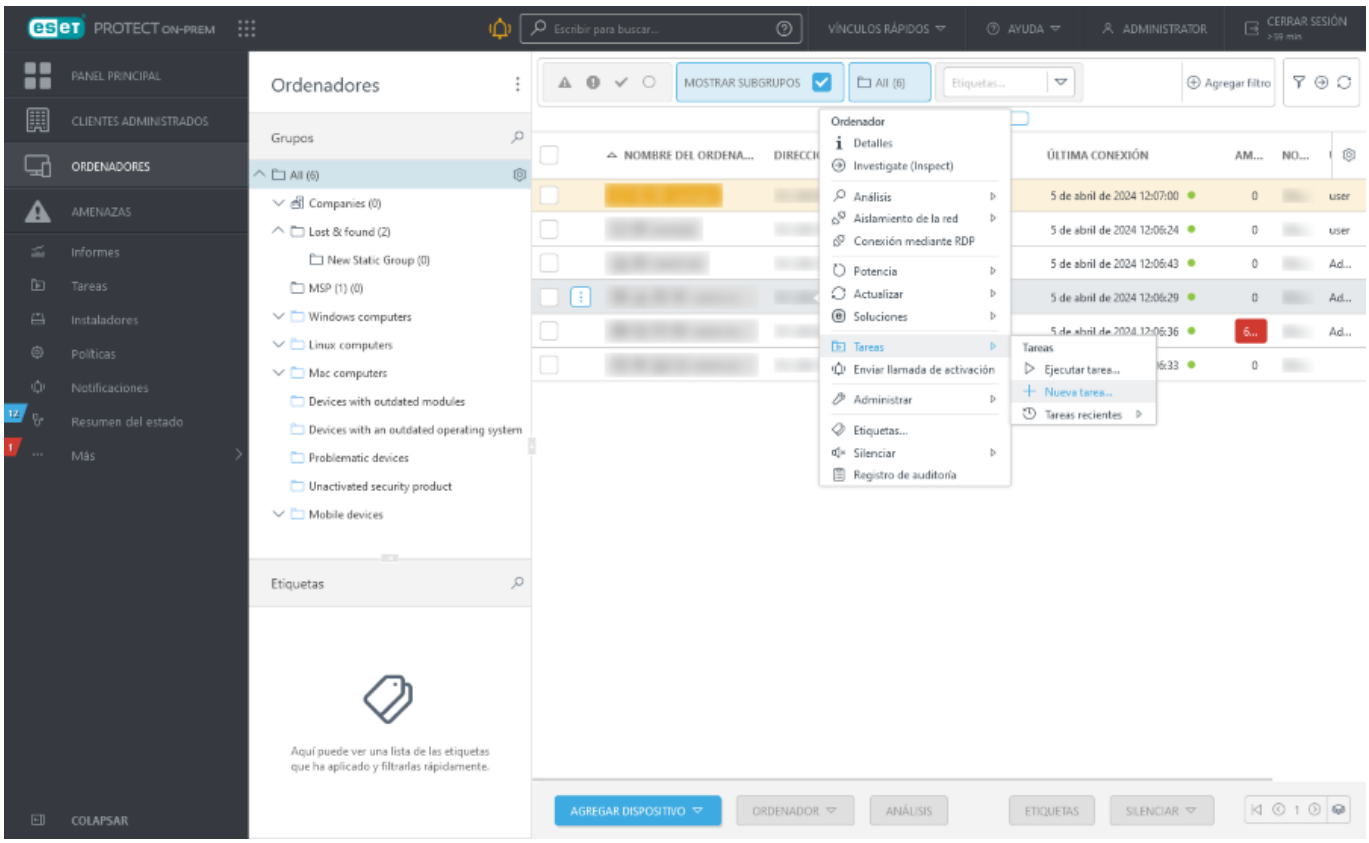


Resumen del estado le enseña cómo sacar el máximo partido de ESET PROTECT On-Prem. Le guiará a lo largo de los pasos recomendados.



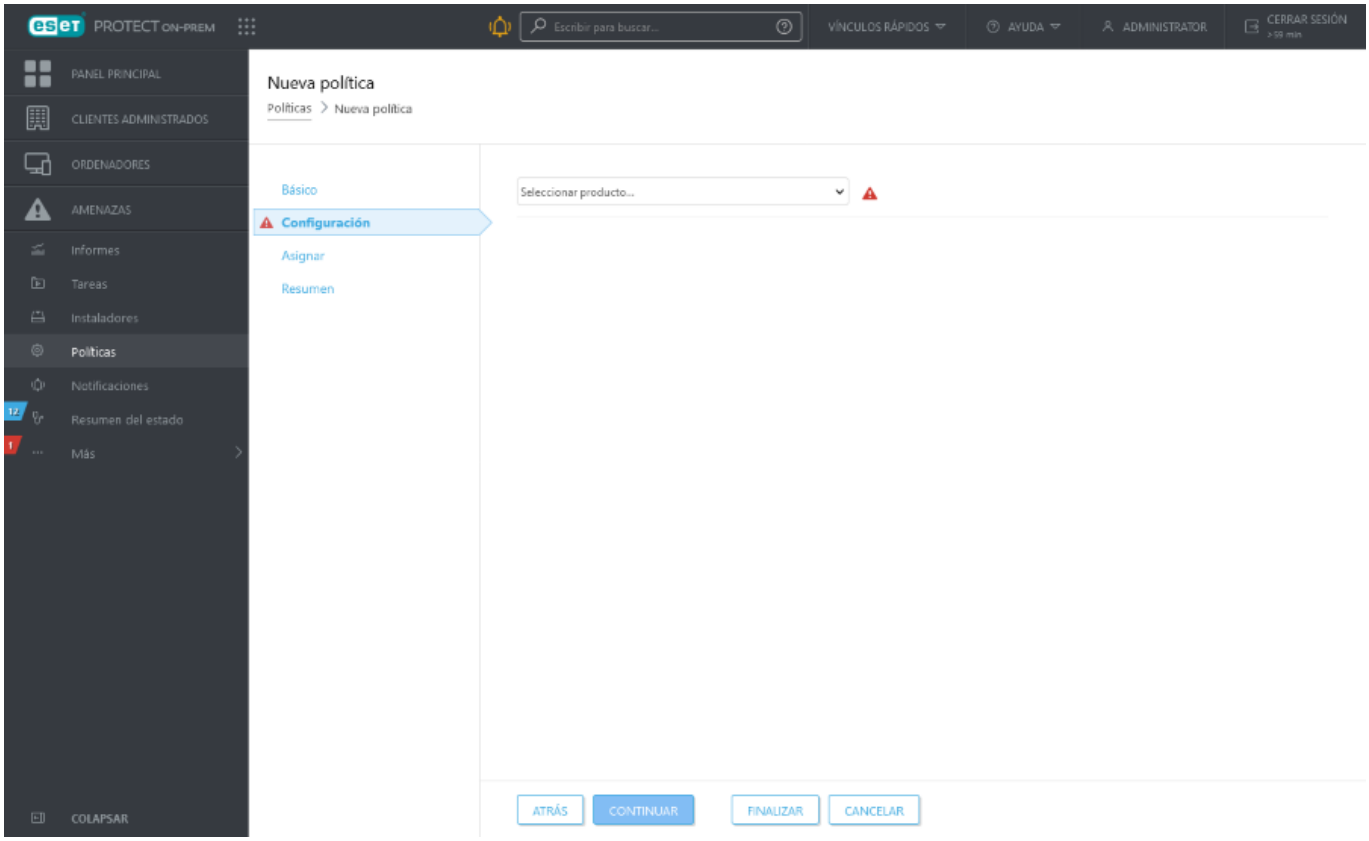
Las pantallas con árboles tienen controles específicos. El árbol en sí se encuentra a la izquierda con las acciones debajo. Haga clic en un elemento del árbol para ver las opciones.

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



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

- Los pasos están orientados verticalmente de arriba a abajo.
- Puede volver a un paso en cualquier momento
- La configuración obligatoria (necesaria) está siempre marcada con un signo de exclamación rojo junto a la sección y los respectivos ajustes.
- Los datos introducidos incorrectamente se marcan cuando mueve el cursor a un campo nuevo. El paso del asistente que contiene los datos de entrada no válidos también se marca.
- **Finalizar** no estará disponible hasta que todos los datos introducidos sean correctos.



Pantalla de inicio de sesión

Los usuarios deben tener credenciales de inicio de sesión (nombre de usuario y contraseña) para acceder a Web Console.

Para iniciar sesión como un usuario de dominio (un miembro del grupo de seguridad de dominio asignado), marque 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`
- LDAP de Linux y dispositivo virtual de ESET PROTECT: `username@FULL.DOMAIN.NAME`

> Si tiene problemas para iniciar sesión o recibe mensajes de error al intentar iniciar sesión, consulte la sección Solución de problemas de Web Console, donde encontrará sugerencias con las que resolver el problema.

Puede **seleccionar el idioma** haciendo clic en la flecha desplegable situada junto al idioma seleccionado; si desea obtener información adicional, consulte nuestro artículo de la base de conocimiento.

> Tenga en cuenta que no todos los elementos de la consola web cambiarán después del cambio de idioma. Algunos de los elementos (paneles predeterminados, políticas, tareas, etc.) se crean durante la instalación de ESET PROTECT On-Prem y su idioma no puede cambiarse.

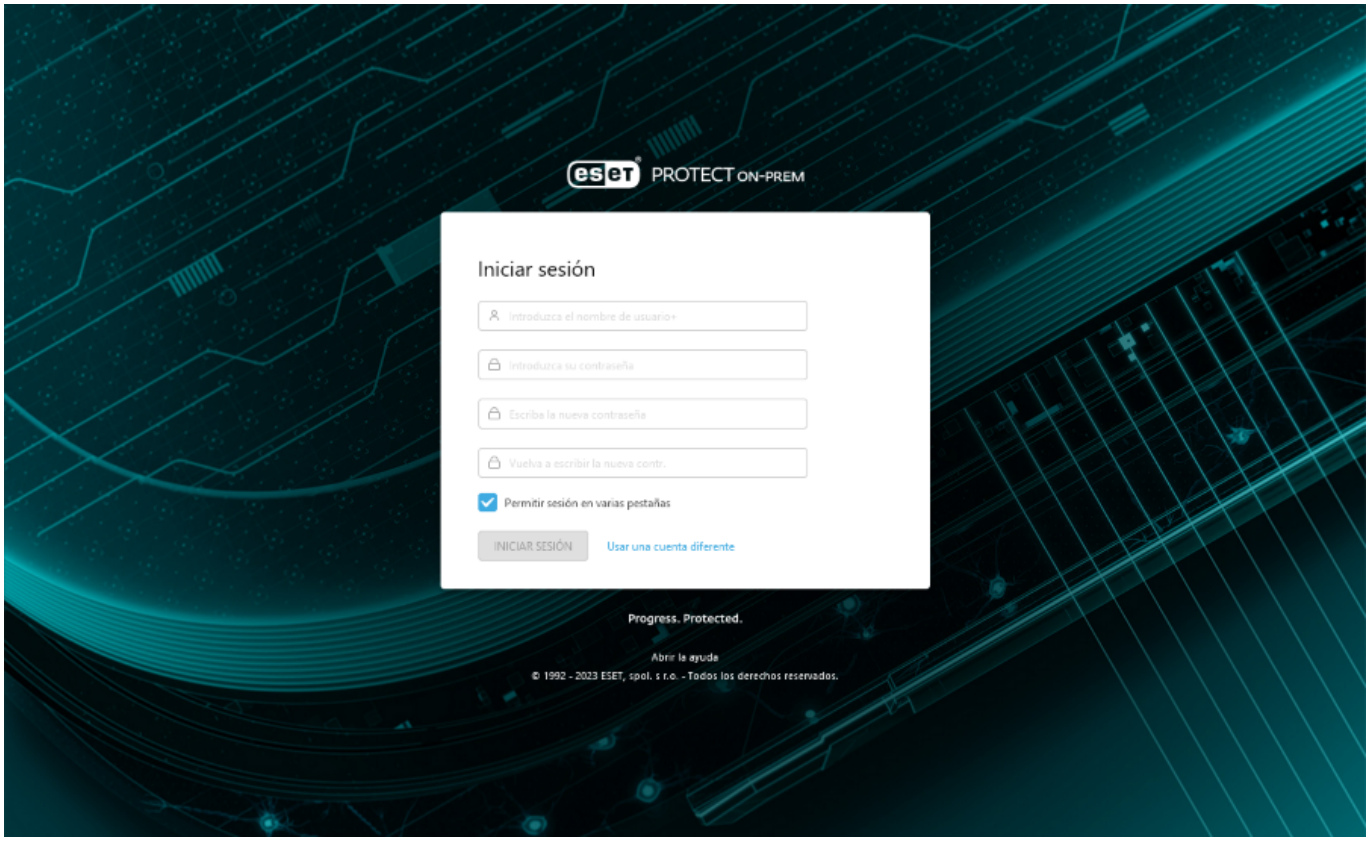
Permitir sesión en varias fichas: Web Console se puede abrir en varias fichas de un mismo navegador.

- Si se marca la casilla de verificación, cada ficha que tenga una sesión de Web Console abierta en un navegador se conectará a la misma sesión. Si se abre una nueva ficha, el resto de fichas conectadas con el

mismo ajuste se conectarán a esta nueva sesión. Si se cierra la sesión de una de las fichas, también se cerrará la sesión del resto de fichas.

- Si la casilla de verificación no se marca, cada nueva ficha abre una sesión de ESET PROTECT Web Console nueva independiente.

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



Administración de la 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, si se utilizan credenciales de inicio de sesión incorrectas), se bloquearán temporalmente los intentos adicionales de inicio de sesión desde esta dirección IP. Esto se indica con el mensaje de error: **No se pudo iniciar sesión: el usuario estaba bloqueado. Inténtelo de nuevo más tarde.** Transcurridos 10 minutos, inicie sesión con las credenciales correctas. La prohibición de intentos de inicio de sesión de la dirección IP no afecta a las sesiones existentes.

Bloqueo de dirección por ID de sesión incorrecta

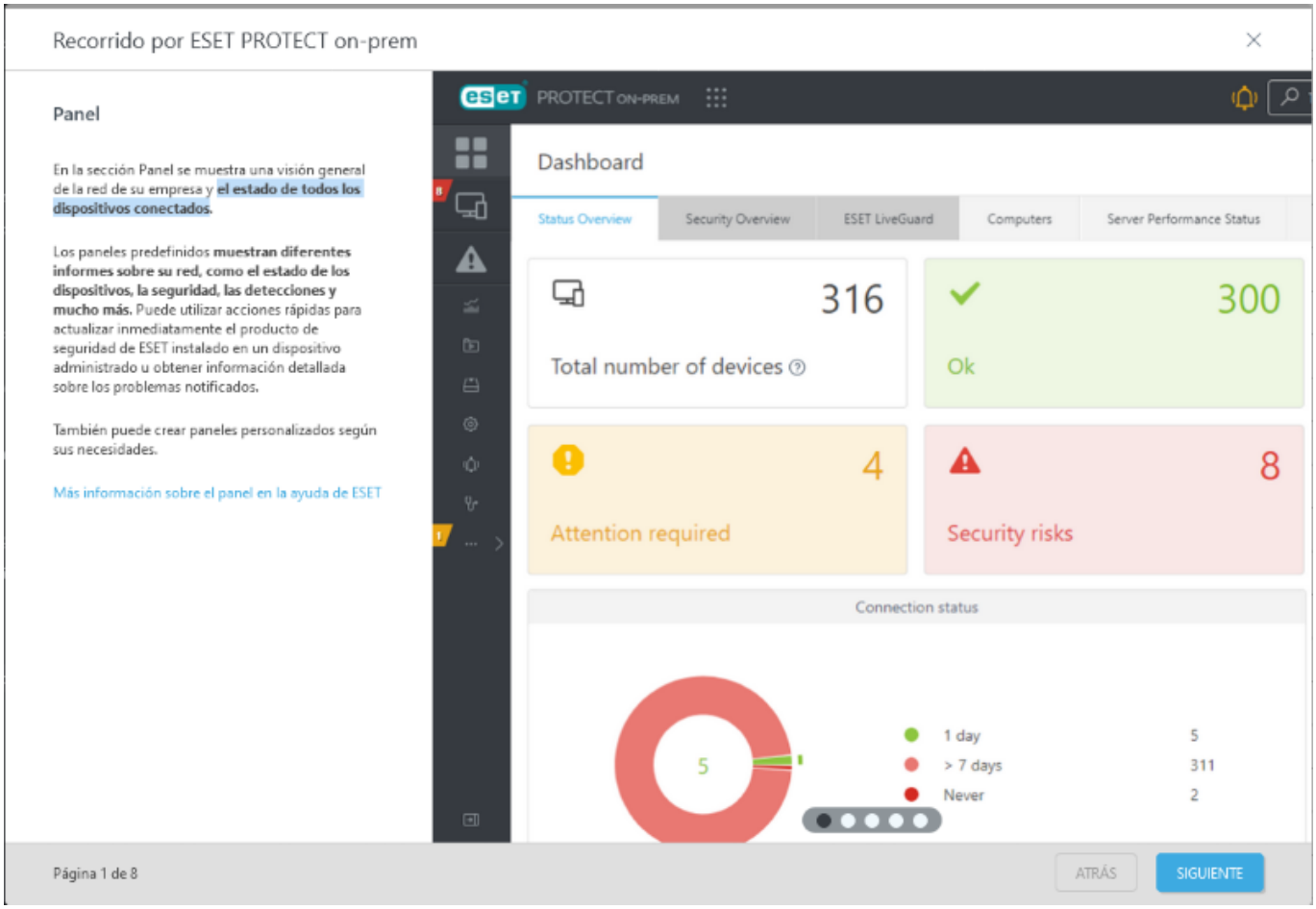
Después de usar un ID de sesión no válido 15 veces desde la misma dirección IP, las conexiones desde esa dirección IP se bloquean durante aproximadamente 15 minutos. No se cuentan los ID de sesiones caducadas. Si en el navegador hay un ID de sesión caducada, no se considera como ataque. La prohibición durante 15 minutos de la dirección IP afecta a todas las acciones (incluidas las solicitudes válidas). La prohibición se puede cancelar reiniciando Web Console (servicio `tomcat`).

Recorrido por ESET PROTECT On-Prem

Cuando inicie sesión en Web Console por primera vez, aparecerá un ESET PROTECT On-PremRecorrido por .

Este asistente le ofrecerá una explicación básica de secciones importantes de ESET PROTECT Web Console, ESET Management Agent y los productos de seguridad de ESET. Obtendrá información sobre Paneles, Ordenadores, Detecciones, Tareas, Políticas, Notificaciones y las Actualizaciones automáticas del producto.

Haga clic en **Proteger dispositivos** en el último paso de **Recorrido por ESET PROTECT On-Prem** para implementar instancias de ESET Management Agent en los ordenadores de su red. También puede crear el instalador del agente sin el asistente haciendo clic en **Instaladores** > Crear instalador.



Si no desea utilizar el **Recorrido por ESET PROTECT On-Prem**, haga clic en **X**. Se abrirá ESET PROTECT Web Console. El **Recorrido por ESET PROTECT On-Prem** no aparecerá la próxima vez que inicie sesión en ESET PROTECT Web Console.

Para volver a ver **Recorrido por ESET PROTECT On-Prem** , haga clic en **Ayuda** > **Recorrido por ESET PROTECT On-Prem**.

Tras el primer inicio de sesión en ESET PROTECT Web Console, le recomendamos ejecutar la tarea del cliente Actualización de los sistemas operativos en el ordenador en el que está instalado ESET PROTECT On-Prem para asegurarse de que el sistema operativo esté actualizado (por motivos de seguridad y de rendimiento).

Configuración del usuario

En esta sección puede personalizar la configuración del usuario. Haga clic en **Cuenta del usuario** en la esquina superior derecha de ESET PROTECT Web Console (a la izquierda del botón **Cerrar sesión**) para mostrar todos los usuarios activos. Puede iniciar sesión en ESET PROTECT Web Console desde diferentes navegadores web, ordenadores o dispositivos móviles al mismo tiempo. Aquí verá todas sus sesiones.

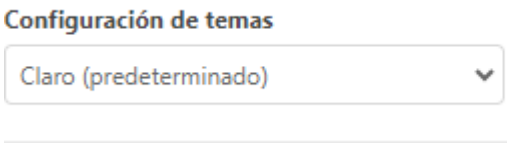
La configuración del usuario solo se aplica al usuario que ha iniciado sesión.

Configuración de temas

Puede seleccionar el ajuste de tema para la pantalla de ESET PROTECT On-Prem:

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

Seleccione el tema en el menú desplegable:



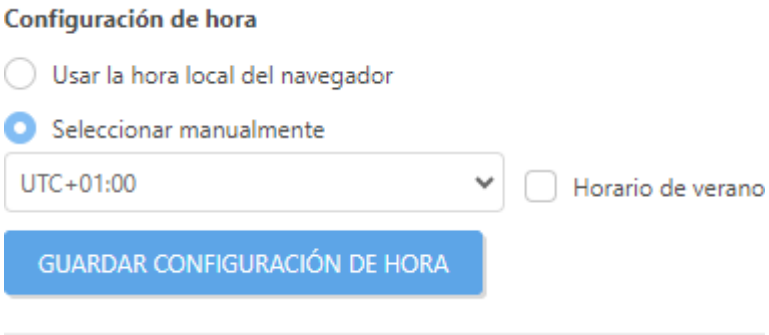
La pantalla permanece en el tema seleccionado tras cerrar sesión en Web Console e iniciar sesión de nuevo.

Configuración de hora

Cada usuario puede tener su propia configuración de fecha y hora favorita en ESET PROTECT Web Console. A cada usuario se le aplica su configuración de fecha y hora específica, sin importar desde dónde acceda a ESET PROTECT Web Console.

Toda la información se almacena de forma interna en ESET PROTECT On-Prem utilizando el estándar UTC (Tiempo universal coordinado). El tiempo UTC se convierte automáticamente a la zona horaria utilizada por ESET PROTECT Web Console (teniendo en cuenta el horario de verano). ESET PROTECT Web Console muestra la hora local del sistema en el que se ejecuta ESET PROTECT Web Console (no la hora UTC interna). Si lo prefiere, puede anular este ajuste para establecer la hora mostrada en ESET PROTECT Web Console manualmente.

Si quiere anular la configuración predeterminada, **Usar la hora local** del navegador, puede elegir la opción **Seleccionar manualmente** y, a continuación, especificar la zona horaria de la consola de forma manual y decidir si desea utilizar el horario de verano.

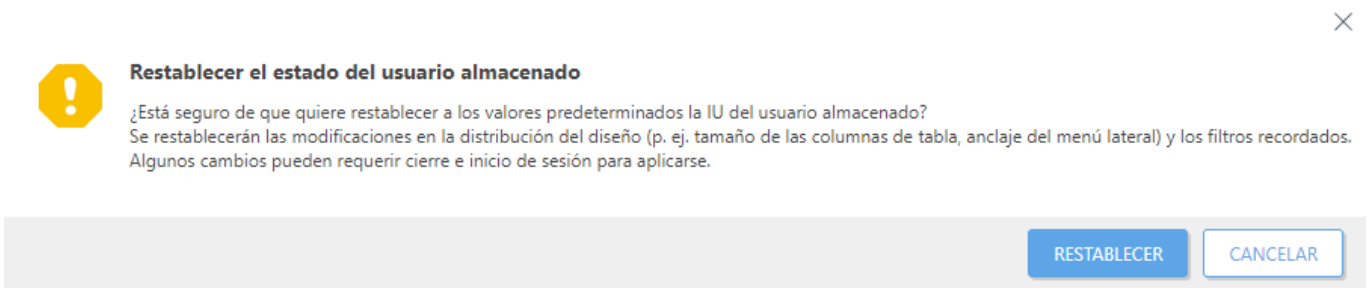


En algunos casos, la opción de utilizar una zona horaria distinta estará disponible. Cuando se configura un desencadenador, se utiliza la zona horaria de ESET PROTECT Web Console de forma predeterminada. También puede marcar la casilla de verificación **Usar la hora local del destino** para usar la zona horaria local del dispositivo de destino en lugar de la zona horaria de ESET PROTECT Web Console para el desencadenador.

Haga clic en el botón **Guardar configuración de hora** para confirmar sus cambios.

Estado almacenado del usuario

Puede restablecer los valores predeterminados de un estado almacenado de la IU del usuario haciendo clic en **Restablecer estado almacenado del usuario**. Esto incluye el ESET PROTECT On-PremRecorrido por***, los tamaños de columna de las tablas, los filtros recordados, el menú lateral anclado, etc.



Dispositivos recordados

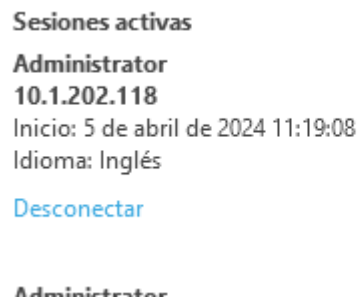
Olvidar dispositivos recordados: requiera autenticación de doble factor en del usuario actual en los dispositivos recordados.

Sesiones activas

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

- Nombre de usuario actual.
- Detalles del ordenador que accede a Web Console: navegador web y sistema operativo.
- La dirección IP de un ordenador cliente o un dispositivo desde el que se conecta un usuario a ESET PROTECT Web Console. La dirección IP de un servidor web que ejecuta ESET PROTECT Web Console se muestra entre paréntesis. En caso de que ESET PROTECT Web Console se esté ejecutando en la misma máquina que ESET PROTECT Server, se mostrará **vía 127.0.0.1**.
- Fecha y hora de inicio de sesión del usuario.

- Idioma seleccionado para ESET PROTECT Web Console.



La sesión actual lleva la etiqueta **Esta sesión**. Si desea desconectar una sesión activa, haga clic en **Desconectar**.

Filtros y personalización del diseño

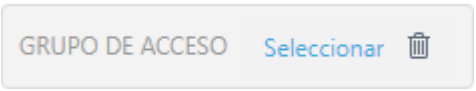
ESET PROTECT Web Console le permite personalizar el diseño de los elementos que aparecen en las secciones principales (por ejemplo, **Ordenadores**, **Tareas**, etc.) de varias maneras:

Agregar filtros y preajustes de filtros

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

Los filtros pueden guardarse en el perfil de usuario para que pueda volver a utilizarlos en el futuro. Haga clic en el icono de **Preestablecidos** para administrar los conjuntos de filtros:

Conjuntos de filtros	Esta opción muestra los filtros guardados; haga clic en uno de ellos para aplicarlo. El filtro aplicado se indica con una marca de verificación. Seleccione **Incluir columnas visibles, ordenación y paginación** para guardar estos parámetros en el filtro preestablecido.
Guardar conjunto de filtros	Guarde la configuración de filtro actual como un nuevo filtro preestablecido. Una vez guardado el filtro preestablecido, no puede editar la configuración del filtro en el filtro preestablecido.
Gestionar conjuntos de filtros	Elimine los filtros preestablecidos existentes o cámbieles el nombre. Haga clic en **Guardar** para aplicar los cambios a los filtros preestablecidos.
Borrar valores del filtro	Haga clic para eliminar solo los valores actuales de los filtros seleccionados. Los filtros preestablecidos guardados no cambiarán.
Quitar filtros	Haga clic para eliminar los filtros seleccionados. Los filtros preestablecidos guardados no cambiarán.
Quitar filtros no utilizados	Elimine los campos de filtros sin ningún valor.
Restablecer filtros predeterminados	Restablezca el panel de filtros y muestre los filtros predeterminados.



El botón de filtrado de **Grupo de acceso** permite a los usuarios seleccionar un grupo estático y filtrar los objetos vistos según el grupo en el que se encuentran.

Puede usar etiquetas para filtrar los elementos mostrados.

Diseño del panel lateral

Haga clic en el icono junto al nombre de la sección y ajuste el diseño del panel lateral utilizando el menú contextual (las opciones disponibles pueden variar en función del diseño actual):

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

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

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

Administrar la tabla principal

Para reordenar una columna, sitúe el ratón sobre el icono situado junto al nombre de la columna y arrastre y coloque la columna. Consulte también **Modificar columnas** a continuación.

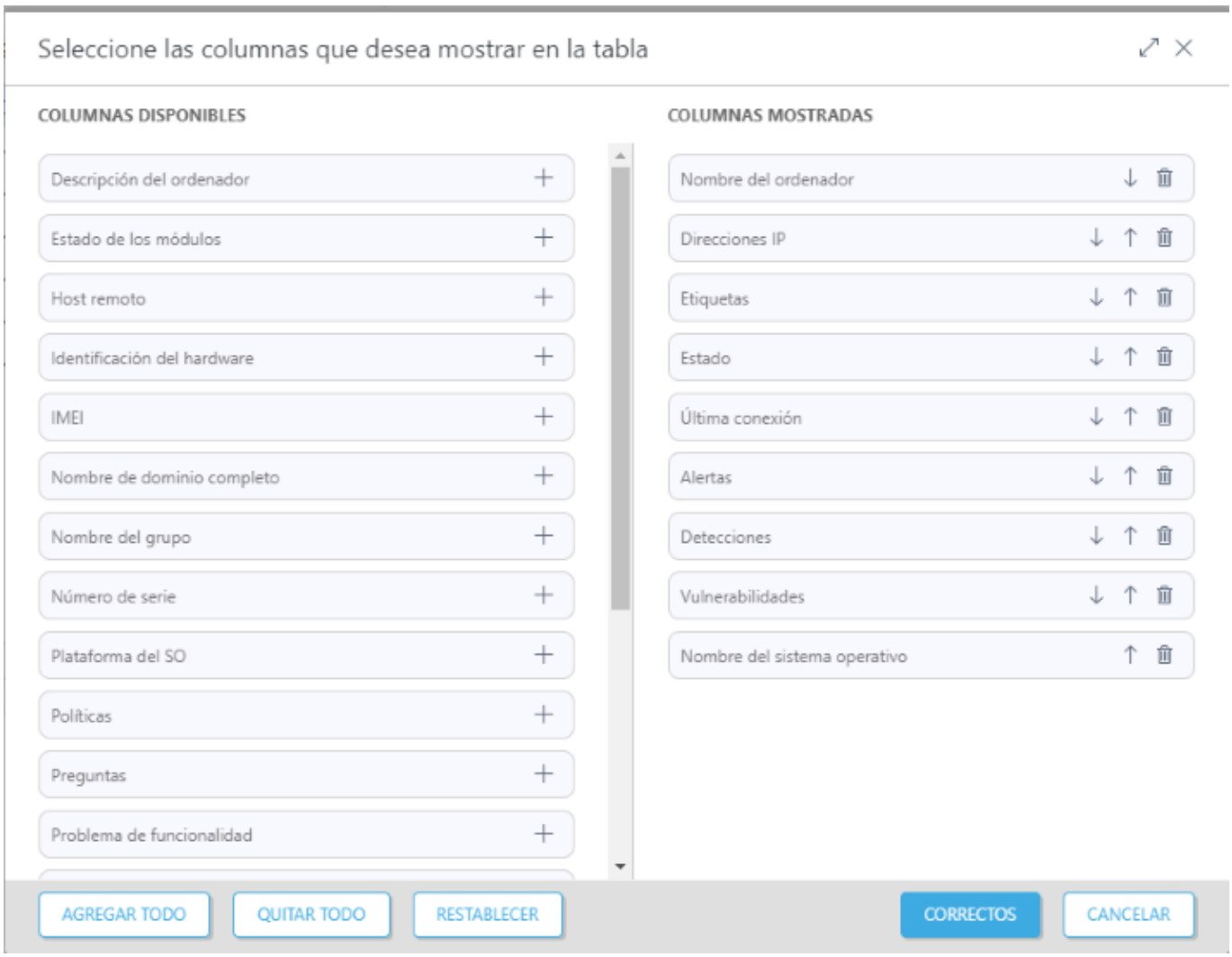
Para clasificar por una sola columna, haga clic en el encabezado de la columna para clasificar las filas de la tabla en función de los datos de la columna seleccionada.

- Si hace clic una vez, la clasificación es ascendente (A–Z, 0–9) y, si hace clic dos veces, la clasificación es descendente (Z–A, 9–0).
- Una vez aplicada la clasificación, una flecha pequeña delante del encabezado de la columna indicará el comportamiento de clasificación.
- Consulte también Clasif. múltiple a continuación.

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

Acciones

- **Modificar columnas** –Use el asistente para ajustar (agregar, quitar y reordenar) las columnas mostradas. También puede utilizar la opción de arrastrar y colocar para ajustar las columnas. Haga clic en **Restablecer** para restablecer las columnas de la tabla a su estado predeterminado (las columnas disponibles predeterminadas en orden predeterminado).



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

• **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 **Ocurrió** en **Detecciones**). Cuando active **Mostrar tiempo relativo**, sitúe el ratón sobre el tiempo relativo en la tabla para ver el tiempo absoluto.

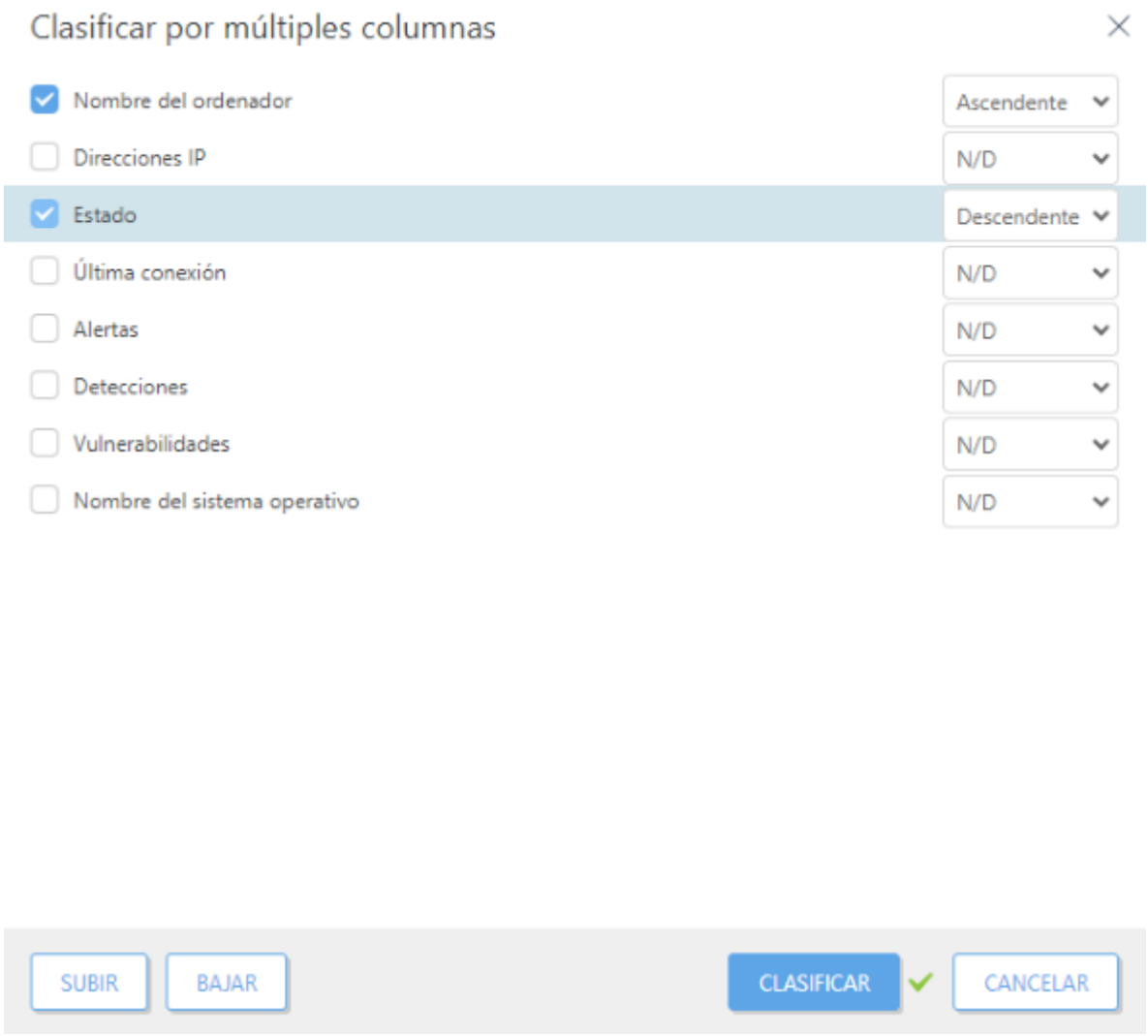
Clasificación de tablas

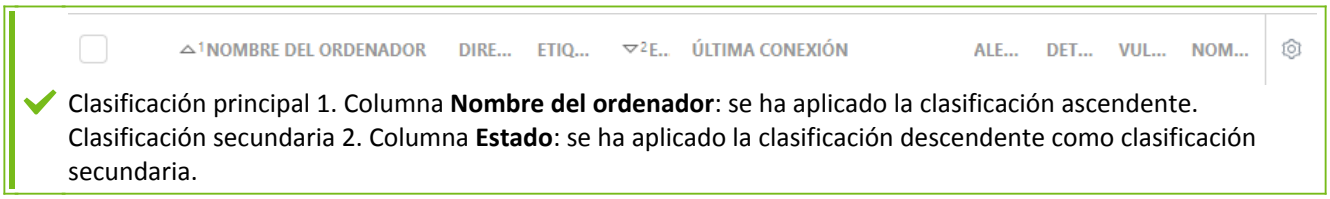
• **Restablecer clasificación**: restablece la clasificación de las columnas.

• **Clasif. múltiple**: puede clasificar los datos de la tabla seleccionando varias columnas (hasta 4). Para cada una de las columnas puede modificar su:

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

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





Clasificación principal 1. Columna **Nombre del ordenador**: se ha aplicado la clasificación ascendente. Clasificación secundaria 2. Columna **Estado**: se ha aplicado la clasificación descendente como clasificación secundaria.

Informes

- **Exportar tabla como**: exporte la tabla como informe en el formato de archivo que desee. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa ; (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe PDF para ver los valores de texto.

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

Etiquetas

ESET PROTECT On-Prem permite marcar todos los objetos pertinentes (ordenadores, detecciones, tareas, instaladores, políticas, notificaciones, licencias, etc.) con etiquetas definidas por el usuario que pueden utilizarse más tarde para mejorar el filtrado y las búsquedas. El etiquetado se integra de forma nativa en todas las pantallas

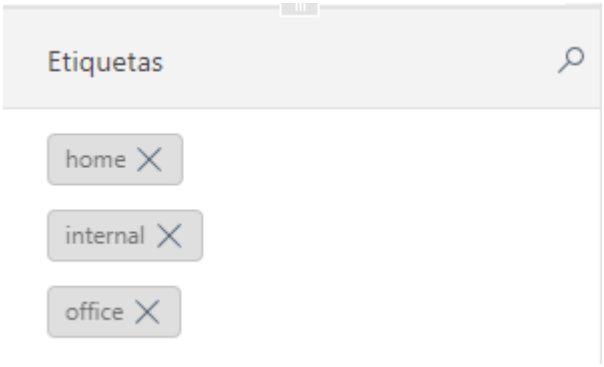
principales de ESET PROTECT Web Console.

Las etiquetas son palabras clave definidas por el usuario que puede agregar a distintos objetos para que sea más fácil agruparlos, filtrarlos y encontrarlos. Por ejemplo, puede asignar la etiqueta "VIP" a sus recursos más importantes e identificar rápidamente todos los objetos que asocian a ellos.

Puede crear y asignar etiquetas manualmente. Los objetos MSP se etiquetan automáticamente con el nombre del cliente.

Panel Etiquetas

Puede ver las etiquetas existentes en la sección **Etiquetas**, que se encuentra en el lateral inferior izquierdo de la pantalla del menú de ESET PROTECT Web Console:



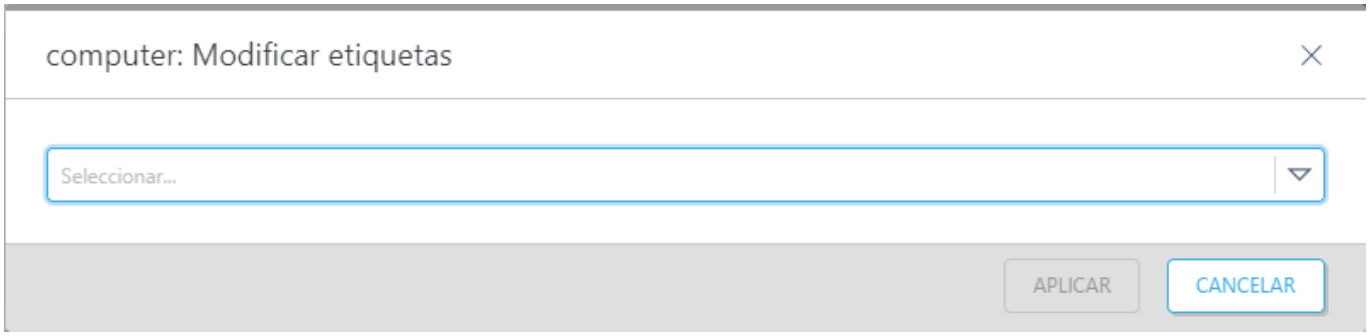
Permisos de administración de etiquetas

Para administrar etiquetas para un objeto, un usuario debe tener el derecho de acceso de **Uso** (conjunto de permisos asignado) del objeto. El resto de usuarios pueden administrar etiquetas, por ejemplo, otro usuario puede eliminar una etiqueta que haya creado usted.

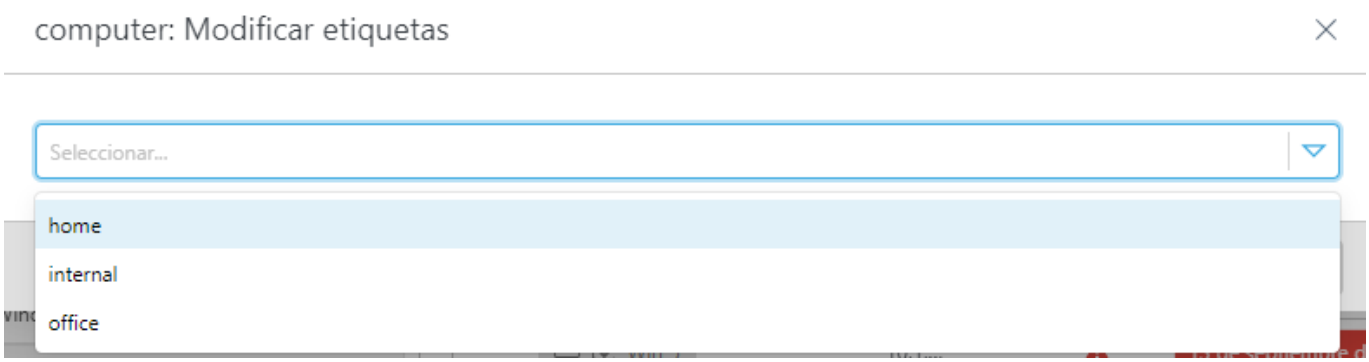
Asignar etiquetas

Puede asignar etiquetas a uno o más objetos.

Para asignar etiquetas, marque las casillas de verificación que se encuentran junto a los objetos y haga clic en **Ordenador** > **Etiquetas**:

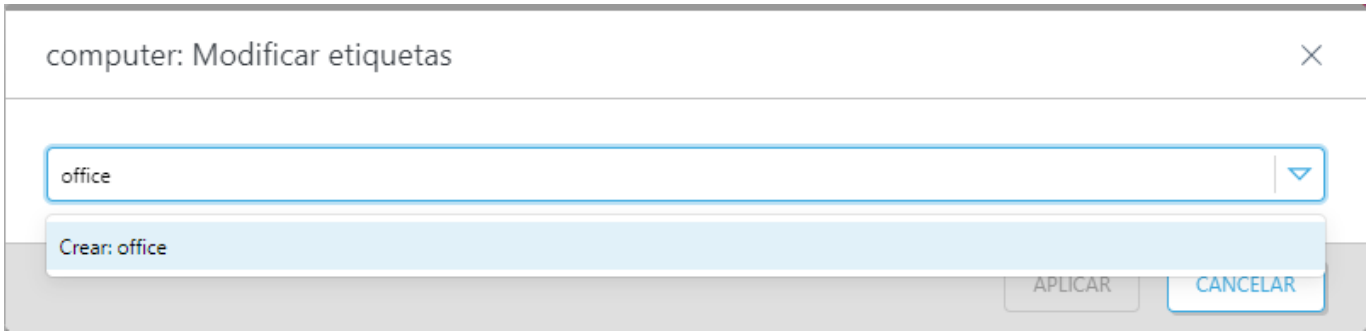


Para asignar etiquetas existentes, haga clic en el campo para escribir de una etiqueta de la lista y haga clic en **Aplicar**.



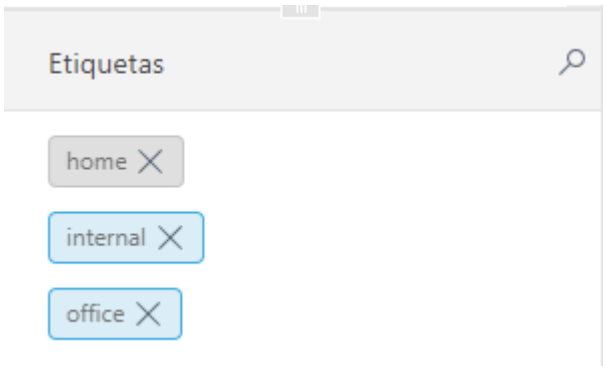
Crear una etiqueta nueva

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



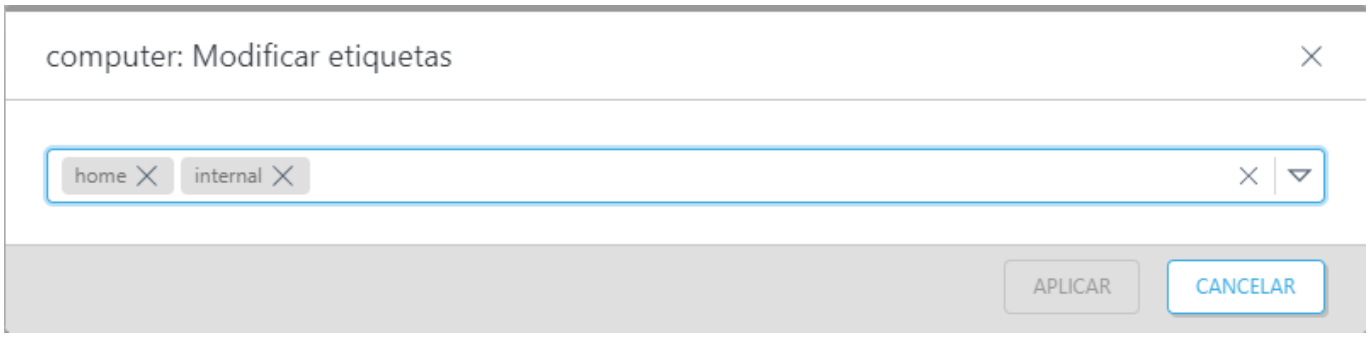
Filtrar objetos con las etiquetas

Haga clic en una etiqueta para aplicar un filtro a los objetos mostrados. Las etiquetas seleccionadas son azules.



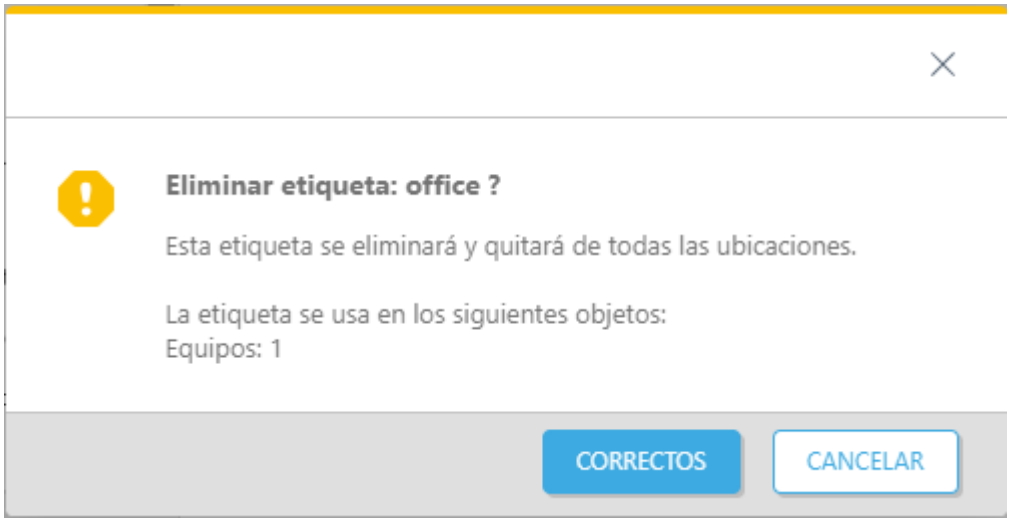
Cancelar asignación de etiquetas

Para asignar etiquetas, marque las casillas de verificación que se encuentran junto a los objetos y haga clic en **Ordenador** > **Etiquetas**: Para quitar la etiqueta, haga clic en X y en **Aplicar**.



Eliminar una etiqueta

Para eliminar una etiqueta, mueva el cursor del ratón por la etiqueta en el panel **Etiquetas**, haga clic en el icono ✕ y haga clic en el botón **Aceptar** para confirmar que desea eliminar la etiqueta de todos los objetos de ESET PROTECT Web Console.



Importar CSV

La importación de una lista se puede realizar mediante un archivo *.csv* que tenga una estructura correcta. Esta función se usa en diversos menús de la interfaz de usuario de ESET PROTECT On-Prem. Las columnas se modificarán en función de lo que haya que importar.

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

2.**Cargar**: haga clic en **Seleccionar archivo**, busque el archivo *.csv* (con codificación UTF-8) que desee cargar y, a continuación, haga clic en **Cargar**.

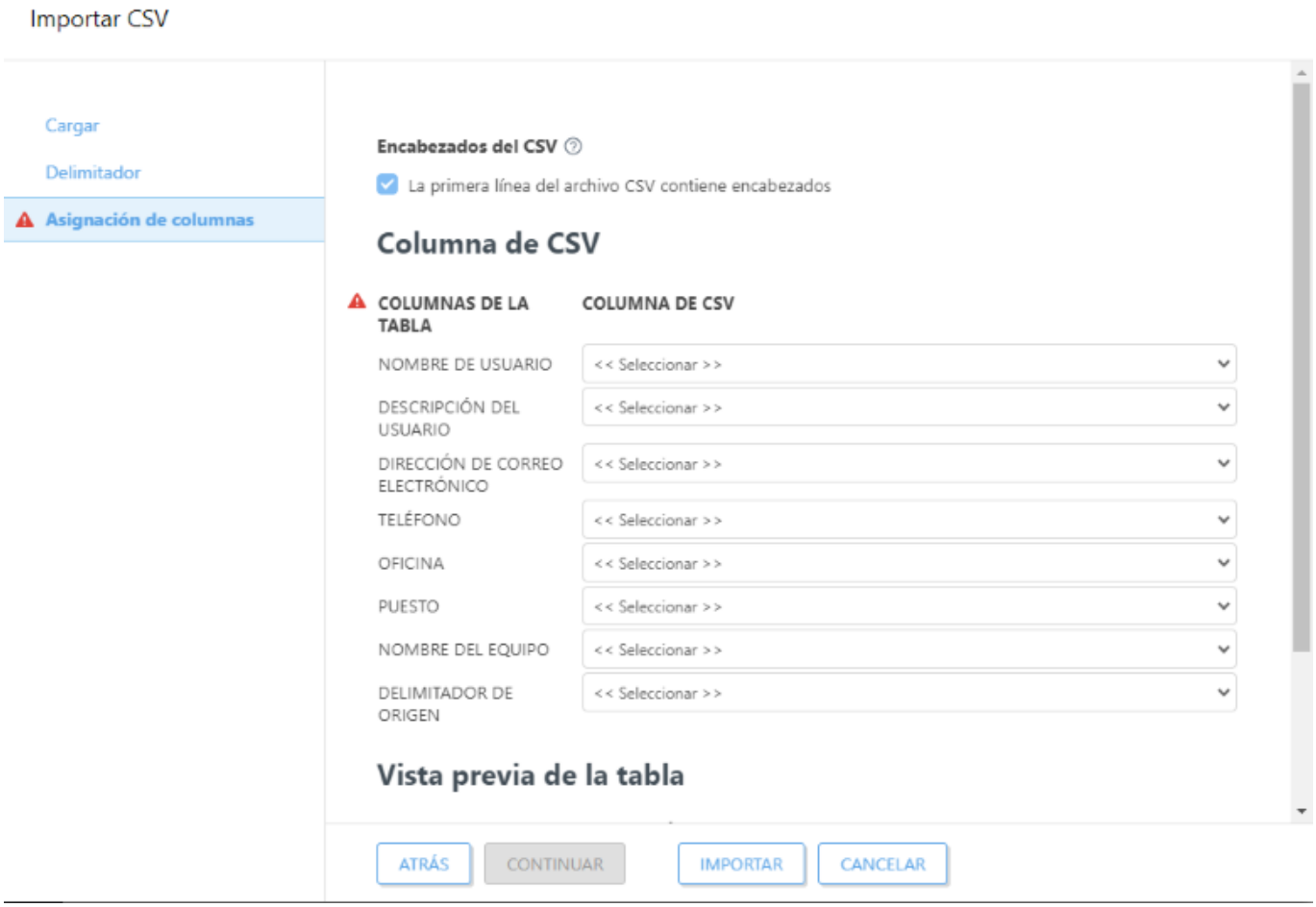
3.**Delimitador**: un delimitador es un carácter utilizado para separar cadenas de texto. Seleccione un delimitador adecuado (**Punto y coma**, **Coma**, **Espacio**, **Tabulador**, **Punto**, **Barra vertical**) en función de la opción que se utilice en el archivo *.csv*. Si en su archivo *.csv* se utilizan otros caracteres como delimitadores, marque la casilla de verificación situada junto a **Otros** e introduzca el carácter. **Vista previa de los datos**

muestra el contenido de su archivo *.csv*, lo que puede ayudarle a identificar el tipo de delimitador utilizado para separar cadenas.

4.**Asignación de columnas**: una vez cargado y analizado el archivo *.csv*, puede asignar cada una de las columnas del archivo *.csv* importado a una **columna de ESET PROTECT On-Prem mostrada en la tabla. Utilice las listas desplegables para seleccionar qué columna de CSV se debe asociar con una columna de ESET PROTECT On-Prem específica. Si su archivo *.csv* no tiene fila de encabezado**, desmarque la casilla de verificación **La primera línea del CSV contiene encabezado**.

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.Una vez asignadas correctamente todas las columnas y cuando la vista previa de la tabla parezca correcta, haga clic en **Importar** para comenzar la operación.



Solución de problemas: Web Console

En la siguiente tabla verá información sobre los mensajes y los estados de error de inicio de sesión más frecuentes en Web Console, lo que significan y algunos pasos adicionales de solución de problemas:

Mensaje de error	Posible causa
⚠ No se pudo iniciar sesión: Nombre de usuario o contraseña no válidos	Asegúrese que ingresó el nombre de usuario y la contraseña correctamente. Puede restablecer la contraseña de ESET PROTECT Web Console.

Mensaje de error	Posible causa
⚠ No se pudo iniciar sesión: La conexión ha fallado con el estado de "No conectado"	Compruebe que el servicio de ESET PROTECT Server y el servicio de su base de datos se estén ejecutando; consulte el artículo de nuestra base de conocimiento si desea ver las instrucciones paso a paso.
⚠ No se pudo iniciar sesión: el usuario estaba bloqueado. Inténtelo de nuevo más tarde.	Después de 10 intentos de inicio de sesión sin éxito desde la misma dirección IP (por ejemplo, si se utilizan credenciales de inicio de sesión incorrectas), se bloquearán temporalmente los intentos adicionales de inicio de sesión desde esta dirección IP. Una vez transcurridos 10 minutos, inicie sesión con las credenciales correctas.
⚠ No se pudo iniciar sesión: Error de comunicación	Compruebe que el servicio de ESET PROTECT Server esté en ejecución y que el servicio de Apache Tomcat esté en ejecución y funcionando correctamente. Consulte los archivos de registro de Apache Tomcat. Consulte nuestro artículo de la base de conocimiento para obtener más información sobre este problema.
⚠ No se pudo iniciar sesión: Tiempo de espera de la conexión agotado	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. También puede ser que ESET PROTECT Server esté sobrecargado, intente reiniciarlo. Este problema también puede darse si utiliza versiones distintas de ESET PROTECT Web Console y ESET PROTECT Server.
⚠ No se pudo iniciar sesión: El usuario no tiene ningún derecho de acceso asignado	El usuario no tiene ningún derecho de acceso asignado. Inicie sesión como administrador y modifique la cuenta del usuario para que tenga al menos un conjunto de permisos asignado.
⚠ No se pudo iniciar sesión: Error de análisis de respuesta	Las versiones de la Consola web y de ESET PROTECT Server no son compatibles. Esto puede ocurrir durante una actualización de componentes o después de ella. Si el problema persiste, implemente la versión correcta de Web Console manualmente.
⚠ Se está usando una conexión no cifrada. Configure el servidor web para que use HTTPS.	Por motivos de seguridad, se recomienda configurar ESET PROTECT Web Console para utilizar HTTPS.
JavaScript está desactivado. Active JavaScript en su navegador.	Active JavaScript o actualice su navegador web.
SEC_ERROR_INADEQUATE_KEY_USAGE (solo Mozilla Firefox).	Mozilla Firefox tiene un almacén de certificados dañado.

Error	Posible causa
No ve la pantalla de inicio de sesión o parece estar cargándose continuamente.	• Reinicie el servicio ESET PROTECT On-PremServer. Cuando el servicio de ESET PROTECT On-Prem Server vuelva a estar activo, reinicie el servicio de Apache Tomcat. Después de esto, la pantalla de inicio de sesión de ESET PROTECT Web Console se cargará correctamente. Lea también el artículo de la base de conocimiento. • Si Apache Tomcat no puede extraer contenido del archivo *era.war* y no puede acceder a Web Console, siga los pasos del artículo de la base de conocimiento.
El texto no está en el menú contextual ni en el menú **Vínculos rápidos** de la Consola web de ESET PROTECT.	Este problema puede deberse a una extensión del navegador que bloquee los anuncios. Para resolver este problema, desactive la extensión del navegador que bloquea los anuncios para la página de la Consola web de ESET PROTECT.

Error	Posible causa
Tras iniciar sesión, Web Console no se muestra correctamente (faltan elementos, etc.).	Asegúrese de estar usando un navegador web compatible.

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

Web Console tarda mucho tiempo en cargarse. Cuando se cargan muchos objetos, la consola se bloquea.	Web Console necesita más memoria para administrar conjuntos de objetos de gran tamaño. Consulte Web Console para ver la configuración empresarial.
Algunas pantallas de Web Console no se cargan correctamente y se muestra un error. Por ejemplo, al editar una política, se muestra el error "ERROR WHILE INITIALIZING CONFIGURATION EDITOR.: (TYPEERROR) : ((INTERMEDIATE VALUE)(INTERMEDIATE VALUE) , K).INITCONFIGEDITOR IS NOT A FUNCTION"	Este problema surge si está utilizando un proxy inverso que impide la carga de algunos módulos de Web Console. Las cadenas de URL de algunos módulos de Web Console (cargados en Apache Tomcat) pueden cambiar de forma dinámica (por ejemplo, la cadena que se encuentra después 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.
Cuando se importa un archivo de gran tamaño (más de 20 MB) (por ejemplo, una política), el proceso falla.	El límite de tamaño de archivo para Web Console es de 20 MB. Puede cambiarlo editando el archivo *EraWebServerConfig.properties*, que se encuentra en la carpeta *[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config*. Cambie `file_size_limit=20` a un valor superior; el valor máximo es 250.

- Después de actualizar ESET PROTECT On-Prem, le recomendamos eliminar la memoria caché y las cookies del navegador web antes de iniciar sesión en la nueva Web Console.
- dado que Web Console utiliza el protocolo seguro (HTTPS), es posible que obtenga un mensaje en su navegador web en relación con un certificado de seguridad o que la conexión no es de confianza (el texto exacto del mensaje depende del navegador que esté utilizando). Esto se debe a que su navegador desea que verifique la identidad del sitio al que está intentando tener acceso. Haga clic en **Opciones avanzadas** > **Continuar a [dirección] (no es seguro)** (Chrome/Edge) o en **Opciones avanzadas** > **Aceptar el riesgo y continuar** (Firefox) para permitir el acceso a ESET PROTECT Web Console. Esto solo se aplica cuando está tratando de acceder a la URL de la Consola web de ESET PROTECT. Para obtener más información sobre la configuración de la conexión HTTPS/SSL, lea el artículo de nuestra base de conocimiento.

Cómo administrar productos Endpoint desde ESET PROTECT On-Prem

Antes de comenzar a administrar las soluciones empresariales de ESET, debe realizar la configuración inicial. Le recomendamos que utilice Resumen de estado, sobre todo si ha omitido el ESET PROTECT On-PremAsistente de inicio. El administrador puede realizar distintas tareas desde ESET PROTECT Web Console para instalar productos

y controlar los ordenadores cliente.

Instalación de ESET Management Agent y productos de seguridad Endpoint

ESET PROTECT On-Prem requiere que ESET Management Agent esté instalado en todos los ordenadores cliente administrados. ESET Management Agent puede instalarse en combinación con su producto de seguridad Endpoint. Antes de la instalación, le recomendamos que importe su licencia en ESET PROTECT On-Prem para poder utilizarla en futuras instalaciones. Existen varios métodos para instalar su producto Endpoint:

- Utilizar el instalador de Agent y el producto de seguridad de ESET o la ESET Remote Deployment Tool para instalar su producto Endpoint y ESET Management Agent al mismo tiempo.
- Haga clic en un ordenador y seleccione **Soluciones** > **Implementar producto de seguridad** para implementar un producto de seguridad ESET en el ordenador.
- Instalar su producto ESET Endpoint en clientes en los que ya haya instalado ESET Management Agent utilizando una tarea del cliente.

Administración del producto de seguridad Endpoint desde ESET PROTECT On-Prem

Todos los productos de seguridad Endpoint pueden administrarse desde ESET PROTECT Web Console. Se utilizan políticas para aplicar la configuración a ordenadores independientes o a grupos de ordenadores. Por ejemplo, puede crear una política para bloquear el acceso a ciertas ubicaciones web, cambiar la sensibilidad de la detección de las configuraciones del explorador o cambiar todas las demás configuraciones de seguridad de ESET. Las políticas pueden fusionarse, como se muestra en nuestro ejemplo. El usuario no puede sobrescribir en los ordenadores cliente las políticas configuradas mediante ESET PROTECT On-Prem. No obstante, el administrador puede utilizar la función anular para permitir que un usuario realice cambios en un cliente temporalmente. Cuando termine de realizar cambios, puede solicitar la configuración final al cliente y guardarla como nueva política.

Para administrar clientes también pueden utilizarse las tareas. Las tareas se implementan desde Web Console y ESET Management Agent las ejecuta en el cliente. Las tareas del cliente más comunes para productos Windows Endpoint son las siguientes:

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

Actualizar productos de seguridad de ESET

1. Haga clic en **Panel** > **Resumen del estado** > Estado de la versión del componente.

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

Generación de informes sobre el estado del ordenador y recepción de información de los clientes en ESET PROTECT On-Prem

Todos los ordenadores cliente se conectan a ESET PROTECT On-Prem a través de ESET Management Agent. El agente comunica toda la información solicitada sobre el ordenador cliente y su software a ESET PROTECT Server. La conexión entre el agente y el servidor se realiza de forma predeterminada cada 1 minuto, pero puede cambiarse en la política de ESET Management Agent. Todos los registros de los productos Endpoint u otros productos de seguridad de ESET se envían a ESET PROTECT Server.

Puede encontrar información sobre los productos de ESET instalados y otra información básica sobre el sistema operativo y el estado de los clientes en **Ordenadores**. Seleccione un cliente y haga clic en **Detalles**. En la sección **Configuración** de esta ventana, el usuario puede buscar configuraciones anteriores o solicitar la configuración actual. En la sección **SysInspector** el usuario puede solicitar registros (solo de ordenadores Windows).

Web Console también le permite acceder a una lista de todas las detecciones de los dispositivos cliente. Las detecciones de un solo dispositivo pueden verse en **Ordenadores**. Seleccione un cliente y haga clic en **Detalles** > **Detecciones y cuarentena**. Si el ordenador cliente ejecuta ESET Inspect On-Prem, puede ver y administrar las detecciones de ESET Inspect.

Puede generar informes personalizados a petición o utilizar una tarea planificada para ver datos sobre los clientes de su red. Las plantillas de informes predefinidas son una forma rápida de recopilar datos importantes, pero también puede crear sus propias nuevas plantillas. Entre los ejemplos de informes se incluye la información agregada sobre ordenadores, detecciones, cuarentenas y actualizaciones necesarias.

> El usuario solo puede utilizar las plantillas de informes en las que tenga permisos suficientes. De forma predeterminada, todas las plantillas se almacenan en el grupo **Todo**. Los informes solo pueden incluir información sobre ordenadores y eventos que estén dentro del ámbito de los permisos del usuario que crea dichos informes. Aunque una plantilla de informe se comparta entre más usuarios, el informe de cada usuario solo contendrá información acerca de los dispositivos sobre los que tenga permiso dicho usuario. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

ESET Push Notification Service

ESET Push Notification Service (EPNS) sirve para recibir mensajes de ESET PROTECT Server si el servidor tiene una notificación para el cliente. La conexión está establecida de modo que ESET PROTECT On-Prem pueda enviar una notificación (push) a un cliente inmediatamente. Cuando la conexión se interrumpe, el cliente intenta volver a conectarse. El objetivo principal de la conexión permanente es que los clientes estén disponibles para recibir mensajes.

Un usuario de Web Console puede enviar llamadas de activación desde EPNS entre ESET PROTECT Server y las instancias de ESET Management Agent. ESET PROTECT Server envía llamadas **Wake on LAN**. Puede configurar direcciones de multidifusión para **Wake On Lan** en **Más** > Configuración.

Detalles de conexión

Para configurar su red local de modo que permita la comunicación con EPNS, tanto ESET Management Agent como ESET PROTECT Server deben ser capaces de conectarse al servidor de EPNS. Si no puede establecer la conexión con EPNS para sus agentes, solo se verán afectadas las llamadas de activación. Asegúrese de que su cortafuegos permita la conexión con el servidor EPNS (consulte la tabla siguiente).

Protocolo de seguridad criptográfico	TLS: la versión más reciente de TLS compatible con el sistema operativo del ordenador administrado.
Protocolo	MQTT (protocolo de conectividad entre equipos)
Puerto	• principal: 8883 • conmutación por error: 443 y el puerto de proxy establecido por la política de ESET Management Agent El puerto 8883 es el preferido, ya que es un puerto MQTT. El 443 solo es un puerto de reserva, y se comparte con otros servicios. Además, un cortafuegos podría anular la conexión en el puerto 443 por inactividad o porque se supere el límite de conexiones abiertas para el servidor proxy HTTP.
Dirección del host	*epns.eset.com*
Compatibilidad del proxy	Si usa el proxy HTTP para reenviar la comunicación, las llamadas de activación 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. Si el proxy HTTP no funciona, las llamadas de activación se envían directamente.

Resolución 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`).

VDI, clonación y detección de hardware

ESET PROTECT On-Prem es compatible con entornos VDI, clonación de equipos y sistemas de almacenamiento no persistente. Esta característica es necesaria para configurar un indicador para el ordenador principal o resolver una pregunta que aparezca después de la clonación o de un cambio de hardware.

- Hasta que se resuelva la pregunta, el equipo cliente no podrá replicar al ESET PROTECT Server. El cliente solo comprueba si la pregunta está resuelta.

- La desactivación de la detección de hardware es irreversible; utilícela con la máxima precaución y solo en equipos físicos.

- Cuando resuelva varias preguntas, utilice la ventana dinámica Resumen del estado - **Preguntas**.

¿Qué sistemas operativos e hipervisores son compatibles?

⚠ Antes de empezar a usar una infraestructura de escritorios virtuales (VDI) con ESET PROTECT On-Prem, lea más información sobre las funciones compatibles y no compatibles de diversos entornos de infraestructura de escritorios virtuales en el 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 no se puede clonar ESET Full Disk Encryption.

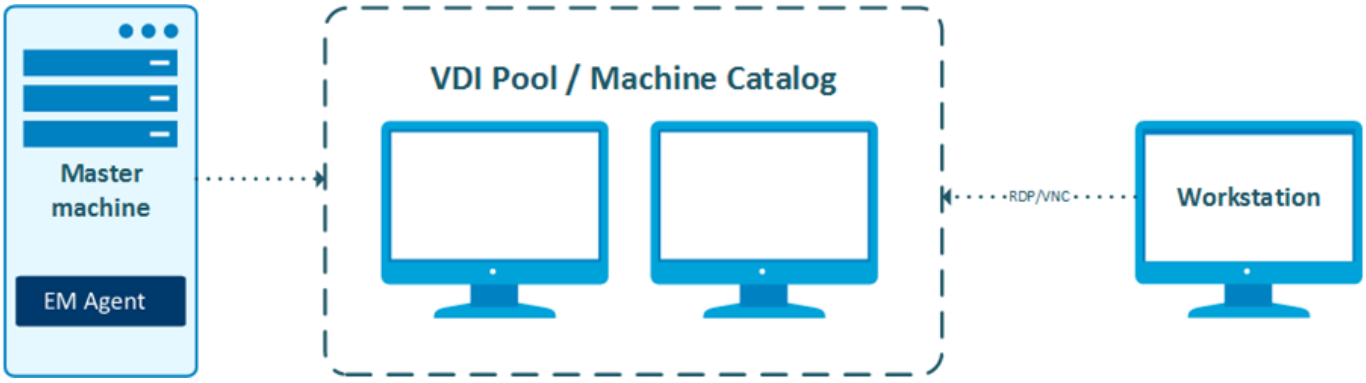
- Los dispositivos móviles administrados a través de MDM no son compatibles.
- Los clones vinculados en Virtual Box no se distinguen unos de otros.
- En casos muy raros, la detección puede ser desactivada automáticamente por el ESET PROTECT On-Prem; esto sucede cuando ESET PROTECT On-Prem no es capaz de analizar el hardware de forma fiable
- Consulte la lista de configuraciones compatibles:
  - Citrix PVS 7.15+ con equipos físicos
  - 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 equipos Citrix
  - (sin PVS) Citrix XenDesktop con Citrix XenServer 7.15+
  - VMware Horizon 8.0+ con VMware ESXi
  - Microsoft SCCM (para volver a crear la imagen)
- ESET PROTECT On-Prem es compatible con patrones de asignación de nombres de VDI para todos los hipervisores compatibles.

entornos VDI

Puede utilizar el equipo principal con ESET Management Agent para un grupo VDI. No es necesario un conector VDI; toda la comunicación se realiza a través de ESET Management Agent. ESET Management Agent debe instalarse en el equipo principal antes de configurar el grupo VDI (catálogo del equipo).

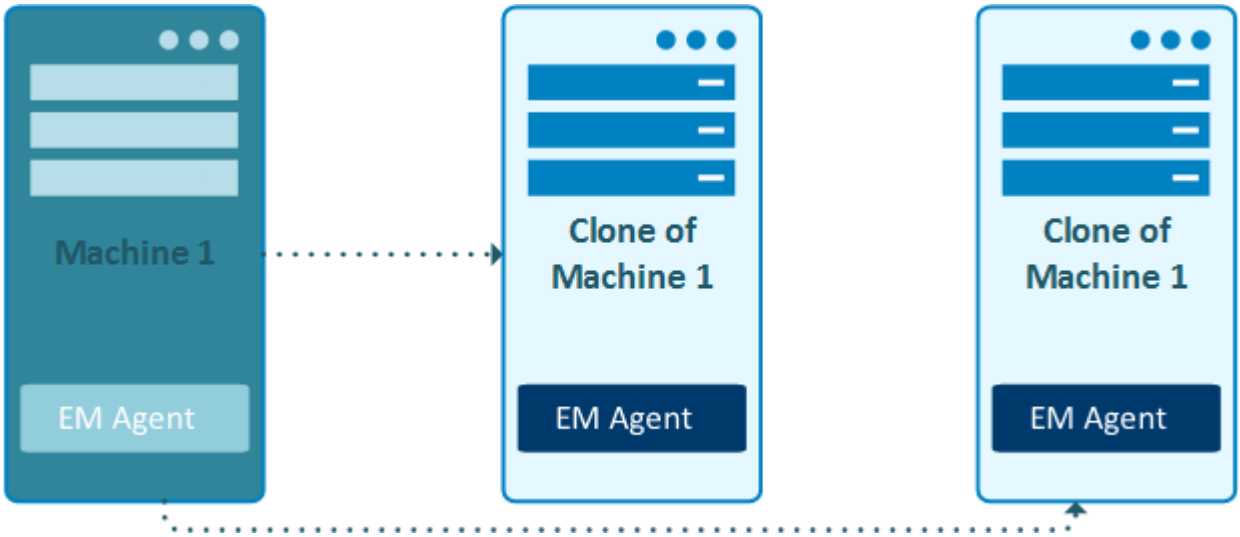
- Si quiere crear un grupo VDI, marque el equipo principal en Detalles del ordenador > **Virtualización** antes de crear el grupo y, a continuación, seleccione **Marcar como maestro para clonación** > **Coincidencia con el equipo existente)**.
- Si el equipo principal se elimina de ESET PROTECT On-Prem, está prohibida 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 un equipo del grupo VDI se conecta por primera vez, tiene un intervalo de conexión obligatorio de 1 minuto. Tras las primeras replicaciones, el intervalo de conexión se hereda del equipo principal.
- Nunca desactive la detección de hardware al utilizar el grupo VDI
- Puede tener el equipo principal funcionando junto con los ordenadores clonados para mantenerlo actualizado.

Grupo predeterminado para máquinas de infraestructura de escritorios virtuales
Los nuevos equipos clonados a partir del maestro aparecen en el grupo estático establecido en el **Grupo de inicio de ordenadores clonados** en la ventana Maestro para clonación.



Clonación de equipos en el hipervisor

Puede crear un clon de un equipo normal. Solo tiene que esperar a que aparezca la Pregunta y resolverla seleccionando **Crear nuevo ordenador solo esta vez**.



Imágenes de sistemas para equipos físicos

Puede utilizar una imagen principal con ESET Management Agent instalado e implementarla en ordenadores físicos. Existen dos formas de hacerlo:

Crear un nuevo ordenador

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:

- Manualmente: resuelva cada nuevo ordenador manualmente en Preguntas y seleccione **Crear un ordenador nuevo cada vez**.
- Automáticamente: marque el equipo maestro antes de la clonación y seleccione **Marcar como maestro para clonación** > **Crear nuevos ordenadores**.

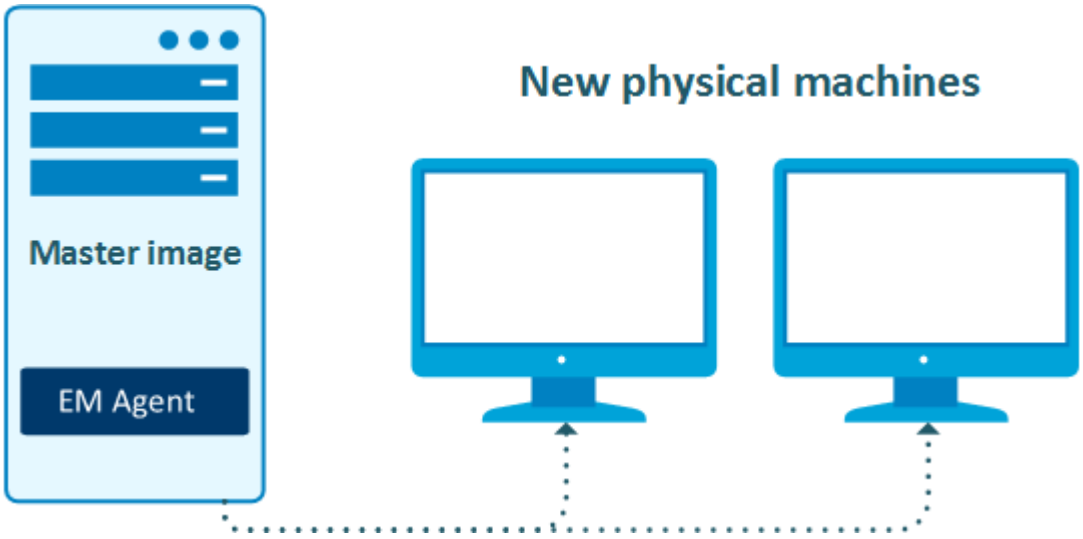
Relacionar con ordenador existente

Si la imagen vuelve a implementarse en un equipo con historial previo en ESET PROTECT On-Prem (que ya tenía ESET Management Agent implementado), este equipo se conecta con su identidad anterior en ESET PROTECT On-Prem. Si no hay ninguna identidad anterior relacionada, el sistema crea un nuevo equipo en ESET PROTECT On-Prem después de que la imagen se implemente en un nuevo equipo.

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

- Manualmente: resuelva cada nuevo ordenador manualmente en Preguntas y seleccione **Relacionar con un ordenador existente cada vez**.
- Automáticamente: marque el equipo maestro antes de la clonación y seleccione **Marcar como maestro para clonación** > **Relacionar con ordenadores existentes**.

⚠ Si tiene una imagen (o una plantilla) de su ordenador maestro, debe mantenerla actualizada. Actualice siempre la imagen después de actualizar o volver a instalar cualquier componente ESET en el equipo principal.



Replicación paralela

ESET PROTECT Server puede reconocer y resolver la replicación paralela de varios equipos con una sola identidad en ESET PROTECT On-Prem. Este evento se comunica a Detalles del ordenador > **Alertas** ("**Varias conexiones con ID de agente idéntico**"). Existen dos formas de resolver este problema:

- Utilice la acción con un clic disponible en la alerta: los ordenadores se dividen y su detección de hardware se desactiva de forma permanente.
- En raras ocasiones, incluso los equipos con la detección de hardware desactivada 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: esto evitará que tenga que desactivar la detección de hardware.

Resolución de problemas

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

Resolución de preguntas de clonación

Cada vez que un equipo se conecta con ESET PROTECT On-Prem, se crea una entrada basada en dos huellas dactilares:

- Un UUID (identificador único universal) de ESET Management Agent: cambia cuando se vuelve a instalar ESET Management Agent en un equipo (consulte Cuando hay dos agentes).
- Una huella dactilar de hardware del equipo: cambia si el equipo se clona o se vuelve a implementar.

Aparece una pregunta si ESET PROTECT Server detecta algo de lo siguiente:

- un dispositivo clonado conectándose
- un cambio de hardware en un dispositivo existente con ESET Management Agent instalado

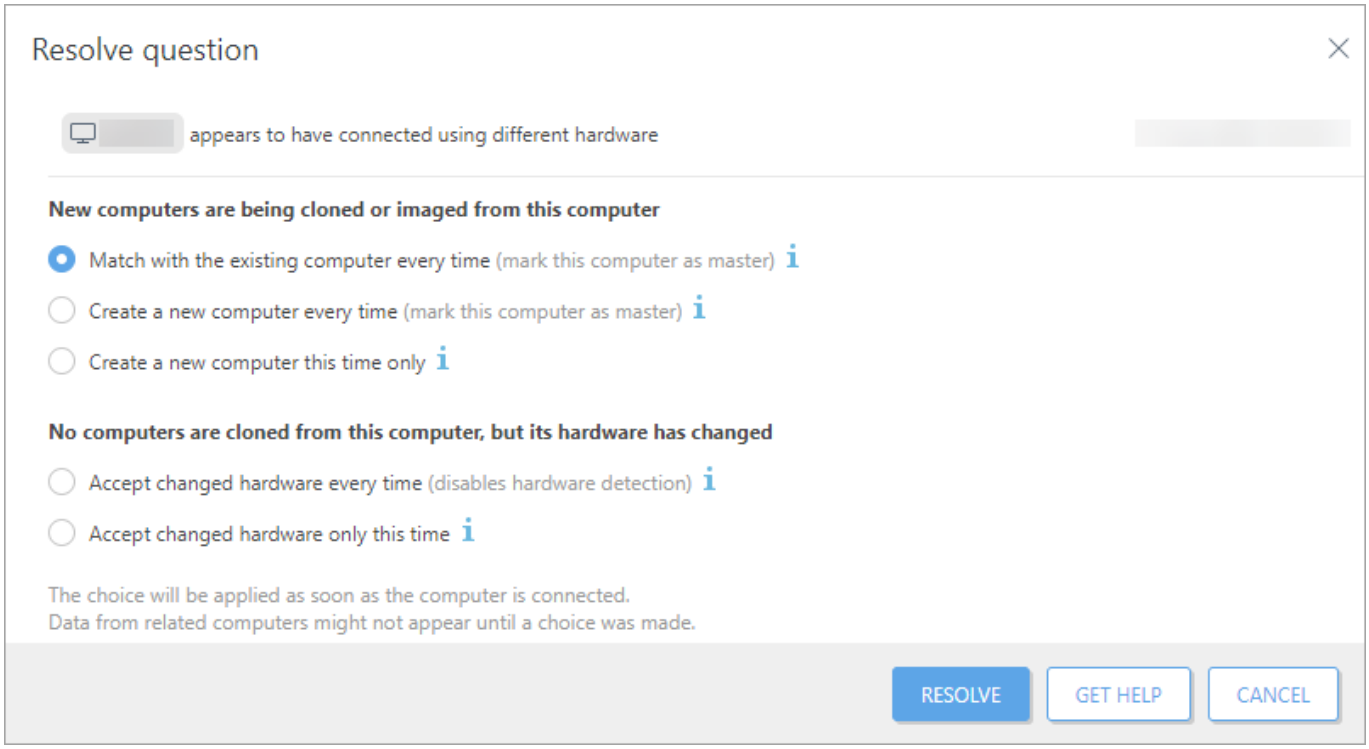
La detección de huella digital de hardware no es compatible con:
- Linux, macOS, Android, iOS
- equipos sin ESET Management Agent

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

Se están clonando nuevos ordenadores o se están obteniendo imágenes de nuevos ordenadores desde este ordenador	Acción	Más detalles
Coincidencia con el equipo existente cada vez	Seleccione esta opción cuando: • Utilice el ordenador como equipo principal y todas sus imágenes deban conectarse con la entrada del ordenador existente en ESET PROTECT On-Prem. • Utilice el ordenador como equipo principal para configurar un entorno VDI y el ordenador esté en el grupo VDI y se espere que recupere su identidad basándose en un identificador de huella digital de hardware.	Artículo de la base de conocimiento
Crear un ordenador nuevo cada vez	Seleccione esta opción cuando utilice este ordenador como imagen principal y quiera que ESET PROTECT On-Prem reconozca automáticamente todos los clones de este ordenador como nuevos ordenadores. No la utilice con entornos VDI.	Artículo de la base de conocimiento
Crear un ordenador nuevo solo esta vez	El ordenador se clona solo una vez. Seleccione esta opción para crear una nueva instancia para el dispositivo clonado.	Artículo de la base de conocimiento

No se han clonado ordenadores desde este ordenador, pero su hardware ha cambiado	Acción
Aceptar hardware cambiado cada vez	Desactive la detección de hardware para este dispositivo de forma permanente. Utilice esta opción solo si se comunican cambios de hardware no existentes. **Esta acción es irreversible.** Si desactiva la detección de hardware, tanto el agente como el servidor almacenan esta configuración. Volver a implementar el agente no restaura la detección de hardware desactivada. Las máquinas con detección de hardware desactivada no son adecuadas para los escenarios de infraestructuras de escritorios virtuales de ESET PROTECT On-Prem.
Aceptar hardware cambiado solo esta vez	Seleccione esta opción para renovar la huella digital de hardware del dispositivo. Utilice esta opción después de que cambie el hardware del ordenador cliente. Las futuras modificaciones del hardware se comunicarán de nuevo.

Haga clic en **Resolver** para enviar la opción seleccionada. La pregunta de clonación se resuelve la próxima vez que el equipo clonado se conecta 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.

Cuando hay dos agentes

Si se desinstala ESET Management Agent (pero el ordenador no se quita de la Consola web) del equipo cliente y se vuelve a instalar, habrá dos ordenadores iguales en la Consola web. Uno se conecta al ESET PROTECT On-Prem y el otro, no. La ventana de diálogo **Preguntas** no controla esta situación. Esta situación es resultado de un procedimiento de eliminación incorrecto del agente. La única solución es quitar manualmente de Web Console el ordenador que no se conecta. Después de eso, el historial y los registros creados antes de que se repitiera la

instalación se perderán.

Uso de la tarea Eliminar ordenadores que no se conecten

Si tiene un grupo de VDI de ordenadores y no ha resuelto la pregunta (ver más arriba) correctamente, la Consola web crea una nueva instancia de ordenador tras cargar de nuevo el ordenador desde el grupo. Las instancias de ordenador se apilan en la Consola web y pueden sobreutilizarse las licencias. No recomendamos resolver esta situación mediante la configuración de una tarea para eliminar los ordenadores que no se conectan. Este procedimiento quita el historial (los registros) de los ordenadores eliminados, y las licencias también se pueden sobreutilizar.

Licencias sobreutilizadas

Cuando se clona un ordenador cliente con ESET Management Agent instalado y un producto de seguridad de ESET activado, cada equipo clonado puede reclamar otro puesto de licencia. Este proceso puede sobreutilizar sus licencias. En entornos VDI, utilice un archivo de licencia sin conexión para activar los productos de ESET y póngase en contacto con ESET para modificar la licencia.

Notificaciones para ordenadores clonados

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

- **Nuevo ordenador inscrito**: notifique si un ordenador se conecta 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 una máquina maestra u otro origen conocido
- **Posible clonación de ordenador detectada**: notifique una modificación importante del hardware o una clonación si el equipo de origen no se marcó antes como equipo principal.

Resolución de problemas

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

Identificación de hardware

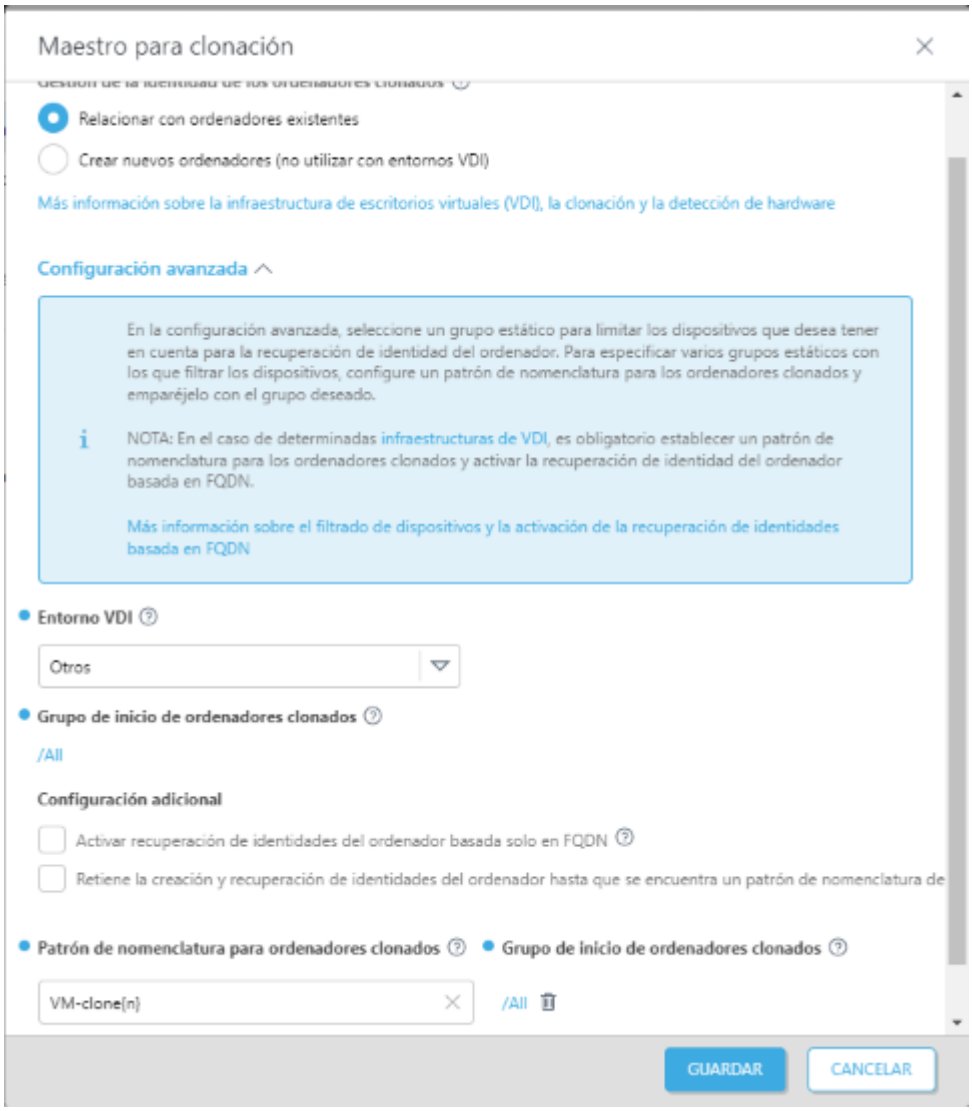
ESET PROTECT On-Prem recopila detalles sobre el hardware de cada dispositivo administrado e intenta identificarlo. Cada dispositivo conectado a ESET PROTECT On-Prem pertenece a una de las categorías que se indican a continuación, mostradas en la columna **Identificación de hardware**, en la ventana **Ordenadores**.

- **Detección de hardware activada**: la detección está activada y funciona correctamente.
- **Detección de hardware desactivada**: el usuario desactivó la detección o ESET PROTECT On-Prem desactivó la detección automáticamente.
- **Sin información del hardware**: no se dispone de información del hardware. El dispositivo cliente está ejecutando un sistema operativo incompatible o una versión antigua del agenteESET Management .

- **Detección de hardware poco fiable**: el usuario ha comunicado que la detección es poco fiable y se va a desactivar. Esto solo puede suceder durante el intervalo de replicación antes de la desactivación de la detección.

Maestro para clonación

Al hacer clic en **Virtualización** > **Marcar como maestro para clonación** en los detalles del ordenador, se muestra la siguiente notificación:



Seleccionar una de las opciones de **Gestión de la identidad de los ordenadores clonados** antes de crear el grupo de VDI:

- **Coincidencia con los equipos existente**: consulte la opción Coincidencia con los equipos existente cada vez.

- **Crear nuevos ordenadores**: consulte la opción Crear un ordenador nuevo cada vez.

Para buscar los ordenadores marcados como Maestro para clonación, vaya a **Ordenadores** > haga clic en **Agregar filtro** > seleccione **Maestro para clonación** > marque la casilla de verificación situada junto al filtro **Maestro para clonación**.
Puede cambiar la configuración de **Maestro para clonación** más adelante en los detalles del ordenador:
- Haga clic en el icono del engranaje de la ventana dinámica **Virtualización** para ajustar la configuración.
- Para quitar la configuración, haga clic en **Virtualización** > **Desmarcar como maestro para clonación**.

Configuración avanzada

1. **Entorno VDI** – 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 inicio de ordenadores clonados**: seleccione un grupo estático para limitar los dispositivos que desea tener en cuenta para la recuperación de identidades del ordenador. El grupo estático seleccionado también sirve como destino de las máquinas virtuales recién creadas.

3. **Configuración adicional**:

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

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

En función del entorno de VDI seleccionado, los ajustes recomendados están preseleccionados (pueden ser obligatorios o no estar disponibles).

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

Patrón de asignación de nombres de VDI

ESET PROTECT On-Prem solo reconoce clones con nombres que coincidan con el patrón de asignación de nombres establecido en el entorno de VDI:

- **VMware**: el patrón de asignación de nombres de VDI es obligatorio para clones instantáneos de VMware. El patrón de asignación de nombres de VDI debe tener un marcador de posición especificado para un número exclusivo `{n}` generado por la infraestructura de VDI; por ejemplo, `VM-instant-clone-{n}`. Consulte la documentación de VMware para obtener más información sobre los patrones de asignación de nombres.
- **Citrix XenCenter/XenServer:** utilice el hash `#` en el esquema de asignación de nombres del catálogo del equipo; por ejemplo, `VM-office-##`. Consulte la documentación de Citrix para obtener más información sobre el esquema de asignación de nombres.

5. Haga clic en **Seleccionar** y seleccione **Grupo de inicio de ordenadores clonados**: seleccione el grupo estático asociado como grupo de inicio de los dispositivos que coincidan con el patrón de asignación de nombres de VDI.

6. Haga clic en **Agregar nuevo** para agregar más patrones de asignación de nombres de VDI y grupos de inicio.

7. Haga clic en **Guardar**.

Para buscar los ordenadores marcados como Maestro para clonación, vaya a **Ordenadores** > haga clic en **Agregar filtro** > seleccione **Maestro para clonación** > marque la casilla de verificación situada junto al filtro **Maestro para clonación**.
Puede cambiar la configuración de **Maestro para clonación** más adelante en los detalles del ordenador:

- Haga clic en el icono del engranaje de la ventana dinámica **Virtualización** para ajustar la configuración.
- Para quitar la configuración, haga clic en **Virtualización** > **Desmarcar como maestro para clonación**.

Resolución de problemas

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

ESET Management Implementación de agente

Esta sección describe todos los métodos que puede utilizar para implementar ESET Management Agent en los ordenadores cliente de su red. Es muy importante, porque las soluciones de seguridad de ESET que se ejecutan en ordenadores cliente se comunican con ESET PROTECT Server exclusivamente a través del agente.

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

Antes de poder comenzar a administrar ordenadores clientes en su red, debe agregarlos a ESET PROTECT On-Prem. Utilice uno de los siguientes métodos para agregarlos:

- Sincronizar con Active Directory
- RD Sensor
- Agregar nuevos dispositivos manualmente

ESET Management Implementación de agente

La implementación de ESET Management Agent se puede realizar de varias maneras. Puede implementar el agente de forma local o remota:

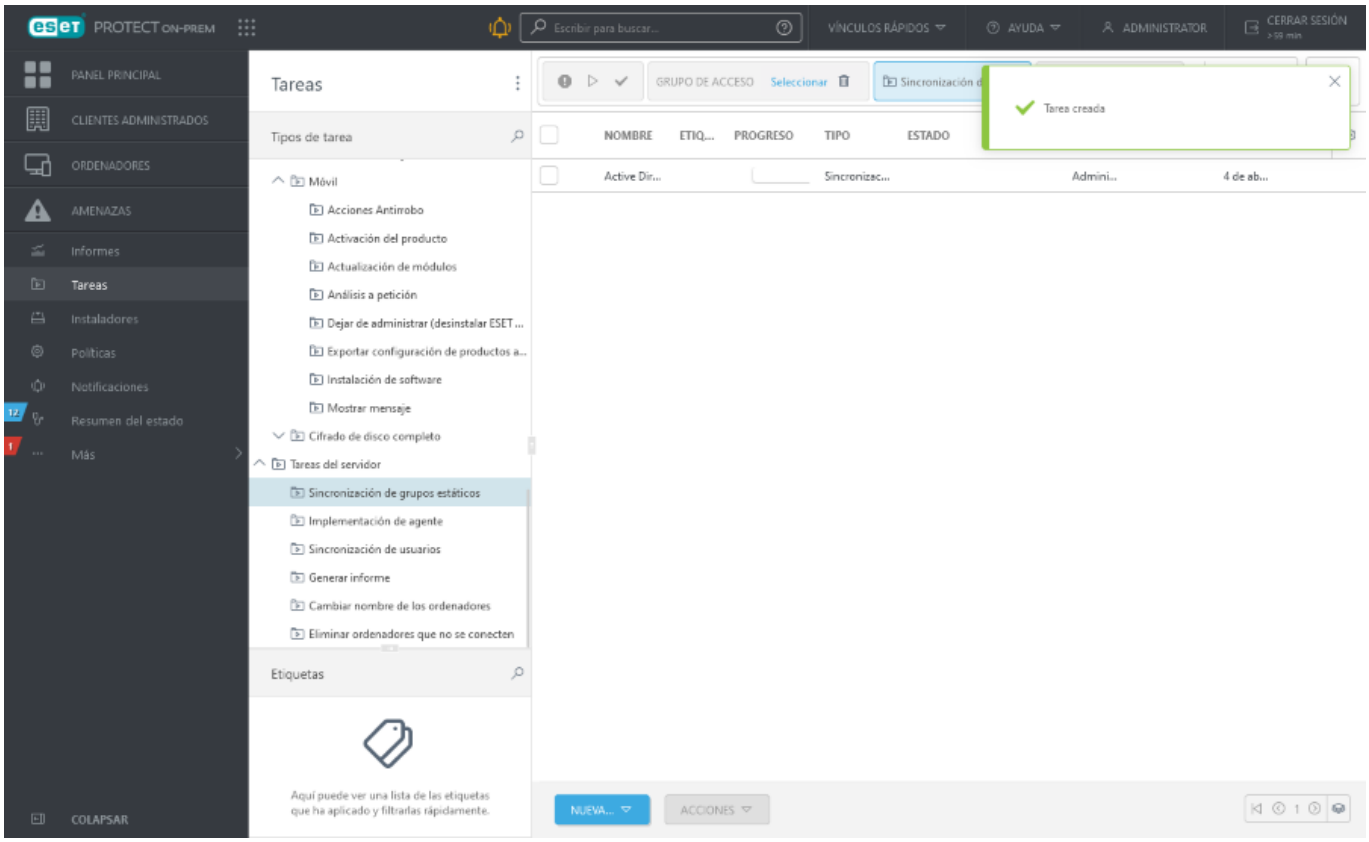
- Implementación local: instala ESET Management Agent y el producto de seguridad de ESET en un ordenador cliente de forma local.

> Le recomendamos que utilice la implementación local solo si tiene una red pequeña (hasta 50 ordenadores). Si la red es mayor, puede implementar ESET Management Agent mediante el uso de GPO o SCCM.

- Implementación remota: le recomendamos utilizar este método para implementar ESET Management Agent en un gran número de ordenadores cliente.

Agregar ordenadores mediante la sincronización con Active Directory

La sincronización con AD se lleva a cabo mediante la ejecución de la tarea del servidor **Sincronización de grupos estáticos**. Es una tarea predeterminada predefinida que se puede elegir para ejecutar automáticamente durante la instalación de ESET PROTECT On-Prem. Si el ordenador está en un dominio, se realizará la sincronización y los ordenadores de AD se incluirán en el grupo predeterminado **Todos**.



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

- Si necesita crear una nueva tarea de sincronización con AD, seleccione un grupo al que desea agregar los nuevos ordenadores desde el AD.

- Puede seleccionar los objetos del AD que desea sincronizar y qué hacer con los duplicados.

- Introduzca los ajustes de conexión del servidor del AD y establezca el modo de sincronización en **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 Implementación de agente para implementar el agente de ESET Management en los ordenadores sincronizados desde Active Directory.

Agregar nuevos dispositivos manualmente

Esta función le permite agregar manualmente **ordenadores** o dispositivos móviles que no se encuentran o agregan automáticamente. La ficha **Ordenadores** o **Grupo** le permite agregar nuevos ordenadores o dispositivos móviles.

1. Para agregar un nuevo ordenador, haga clic en **Ordenadores**, **Agregar dispositivo** y, a continuación, seleccione **Ordenadores** (también puede hacer clic en el icono del engranaje situado junto al **Grupo estático** existente y, a continuación, hacer clic en **Agregar nuevo**).

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

   - Escriba la **dirección IP** o el **nombre de cliente** de una máquina que desee agregar y ESET PROTECT On-Prem la buscará en la red. Opcionalmente puede escribir una **Descripción** de los ordenadores.

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

   - También puede usar **Importar CSV** para cargar un archivo *.csv* con una lista de los ordenadores que desea agregar. Para obtener más información, consulte Carga de CSV de importación.

   - **Copiar y pegar** una lista personalizada de ordenadores separada por delimitadores personalizados. Esta función tiene un comportamiento similar al de la importación de *.csv*.

3. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

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

5. **Usar resolución de FQDN**:

   - Marque la casilla de verificación y ESET PROTECT Server convertirá la dirección IP o el nombre de cliente del ordenador facilitados en un nombre de dominio completo.

   - Desmarque la casilla de verificación para importar los nombres de ordenador suministrados. Esta opción acelera la importación en lote de ordenadores con nombres en formato FQDN (por ejemplo, la importación desde un *.csv*).

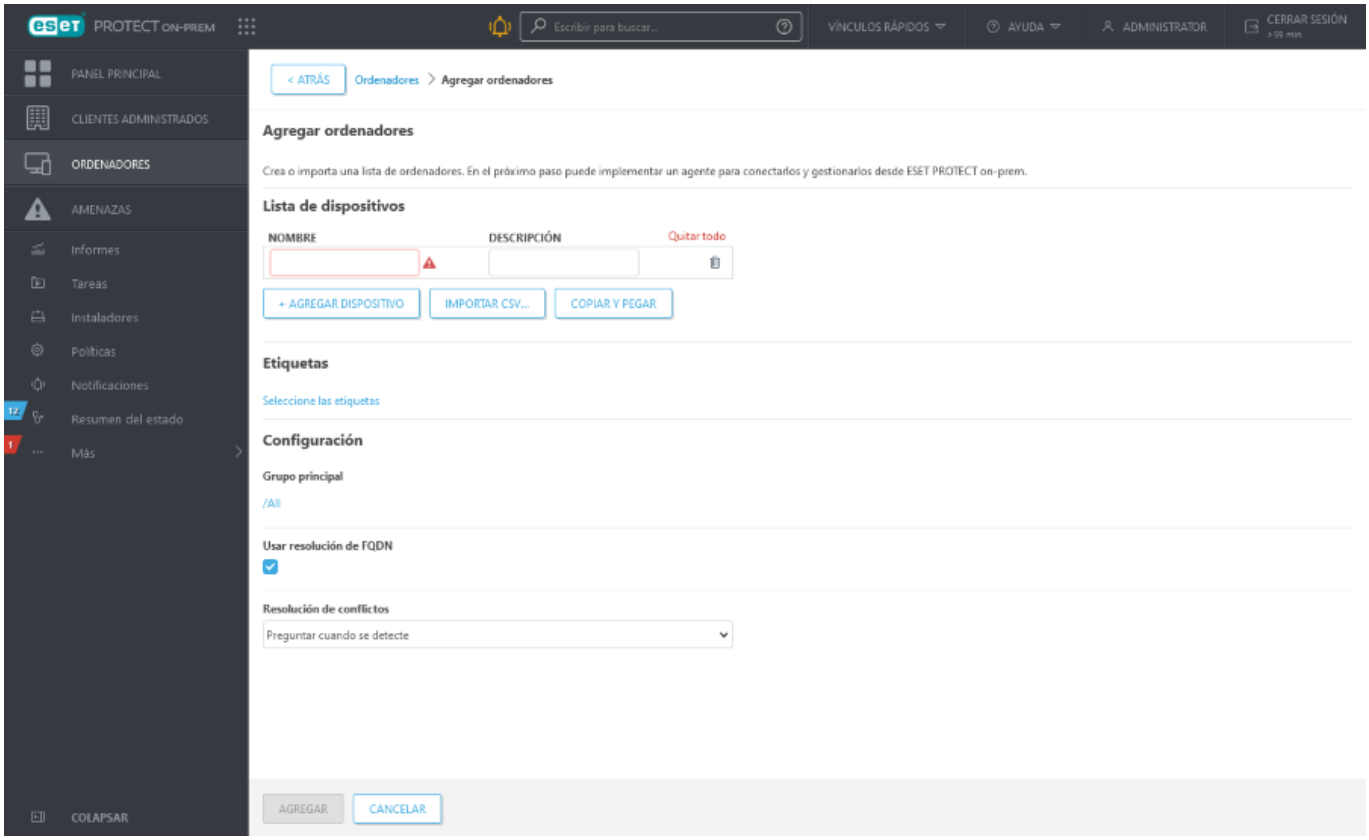
6. Utilice el menú desplegable **Resolución de conflictos** para seleccionar la acción que desea efectuar si un ordenador que está agregando ya existe en ESET PROTECT On-Prem:

• **Preguntar cuando se detectan conflictos**: cuando se detecte un conflicto, el programa le pedirá que seleccione una acción (ver las opciones a continuación).

• **Omitir dispositivos duplicados**: no se agregarán ordenadores duplicados.
• **Crear dispositivos duplicados**: Los equipos nuevos se agregarán, pero con nombres diferentes.

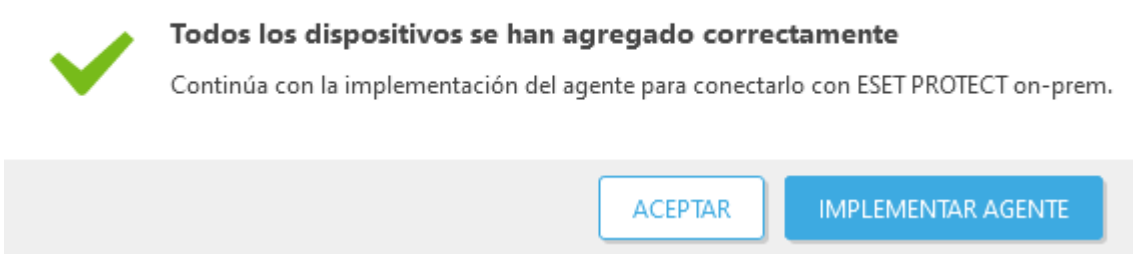
• **Mover dispositivos duplicados al grupo**: los ordenadores en conflicto se moverán al grupo principal.

7. Haga clic en **Agregar** cuando haya terminado de hacer 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 la ventana **Todos los dispositivos se han agregado 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 ordenadores agregados aparecerán en **Ordenadores**. Haga clic en el ordenador > **Soluciones** para implementar el agente:

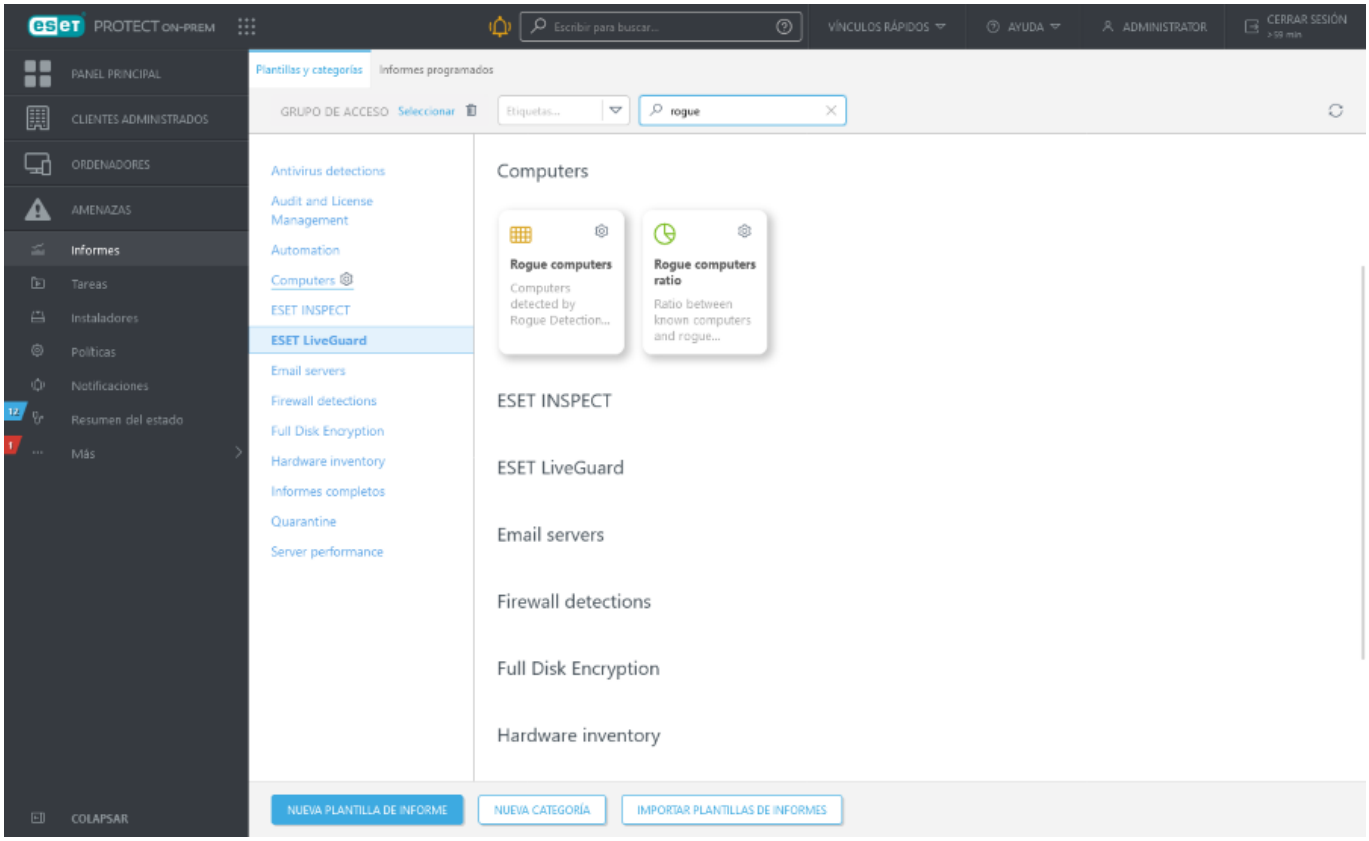
o **Implementar un agente usando un instalador**: en Crear instalador, seleccione el sistema operativo y el tipo de implementación del agente.

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

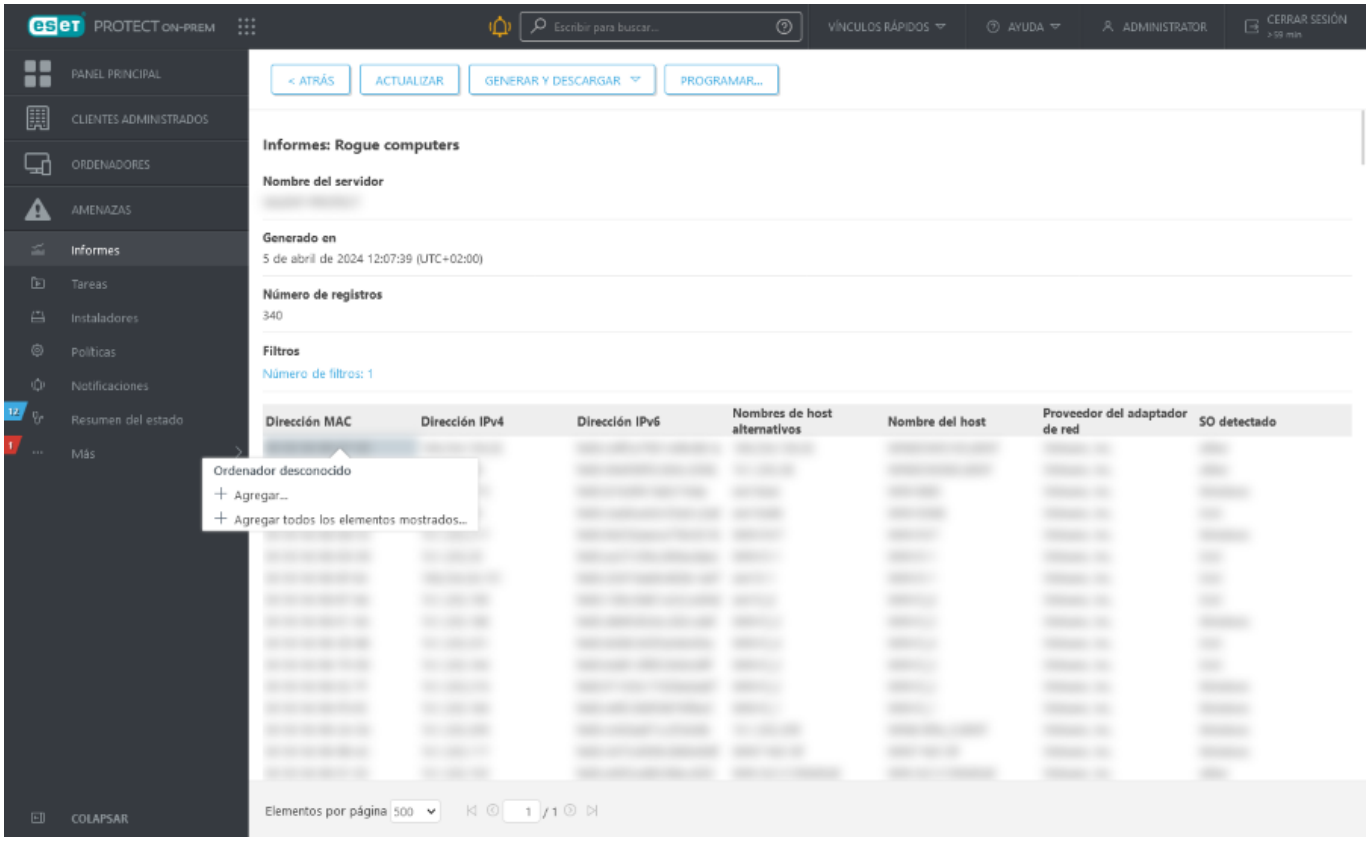
Agregar ordenadores con RD Sensor

Si no utiliza la sincronización con AD, la forma más fácil de encontrar un ordenador no administrado en la estructura de su red es utilizar RD Sensor. RD Sensor supervisa la red en la que se implementa y, cuando se conecta a la red un nuevo dispositivo sin agente, envía esta información a ESET PROTECT On-Prem.

En **Informes**, vaya a la sección **Ordenadores** y haga clic en el informe **Ordenadores sin registrar**.



En el informe Ordenadores sin registrar se incluyen los ordenadores encontrados por el Sensor de RD. Puede ajustar la información del informe de RD Sensor con la política de RD Sensor. Para agregar ordenadores, haga clic en el ordenador que desea agregar. También puede hacer clic en Agregar todos los elementos mostrados.



Si va a agregar un solo ordenador, puede utilizar un nombre predefinido o especificar el suyo propio (este es un nombre de visualización que solo se utilizará en ESET PROTECT Web Console, no un nombre de host real).

- También puede añadir una descripción si lo desea. Si este ordenador ya existiera en su directorio ESET PROTECT On-Prem, se le notificará y podrá decidir qué hacer con el duplicado. Las opciones disponibles son: **Implementar agente**, **Omitir**, **Reintentar**, **Mover**, **Duplicar** o **Cancelar**.

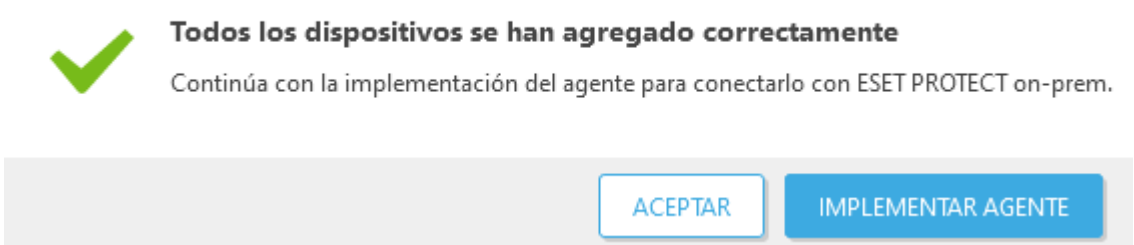
- Cuando se agrega el ordenador se abre una ventana con la opción **Implementar agente**.

Si utiliza **Agregar todos los elementos mostrados** se mostrará una lista de los ordenadores que se añadirán.

1.Haga clic en junto al nombre de un ordenador específico si no desea incluirlo en su directorio de ESET PROTECT On-Prem en este momento. Cuando termine de eliminar ordenadores de la lista, haga clic en **Agregar**.

2.Seleccione la acción que realizar con los duplicados (se producirá un ligero retraso en función del número de ordenadores de la lista): **Omitir, Reintentar, Mover**, **Duplicar** o **Cancelar**.

3.Aparecerá la ventana **Todos los dispositivos se han agregado 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 ordenadores agregados aparecerán en **Ordenadores**. Haga clic en el ordenador > **Soluciones** para implementar el agente:

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

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

Los resultados del análisis del Sensor de RD se anotan en un archivo de registro llamado `detectedMachines.log`. que contiene una lista de los ordenadores que se han encontrado en la 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

Configuración de políticas de ESET Rogue Detection Sensor

Es posible cambiar el comportamiento de ESET RD Sensor mediante una política. Esto se utiliza sobre todo para cambiar el filtrado de direcciones. Puede, por ejemplo, incluir determinadas direcciones en la lista negra para que no se detecten.

Haga clic en **Políticas** y despliegue **Políticas personalizadas para** modificar una política existente o crear una nueva.

Filtros

IPv4 Filtro

Habilitar el filtrado de direcciones IPv4: al habilitar el filtrado solo se detectarán los ordenadores cuyas direcciones IP formen parte de la lista blanca de la lista del filtro de IPv4, o solo los ordenadores que no estén en la lista negra.

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

Lista de direcciones **IPv4**: haga clic en Modificar lista de **IPv4** para agregar direcciones a la lista o quitarlas.

MAC Filtro de prefijos de direcciones

Habilitar el filtrado de prefijos de direcciones MAC: al habilitar el filtrado solo se detectarán los ordenadores cuyas direcciones MAC con prefijo de dirección (xx:xx:xx) formen parte de la lista de direcciones MAC, o solo los ordenadores que no estén en la lista negra.

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

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

Detección

Detección activa: activa Si esta opción, RD Sensor podrá buscar ordenadores activamente en la red local. Esto puede mejorar los resultados de la búsqueda, pero también puede desencadenar advertencias del cortafuegos en algunos ordenadores.

Puertos de detección de SO: RD Sensor utiliza una lista preconfigurada de puertos para buscar ordenadores en la red local. Puede editar la lista de puertos.

Configuración avanzada

Participar en el programa para la mejora del producto: active o desactive el envío de informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto).

Asignar

Especifique los clientes que recibirán esta política. Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione el ordenador en el que quiera aplicar una política y haga clic en **Aceptar**.

Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**.

Implementación local

Este método de implementación está pensado para instalaciones in situ. Cree o descargue un paquete de instalación y permita el acceso a él a través de una carpeta compartida, una unidad flash o un mensaje de correo electrónico.

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

Le recomendamos que utilice la implementación local solo si tiene una red pequeña (hasta 50 ordenadores). Si la red es mayor, puede implementar ESET Management Agent mediante el uso de GPO o SCCM.

La implementación local se puede realizar de tres maneras:

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

Implementación local y permiso

Para obtener más información sobre cómo permitir que un usuario implemente ESET Management Agent de forma local, siga las instrucciones de este ejemplo.

Recuerde que el usuario podrá trabajar con Certificados al crear instaladores. Un usuario debe tener permiso de **Uso** para **Certificados** con acceso al grupo estático que contiene los certificados. Si un usuario quiere implementar ESET Management Agent, es necesario que se le asigne permiso de **Uso** en la autoridad certificadora que ha firmado el correspondiente certificado del servidor. Para obtener información sobre cómo dividir el acceso a certificados y autoridades certificadoras, lea este ejemplo. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Crear instalador de Agent y productos de seguridad de ESET (Windows)

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

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

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

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

1. **Distribución**: seleccione **Descargar el instalador o utilizar ESET Remote Deployment Tool**.

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

2. **Componentes**: marque las casillas de verificación de las siguientes opciones:

- **Management Agent**: si no selecciona otros elementos en el **Componentes** el instalador solo incluirá ESET Management Agent. Seleccione esta opción si quiere instalar el producto de seguridad de ESET en el ordenador cliente posteriormente o si el ordenador cliente ya tiene un producto de seguridad de ESET instalado.

- **Producto de seguridad**: incluya el producto de seguridad de ESET con ESET Management Agent. Seleccione esta opción si el ordenador cliente no tiene ningún producto de seguridad de ESET instalado y quiere instalarlo con ESET Management Agent.

- **Cifrado de disco completo**: incluya ESET Full Disk Encryption en el instalador. Esta opción solo se muestra si la licencia de ESET Full Disk Encryption está activa.

• **ESET Inspect Connector**: incluya ESET Inspect Connector en el instalador. Esta opción solo se muestra si la licencia de ESET Inspect On-Prem está activa.

Si falta una casilla de producto ESET

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

3. Marque la casilla de verificación **Participar en el programa para la mejora del producto** para enviar informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto).

4. **Grupo principal**: seleccione el grupo principal en el que ESET PROTECT Web Console situará el ordenador tras la instalación de un agente.

• Puede seleccionar un grupo estático existente o crear un nuevo grupo estático a los que se les asignará el dispositivo una vez implementado el instalador.

• 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 se utiliza ESET Business Account con sitios o ESET MSP Administrator y opcional si se utiliza ESET Business Account sin sitios.

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

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

6. **Certificado de igual**:

• **certificado de ESET PROTECT**: el certificado de igual para la instalación del agente y la autoridad certificadora de ESET PROTECT se seleccionan automáticamente. 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 **Personalizar certificado** > **cargue** el certificado .pfx y selecciónelo al instalar el agente. Si desea obtener más información, consulte Certificados.

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

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

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

7. Personalizar más configuraciones

- 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 se desea utilizar el instalador durante más tiempo, para garantizar que se instala siempre la versión más reciente de los productos y componentes.
- Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
- **Configuración inicial (opcional)**: utilice esta opción para aplicar una política de configuración a ESET Management Agent. Haga clic en **Seleccionar** en **Configuración del agente** y elija en la lista de políticas disponibles. Si ninguna de las políticas predefinidas es adecuada, puede crear una nueva política o personalizar las existentes.
- Si utiliza un proxy HTTP (recomendamos utilizar ESET Bridge), marque la casilla **Activar configuración del proxy HTTP** y especifique la configuración del proxy (**Cliente**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador desde el proxy y establezca la conexión de ESET Management Agent con el proxy para activar el reenvío de comunicación entre ESET Management Agent y ESET PROTECT Server. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge utiliza el puerto 3128 de forma predeterminada. Puede establecer un puerto distinto si lo necesita. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

  El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

La casilla **Usar conexión directa si el proxy HTTP no está disponible** está marcada de forma predeterminada. El asistente aplica el ajuste como reserva para el instalador: no puede desmarcar la casilla. Puede deshabilitar la configuración mediante una política de ESET Management Agent:

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

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 **Avanzado**. De forma predeterminada, se selecciona previamente la versión más reciente (recomendado). Puede seleccionar una versión anterior.

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

b. Marque la casilla de verificación situada junto al ajuste para activarlo para el instalador:
oActivar el sistema de respuesta de ESET LiveGrid® (recomendado)
oActivar la detección de aplicaciones potencialmente indeseables: obtenga más información en este artículo de la base de conocimiento.
o**Permitir cambiar la configuración de protección durante la instalación**: le recomendamos que no marque esta casilla de verificación.

c.Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.
d.**Personalizar más configuraciones**:
o**Licencia**: Seleccione la licencia del producto adecuada en 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 caducadas o sobreutilizadas (las que tienen 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 con uno de los métodos descritos en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de inicio sea **Todo** y que tenga el permiso de **Escritura** en las licencias.
o**Configuración** También puede seleccionar una **política** para que se aplique al producto de seguridad de ESET durante la instalación.
o **Ejecutar ESET AV Remover**: marque la casilla de verificación para desinstalar o quitar por completo otros programas antivirus del dispositivo de destino.
o**Instalación de módulos**: es posible que la opción no esté disponible, según el producto de seguridad de ESET seleccionado. De forma predeterminada, el instalador del producto contiene solo los módulos esenciales de ESET. El resto de 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 implementaciones sin conexión).

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

Cifrado de disco completo

a.Haga clic en la opción **ESET Full Disk Encryption** seleccionada previamente y cambie sus detalles:
o Seleccione el idioma en el menú desplegable **Idioma**.
oMarque la casilla de verificación **Avanzado**. De forma predeterminada, se selecciona previamente la versión más reciente (recomendado). Puede seleccionar una versión anterior.
b.Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.
c.**Configuración**: seleccione la política que se aplicará a ESET Full Disk Encryption durante la instalación.
d.**Personalizar más configuraciones**:
o**Licencia**: Seleccione la licencia del producto adecuada en 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 caducadas o sobreutilizadas (las que tienen 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 con uno de los métodos descritos en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de inicio sea **Todo** y que tenga el permiso de **Escritura** en las licencias.

ESET Inspect Connector

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

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

b.Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.
c.**Personalizar más configuraciones**:
o**Licencia**: Seleccione la licencia del producto adecuada en 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 caducadas o sobreutilizadas (las que tienen 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 con uno de los métodos descritos en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de inicio sea **Todo** y que tenga el permiso de **Escritura** en las licencias.
o**Configuración**: haga clic en **Seleccionar** para seleccionar una política de ESET Inspect Connector existente o **Crear** para crear una nueva política de ESET Inspect Connector. El instalador aplicará la configuración de la política durante la instalación de ESET Inspect Connector.
oEscriba el **Nombre de host del servidor** de ESET Inspect On-Prem y el **puerto** de conexión especificado durante la instalación del servidor de ESET Inspect (el puerto predeterminado es 8093).
oSeleccione la **autoridad certificadora** para conectarse al servidor de ESET Inspect.

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

    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 de ESET Management Agent o un producto de seguridad de ESET en Windows ARM64.

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

12. Tras crear y descargar el paquete de instaladores todo en uno, hay dos opciones para implementar ESET Management Agent:

- Localmente en un ordenador cliente Ejecute el archivo del paquete de instalación en un ordenador cliente. Instalará ESET Management Agent y el producto de seguridad de ESET en el dispositivo y conectará 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 multisesión de Windows 10. Para instrucciones detalladas, consulte la sección Asistente de instalación. Puede ejecutar el paquete de instalación en modo silencioso para ocultar la ventana del asistente de instalación.

- Utilizar la Herramienta de implementación remota de ESET para implementar instancias de ESET Management Agent en varios ordenadores cliente al mismo tiempo.

Crear instalador de script de agente: Windows/Linux/macOS

Este tipo de implementación del agente es útil cuando las opciones de implementación remota y local no le convienen. Puede distribuir el instalador de scripts del agente por correo electrónico y dejar que el usuario lo implemente. También puede ejecutar el instalador de scripts del agente desde un medio extraíble (una unidad de memoria USB, por ejemplo).

El ordenador cliente debe tener conexión a Internet para descargar el paquete de instalación del agente y conectarse a ESET PROTECT On-Prem.

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

- **Vínculos rápidos** > **Implementar agente**

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

- Recorrido por ESET PROTECT On-Prem

1. Marque la casilla de verificación **Participar en el programa para la mejora del producto** para enviar

informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto).

2. **Grupo principal**: seleccione el grupo principal en el que ESET PROTECT Web Console situará el ordenador tras la instalación de un agente.

- Puede seleccionar un grupo estático existente o crear un nuevo grupo estático a los que se les asignará el dispositivo una vez implementado el instalador.
- 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 se utiliza ESET Business Account con sitios o ESET MSP Administrator y opcional si se utiliza ESET Business Account sin sitios.

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

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

4. **Certificado de igual**:

- **certificado de ESET PROTECT**: el certificado de igual para la instalación del agente y la autoridad certificadora de ESET PROTECT se seleccionan automáticamente. 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 **Personalizar certificado** > **cargue** el certificado .pfx y selecciónelo al instalar el agente. Si desea obtener más información, consulte Certificados.

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

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

5. Personalizar más configuraciones

- Escriba el **nombre del instalador** y la **descripción** (opcional).
- Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
- **Configuración inicial (opcional)**: utilice esta opción para aplicar una política de configuración a ESET Management Agent. Haga clic en **Seleccionar** en **Configuración del agente** y elija en la lista de políticas disponibles. Si ninguna de las políticas predefinidas es adecuada, puede crear una nueva política o personalizar las existentes.
- Si utiliza un proxy HTTP (recomendamos utilizar ESET Bridge), marque la casilla **Activar configuración del proxy HTTP** y especifique la configuración del proxy (**Cliente**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador desde el proxy y establezca la conexión de ESET Management Agent con el proxy para activar el reenvío de comunicación entre ESET Management Agent y ESET PROTECT Server. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge utiliza el puerto 3128 de forma predeterminada. Puede establecer un puerto distinto si lo necesita. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

> El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

La casilla **Usar conexión directa si el proxy HTTP no está disponible** está marcada de forma predeterminada. El asistente aplica el ajuste como reserva para el instalador: no puede desmarcar la casilla. Puede deshabilitar la configuración mediante una política de ESET Management Agent:

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

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

7. Extraiga el archivo comprimido descargado en el ordenador cliente en el que desea implementar ESET Management Agent.

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

- Implementación del agente: Windows
- Implementación del agente: Linux
- Implementación del agente: macOS

> ESET PROTECT On-Prem admite la actualización automática de las instancias de ESET Management Agent en ordenadores administrados.

Implementación 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 en la que se encuentra el paquete del agente. También puede utilizar la dirección IP del nuevo paquete.
Busque y modifique estas 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
```

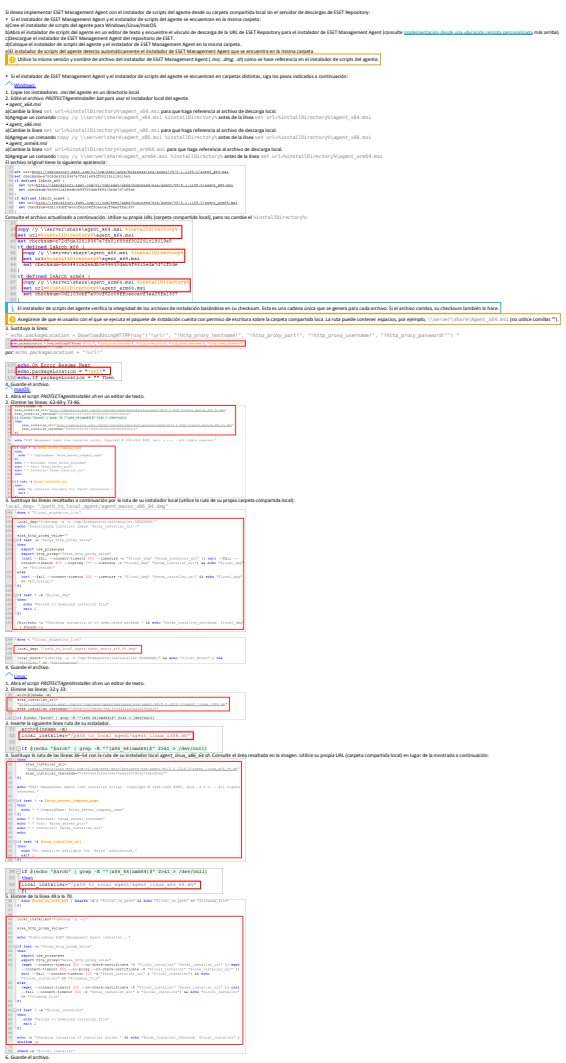
Linux:

```
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
```

Implementación desde una carpeta compartida local



Implementación del agente: Windows

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

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

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

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

5. El ordenador con el agente instalado aparecerá en ESET PROTECT Web Console y podrá administrarlo con ESET PROTECT On-Prem.

- Si hay algún problema con el agente (por ejemplo, si no se conecta a ESET PROTECT Server), consulte la sección sobre resolución de problemas.
- ESET PROTECT On-Prem admite la actualización automática de las instancias de ESET Management Agent en ordenadores administrados.

Implementación del agente: Linux

Requisitos previos

- El ordenador debe estar accesible desde la red.
- Se recomienda **usar la versión más reciente de OpenSSL1.1.1**. ESET Management Agent es compatible con OpenSSL 3.x. La versión mínima compatible de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema a la vez. En su sistema debe haber al menos una versión compatible.
    - Use el comando `openssl version` para mostrar la versión predeterminada actual.
    - Puede enumerar todas las versiones de OpenSSL presentes en su sistema. Vea las extensiones de nombre de archivo con el comando `sudo find / -iname *libcrypto.so*`
    - Puede comprobar si su cliente Linux es compatible utilizando el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`

> **OpenSSL 3.x compatibilidad**
> - ESET Management Agent es compatible con OpenSSL 3.x.
> - ESET PROTECT Server/MDM no es compatible de forma nativa con OpenSSL 3.x, pero puede habilitar la compatibilidad de OpenSSL 3.x con ESET PROTECT On-Prem.

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

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

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

```
yum install policycoreutils-devel
```

Instalación

Proceda a instalar el componente ESET Management Agent en Linux mediante un comando en el terminal.

> El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

Siga los pasos indicados a continuación para la instalación de Agent en la estación de trabajo Linux.

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

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

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

5. Cuando se le indique, escriba la contraseña de administrador local y pulse **Entrar**.

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

7. El ordenador con el agente instalado aparecerá en ESET PROTECT Web Console y podrá administrarlo con ESET PROTECT On-Prem.

Si el ordenador con el agente instalado no aparece en su ESET PROTECT On-Prem, realice la solución de problemas.

ESET PROTECT On-Prem admite la actualización automática de las instancias de ESET Management Agent en ordenadores administrados.

Implementación del agente: macOS

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

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

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

4. Activar acceso total al disco para el terminal:

   a)Abra **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. Activar acceso total al disco para ESET Management Agent:

De forma local:

a)Abra **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 ESET Management Agent a la lista de aplicaciones en la carpeta **Acceso total al disco**.

e)Bloquee la configuración en la esquina inferior izquierda.

De forma remota:

a)Descargue el archivo de configuración .plist.

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

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

8. El ordenador con el agente instalado aparecerá en ESET PROTECT Web Console y podrá administrarlo con ESET PROTECT On-Prem.

Se instalará una instancia de ESET Management Agent nativa de ARM64 (versión 9.1 y versiones posteriores) en los sistemas macOS ARM64.
ESET PROTECT On-Prem admite la actualización automática de las instancias de ESET Management Agent en ordenadores administrados.

Instalación y resolución de problemas del agente

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

El archivo de registro de ESET Management Agent se encuentra en el siguiente directorio:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

Descargar agente del sitio web de ESET

Descargue el paquete de instalación de ESET Management Agent del sitio web de ESET. Seleccione el paquete adecuado dependiendo del sistema operativo del ordenador cliente:

- Instalación asistida por el servidor e instalación sin conexión en Linux
- macOS
- Windows

  oInstalación asistida por el servidor: con el paquete de instalación del agente, este método descarga automáticamente los certificados de ESET PROTECT Server (recomendado para implementación local).

  - No puede utilizar un usuario con autenticación de doble factor en instalaciones ayudadas por el servidor.
  - Si decide permitir la instalación asistida por servidor por parte de otro usuario, asegúrese de tener configurados los siguientes permisos:

  oEl usuario debe tener permiso de Uso en la autoridad certificadora que firmó el certificado de igual del servidor y permiso de Uso en al menos un certificado de igual. Si no existe tal certificado, el usuario necesitará permiso de Escritura para crear uno nuevo.
  oPermiso de **Escritura** en el grupo estático al que el usuario quiera agregar el ordenador.

  oInstalación sin conexión: utilizando el paquete de instalación del agente. En este método de implementación debe exportar los certificados y aplicarlos manualmente.

Consulte el registro de estado del ordenador cliente (disponible en *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html*) para asegurarse de que ESET Management Agent funcione correctamente.

Si surgieran problemas con el agente (p. ej., que no se conecte a ESET PROTECT Server), consulte la sección Resolución de problemas: implementación del agente.

Implementación remota

La implementación se puede realizar de las siguientes formas:

- ESET Remote Deployment Tool: esta herramienta le permite implementar los paquetes del instalador de ESET Management Agent (y el producto de seguridad de ESET) que ha creado en ESET PROTECT Web Console.
- Objeto de política de grupo (GPO) y Administrador de configuración del centro de sistema (SCCM): Utilice esta opción para la implementación masiva de ESET Management Agent en ordenadores cliente.
- Tarea del servidor de implementación de agente: alternativa a GPO y SCCM.

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

- Resolución de problemas - Implementación del agente

- Resolución de problemas - Conexión con el agente
- Situaciones de ejemplo de la implementación de ESET Management Agent

Implementación remota y permisos

Si quiere permitir que el usuario cree instaladores de GPO o scripts de SCCM, configure sus permisos según nuestro ejemplo.

Para la tarea del servidor Implementación del agente son necesarios los siguientes permisos:

- Permiso de **Escritura** de **Grupos y ordenadores** donde se ejecuta la implementación
- Permiso de **Uso** en **Certificados** con acceso al grupo estático en el que están los certificados
- Permiso de **Uso** en **Implementación de agente** en la sección **Tareas y desencadenadores de servidor**

Implementación del agente con GPO o SCCM

Además de la implementación local, también puede usar herramientas de administración como Objeto de política de grupo (GPO), Administrador de configuración del centro de sistema (SCCM), Symantec Altiris o Puppet para implementar el agente de forma remota.

Utilice esta opción para la implementación masiva de ESET Management Agent en ordenadores cliente.

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

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

2. Marque la casilla de verificación **Participar en el programa para la mejora del producto** para enviar informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto).

3. **Grupo principal**: seleccione el grupo principal en el que ESET PROTECT Web Console situará el ordenador tras la instalación de un agente.

   - Puede seleccionar un grupo estático existente o crear un nuevo grupo estático a los que se les asignará el dispositivo una vez implementado el instalador.
   - 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 se utiliza ESET Business Account con sitios o ESET MSP Administrator y opcional si se utiliza ESET Business Account sin sitios.

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

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

5. **Certificado de igual**:

• **certificado de ESET PROTECT**: el certificado de igual para la instalación del agente y la autoridad certificadora de ESET PROTECT se seleccionan automáticamente. 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 **Personalizar certificado** > **cargue** el certificado .pfx y selecciónelo al instalar el agente. Si desea obtener más información, consulte Certificados.

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

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

6. Personalizar más configuraciones

- Escriba el **nombre del instalador** y la **descripción** (opcional).
- Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
- **Configuración inicial (opcional)**: utilice esta opción para aplicar una política de configuración a ESET Management Agent. Haga clic en **Seleccionar** en **Configuración del agente** y elija en la lista de políticas disponibles. Si ninguna de las políticas predefinidas es adecuada, puede crear una nueva política o personalizar las existentes.
- Si utiliza un proxy HTTP (recomendamos utilizar ESET Bridge), marque la casilla **Activar configuración del proxy HTTP** y especifique la configuración del proxy (**Cliente**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador desde el proxy y establezca la conexión de ESET Management Agent con el proxy para activar el reenvío de comunicación entre ESET Management Agent y ESET PROTECT Server. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge utiliza el puerto 3128 de forma predeterminada. Puede establecer un puerto distinto si lo necesita. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

  El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

  La casilla **Usar conexión directa si el proxy HTTP no está disponible** está marcada de forma predeterminada. El asistente aplica el ajuste como reserva para el instalador: no puede desmarcar la casilla. Puede deshabilitar la configuración mediante una política de ESET Management Agent:
  - Durante la creación del instalador: incluya la política en **Configuración inicial**.
  - Tras la instalación del agente de ESET Management: asigne la política al ordenador.

7. Haga clic en **Finalizar**.

8. Descargue el script de GPO/SCCM y los instaladores del agente (32 bits, 64 bits, ARM64). También puede descargar los archivos *.msi* del instalador del **Agente** desde la página de descargas de ESET, sección Instaladores independientes.

Haga clic en el vínculo correspondiente a continuación para ver instrucciones detalladas de dos métodos de

implementación remota populares de ESET Management Agent:

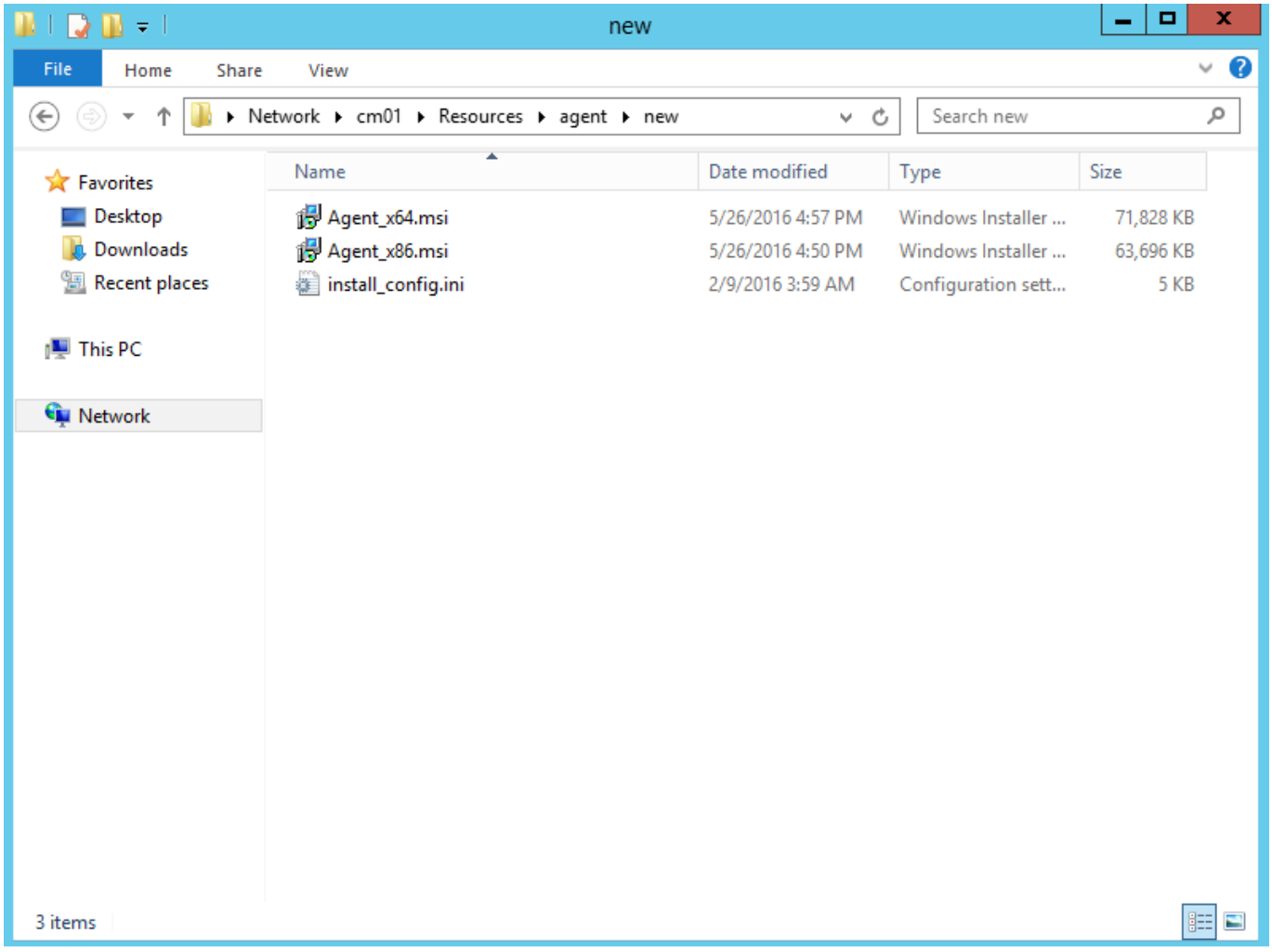
- Implementación de ESET Management Agent utilizando Objeto de política de grupo (GPO): este artículo de la Base de conocimiento puede no estar disponible en su idioma.

- Implementación de ESET Management Agent utilizando Administrador de configuración del centro de sistema (SCCM)

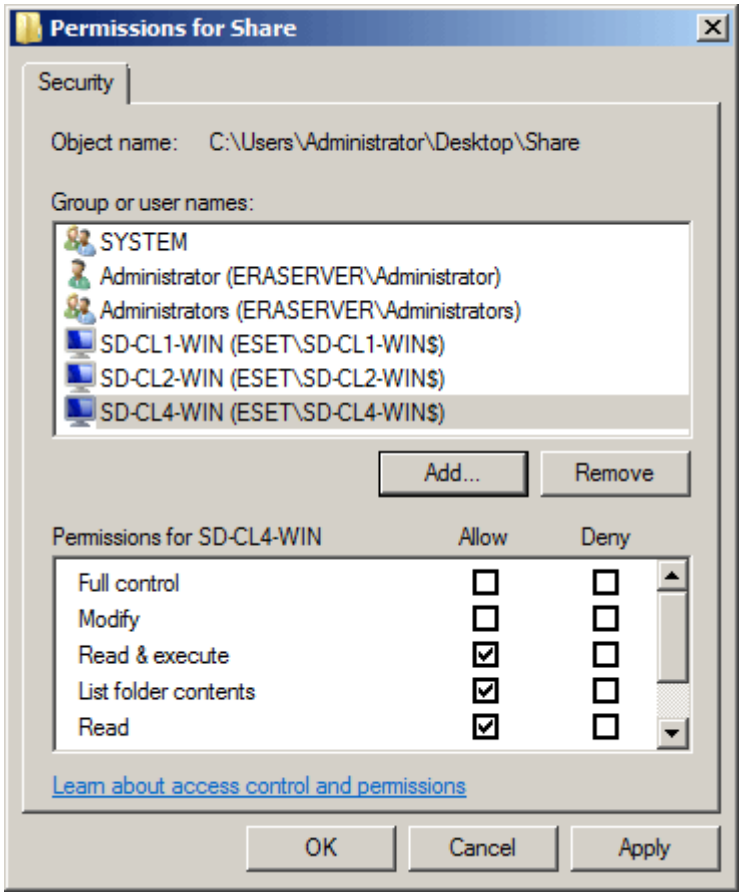
Pasos de implementación - SCCM

Para implementar ESET Management Agent con SCCM, siga estos pasos:

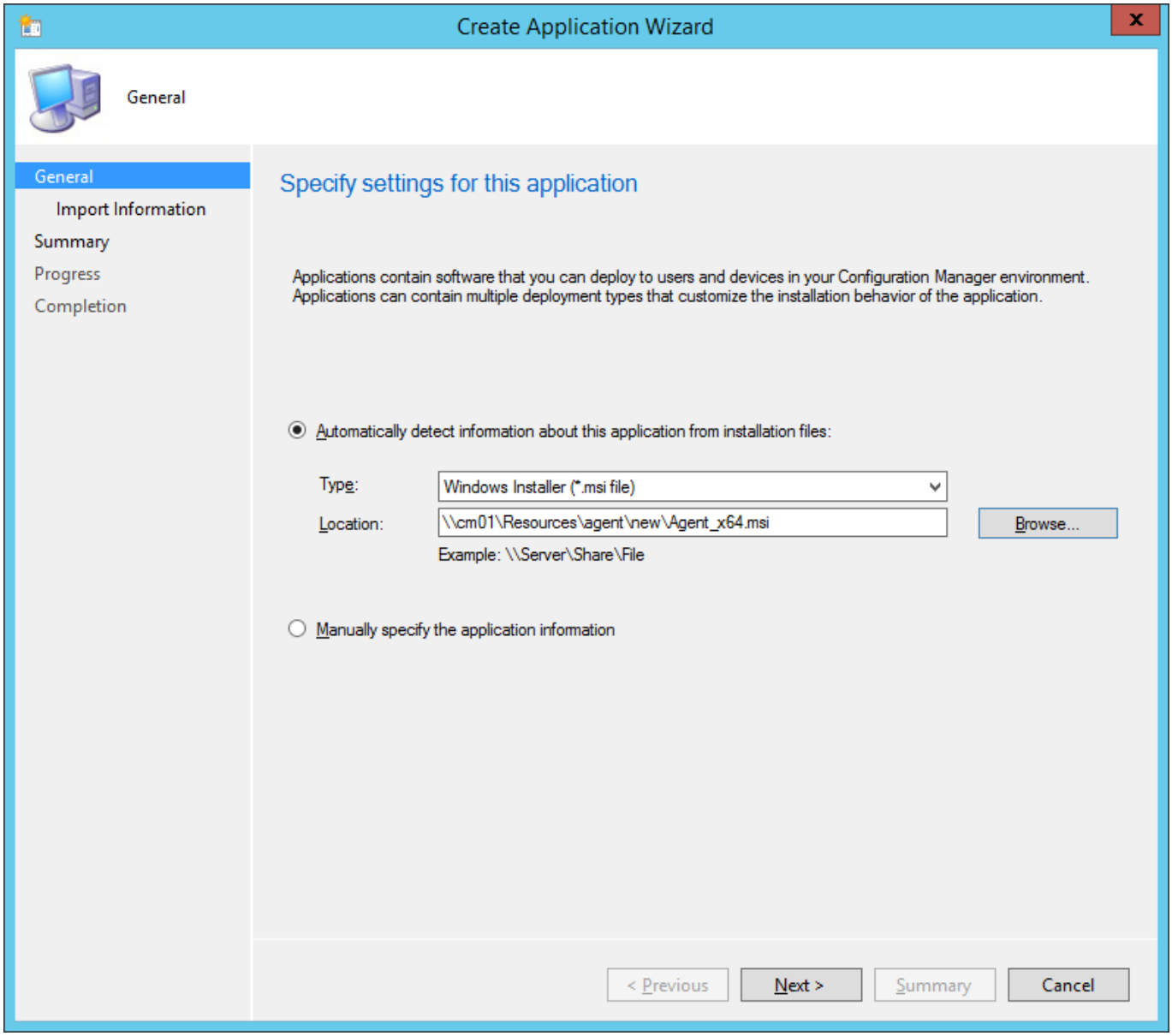
1. Coloque los archivos *.msi* del instalador de ESET Management Agent y el archivo *install_config.ini* en una carpeta compartida.



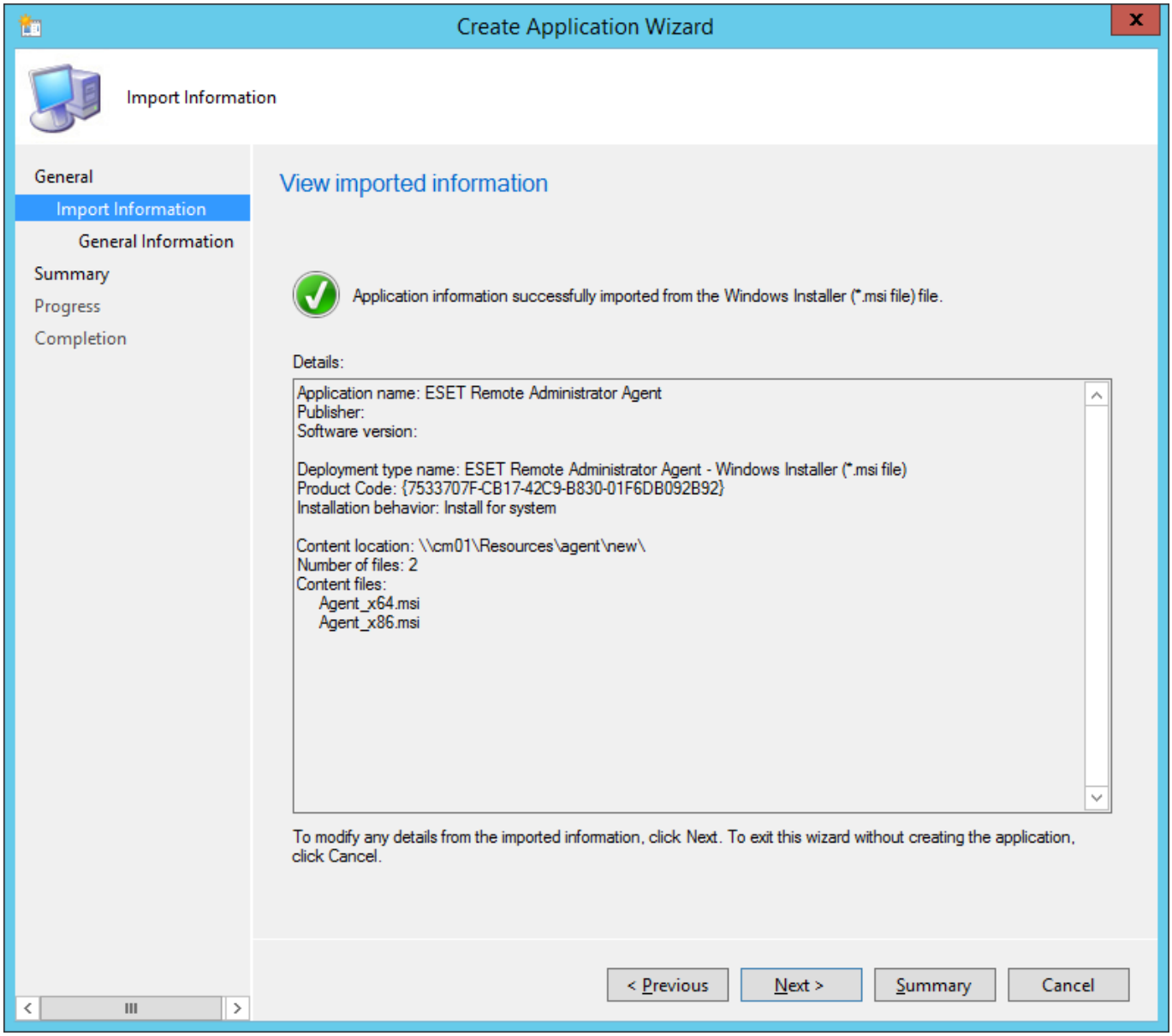
los ordenadores cliente necesitarán acceso de lectura o ejecución en esta carpeta compartida.



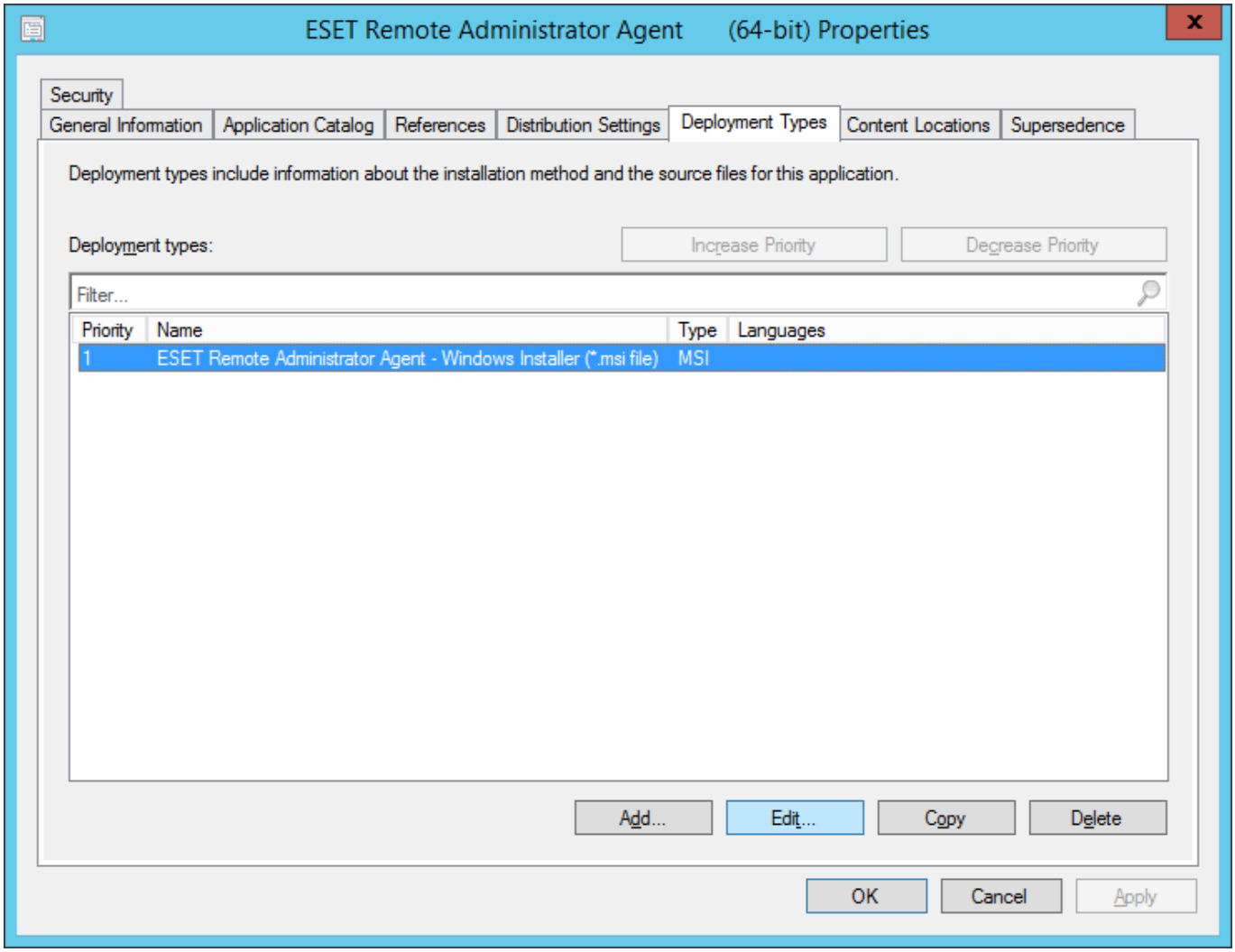
2. Abra la consola de SCCM y haga clic en **Biblioteca de software**. En **Gestión de aplicaciones** haga clic con el botón derecho en **Aplicaciones** y elija **Crear aplicación**. Elija **Instalador de Windows (archivo *.msi)**.



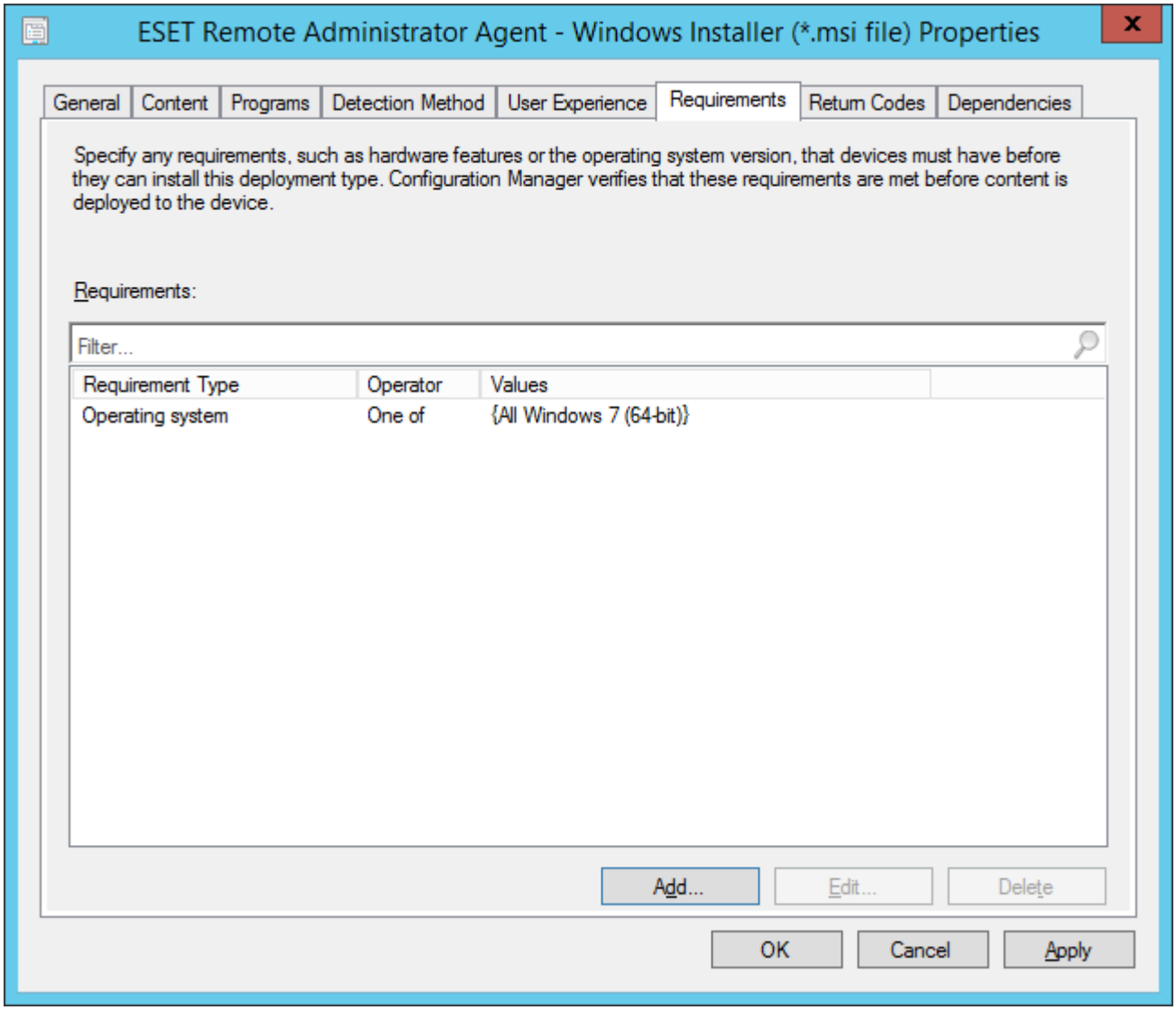
3. Especifique toda la información necesaria sobre la aplicación y haga clic en **Siguiente**.

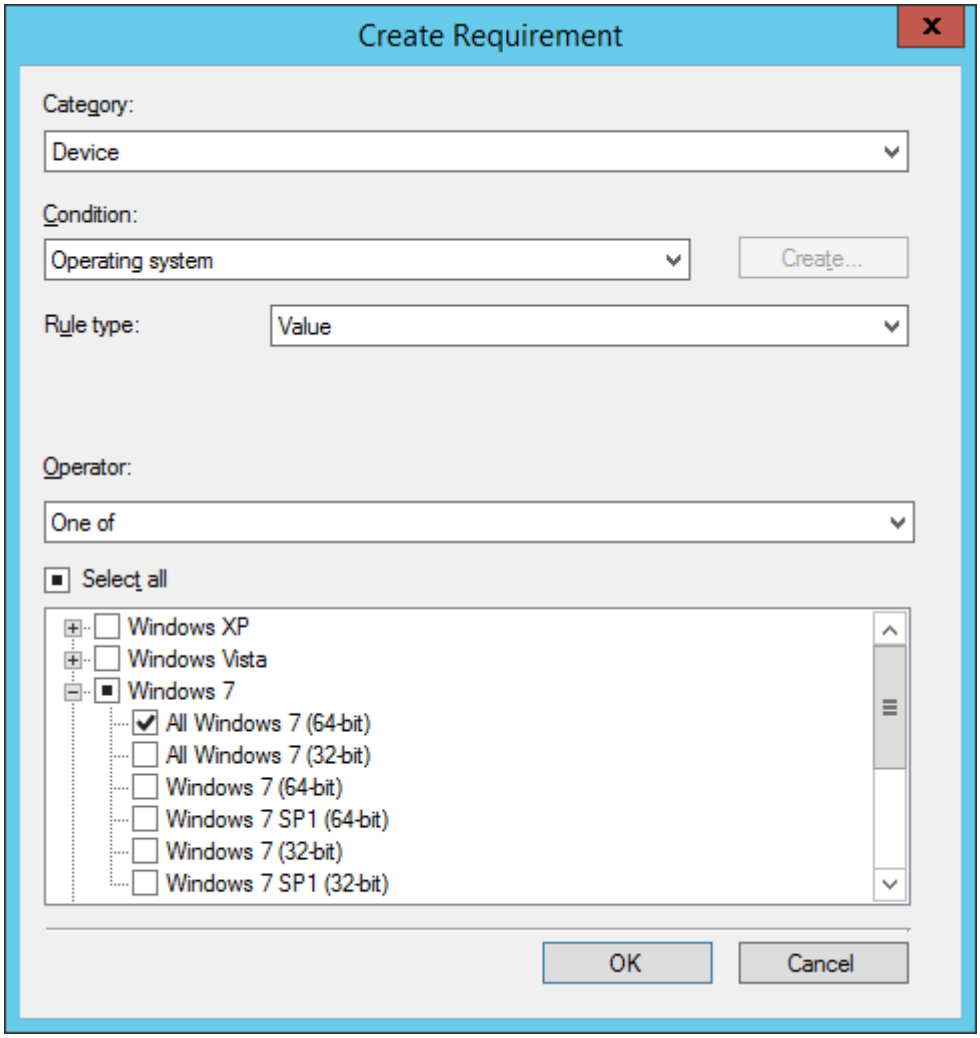


4. Haga clic con el botón derecho en la aplicación ESET Management Agent, haga clic en la ficha **Tipos de implementación**, seleccione la única implementación disponible y, a continuación, haga clic en **Edición**.

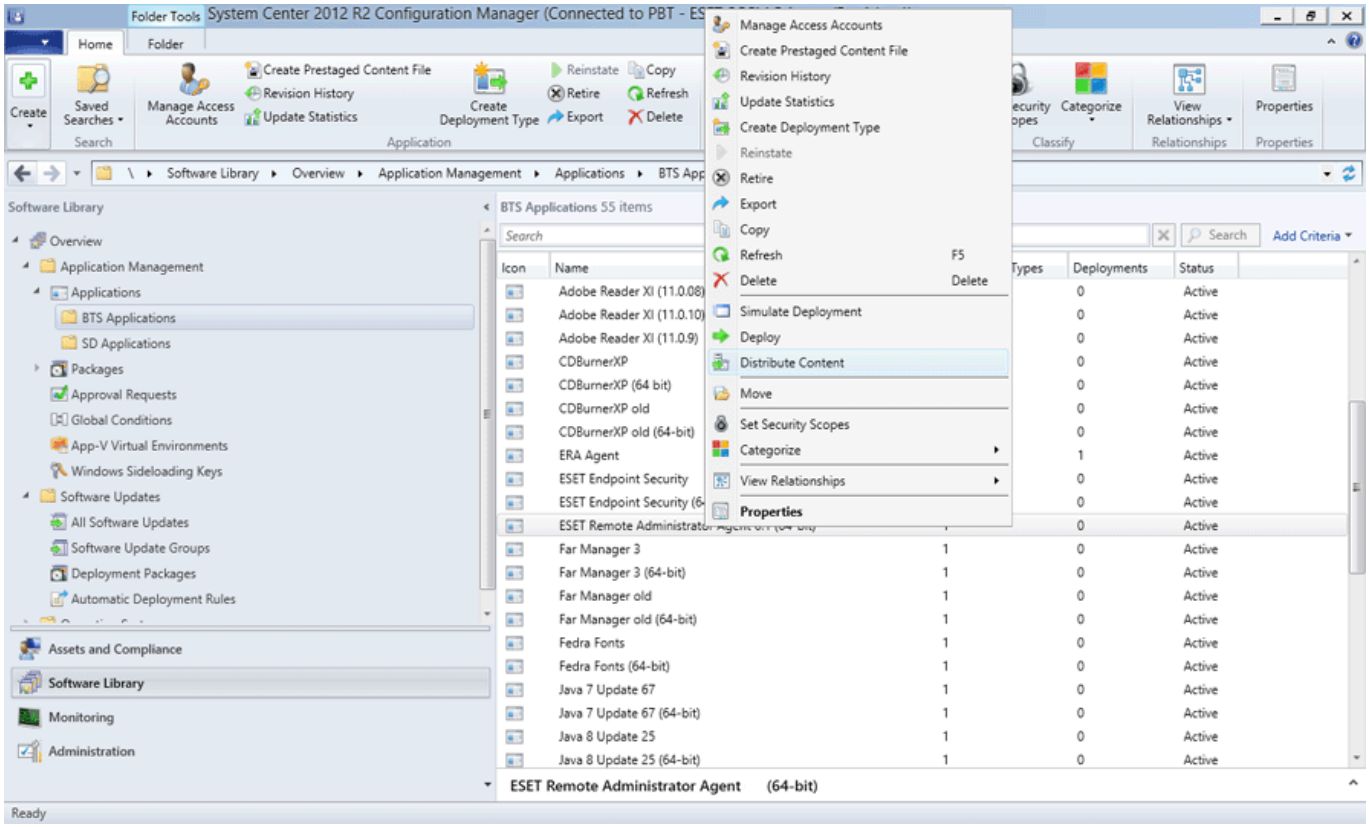


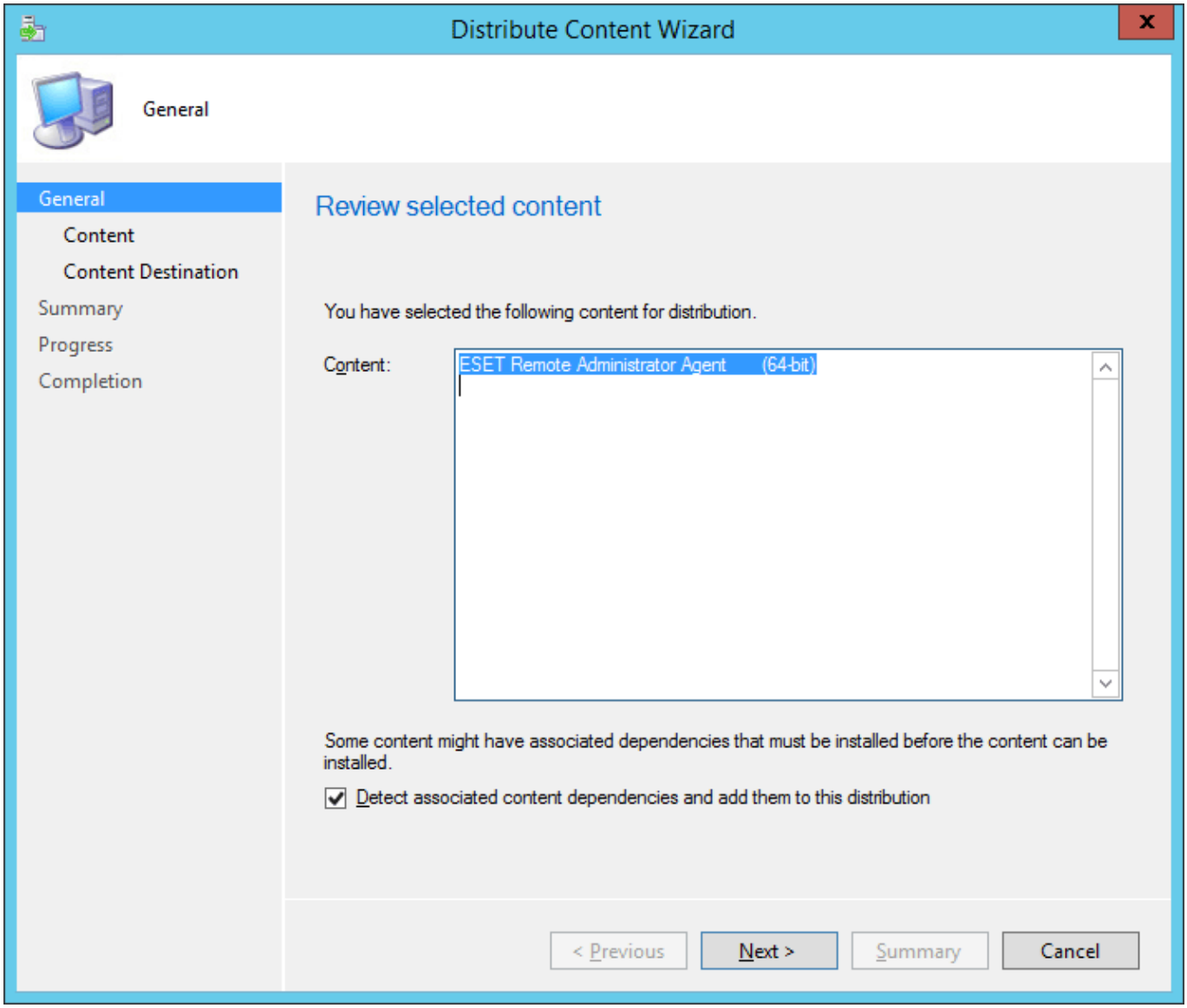
5. Haga clic en la ficha **Requisitos** y, a continuación, haga clic en **Agregar**. Seleccione **Sistema operativo** en el menú desplegable **Condición**, seleccione **Uno de** en el menú desplegable **Operador** y, a continuación, especifique los sistemas operativos en los que realizará la instalación marcando las casillas correspondientes. Cuando termine, haga clic en **Aceptar** y, a continuación, haga clic en **Aceptar** para cerrar las ventanas restantes y guardar los cambios realizados.

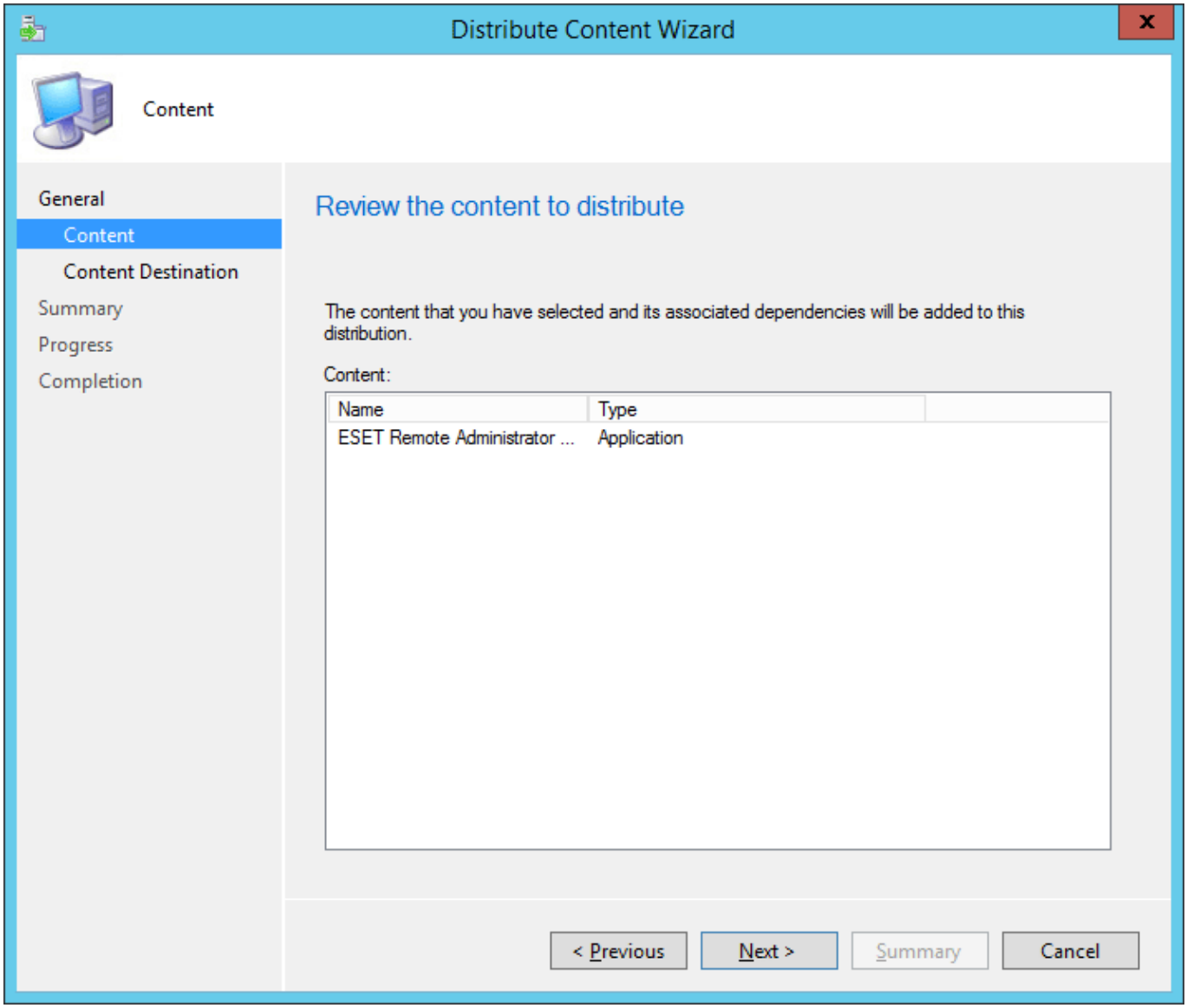

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install 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



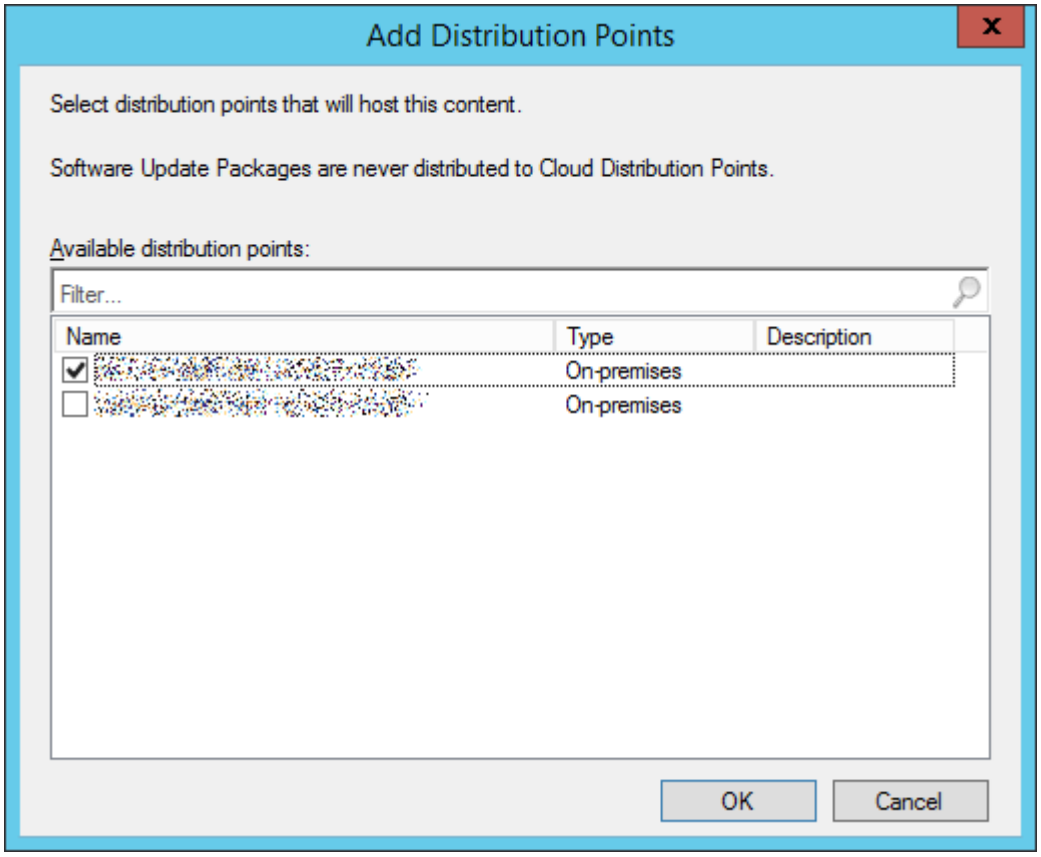
6. En la Biblioteca de software del centro del sistema, haga clic con el botón derecho en su nueva aplicación y seleccione **Distribuir contenido** en el menú contextual. Siga los mensajes del Asistente para la implementación de software para completar la implementación de la aplicación.

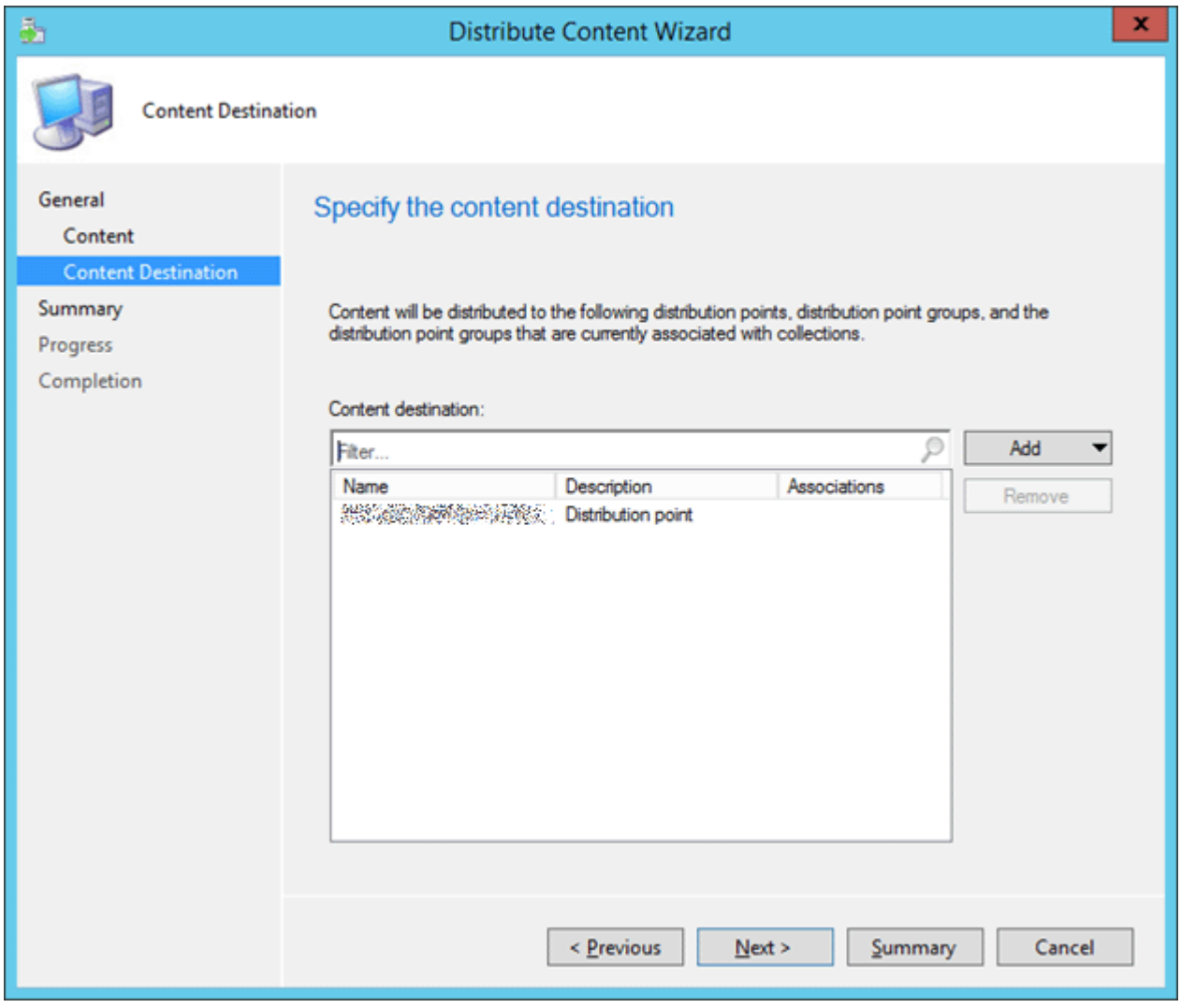

Folder Tools
System Center 2012 R2 Configuration Manager (Connected to PBT - ES
Home
Folder
Create
Saved Searches
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Search
Application
Categorize
View 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

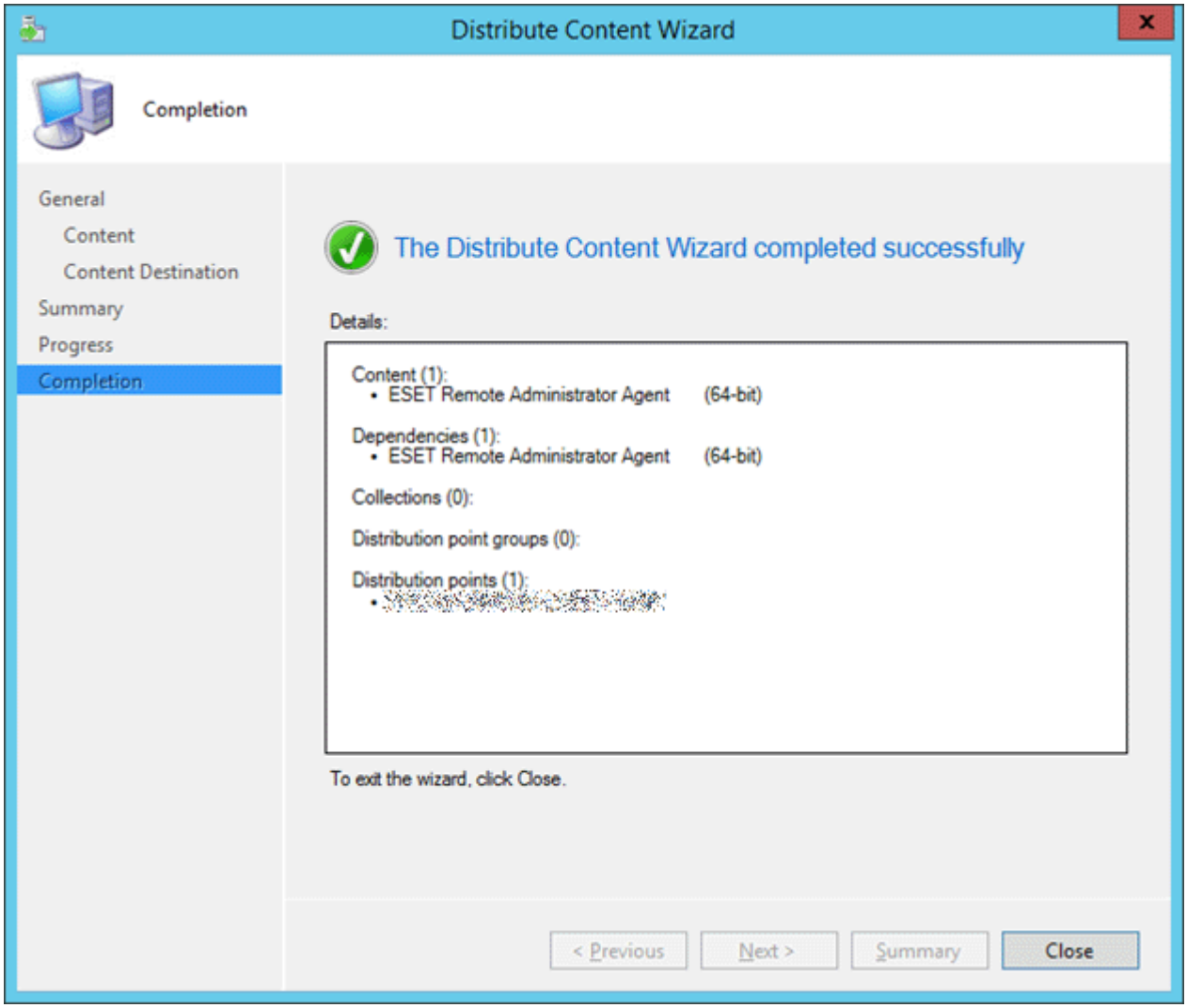

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed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

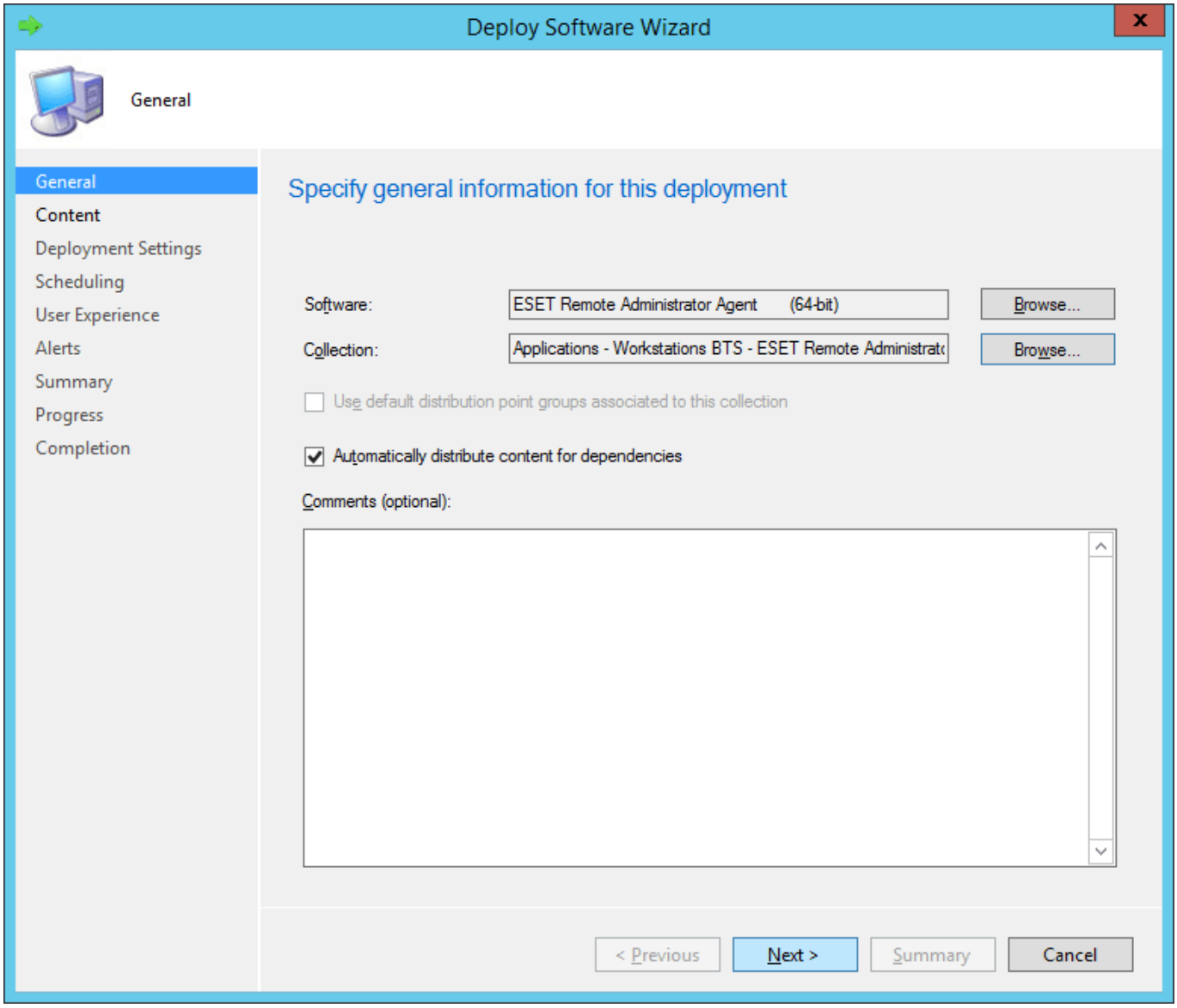


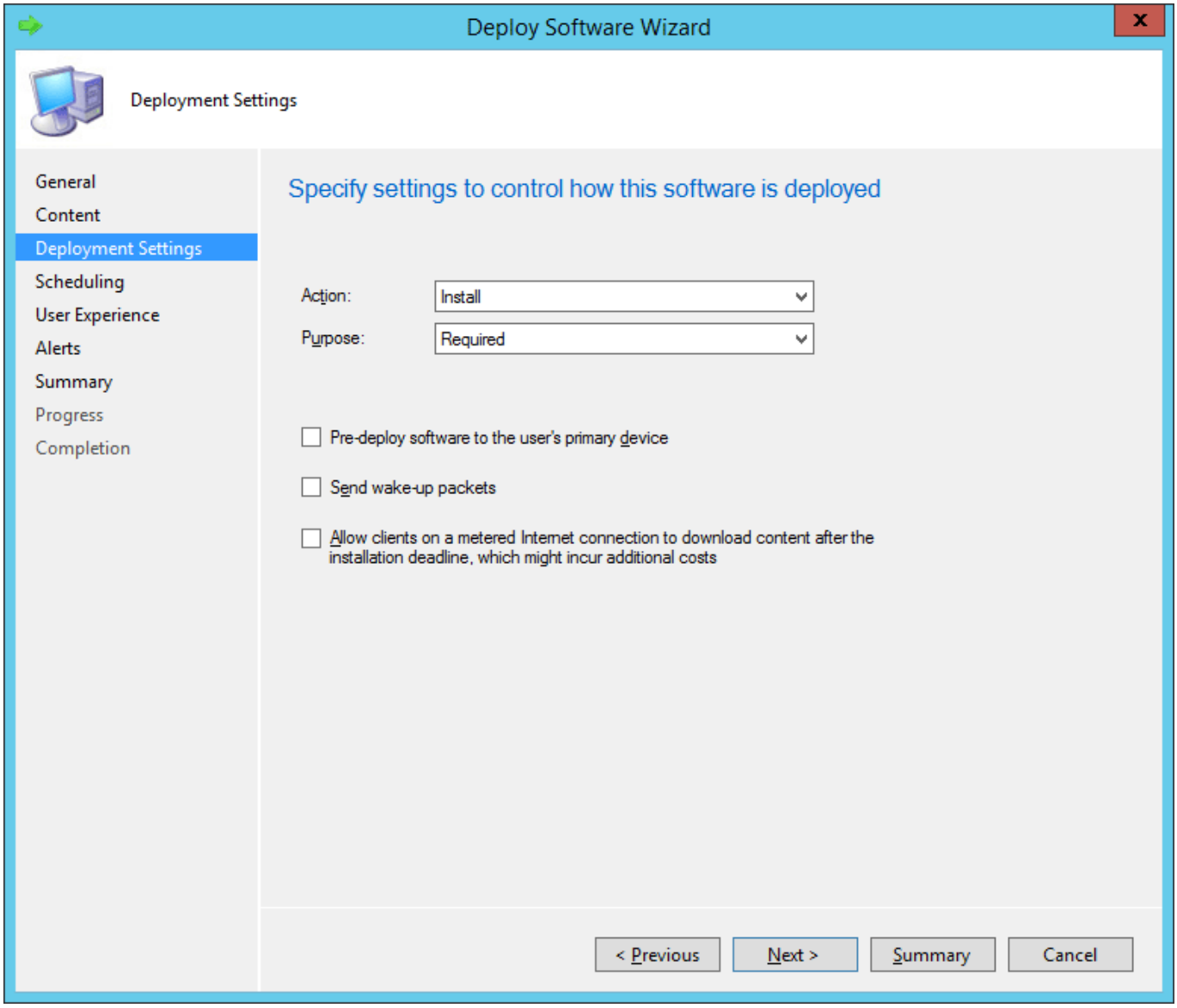
7. Haga clic con el botón derecho del ratón en la aplicación y elija **Implementar**. Siga el asistente y elija la colección y el destino en los que desea implementar el agente.

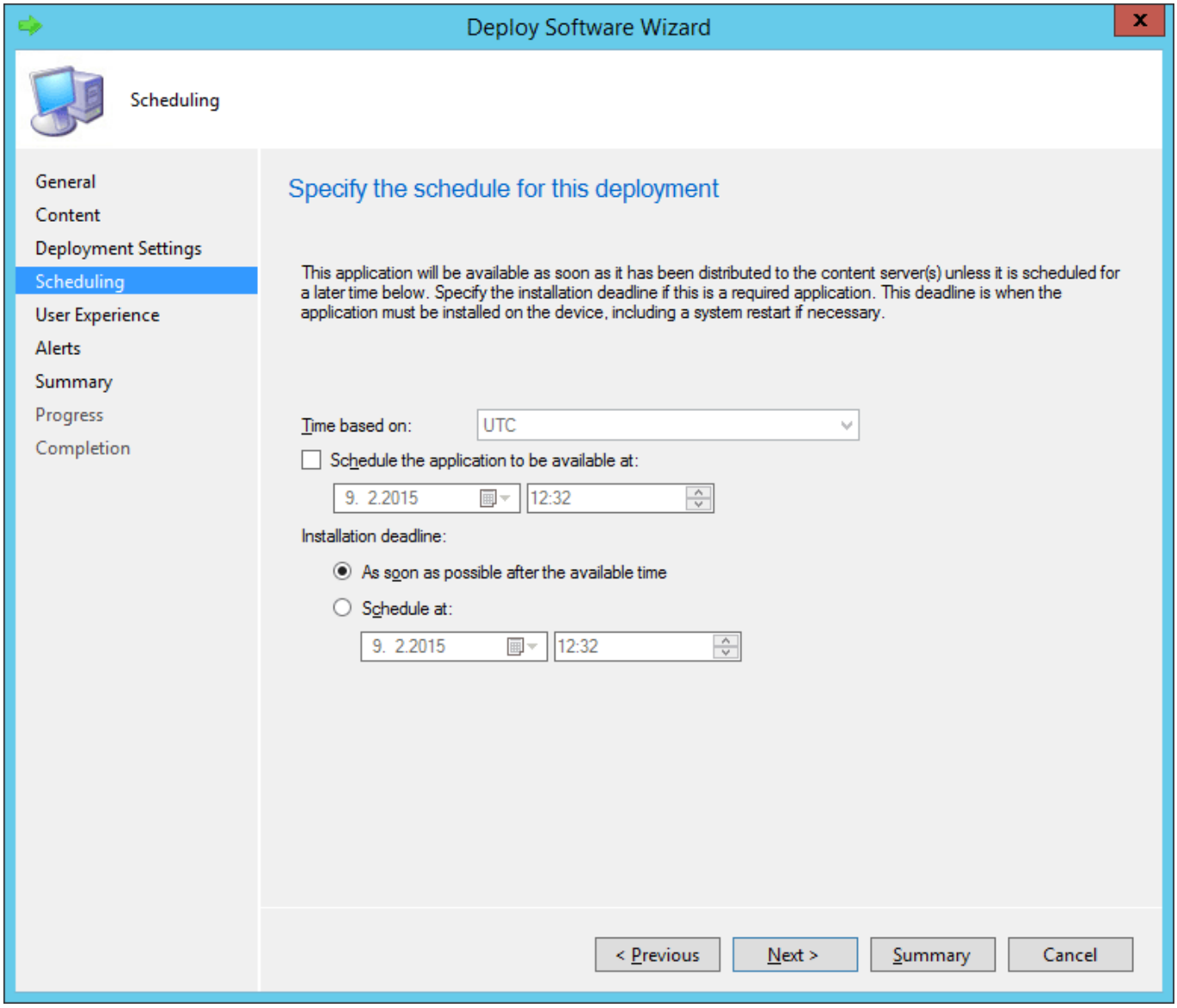

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

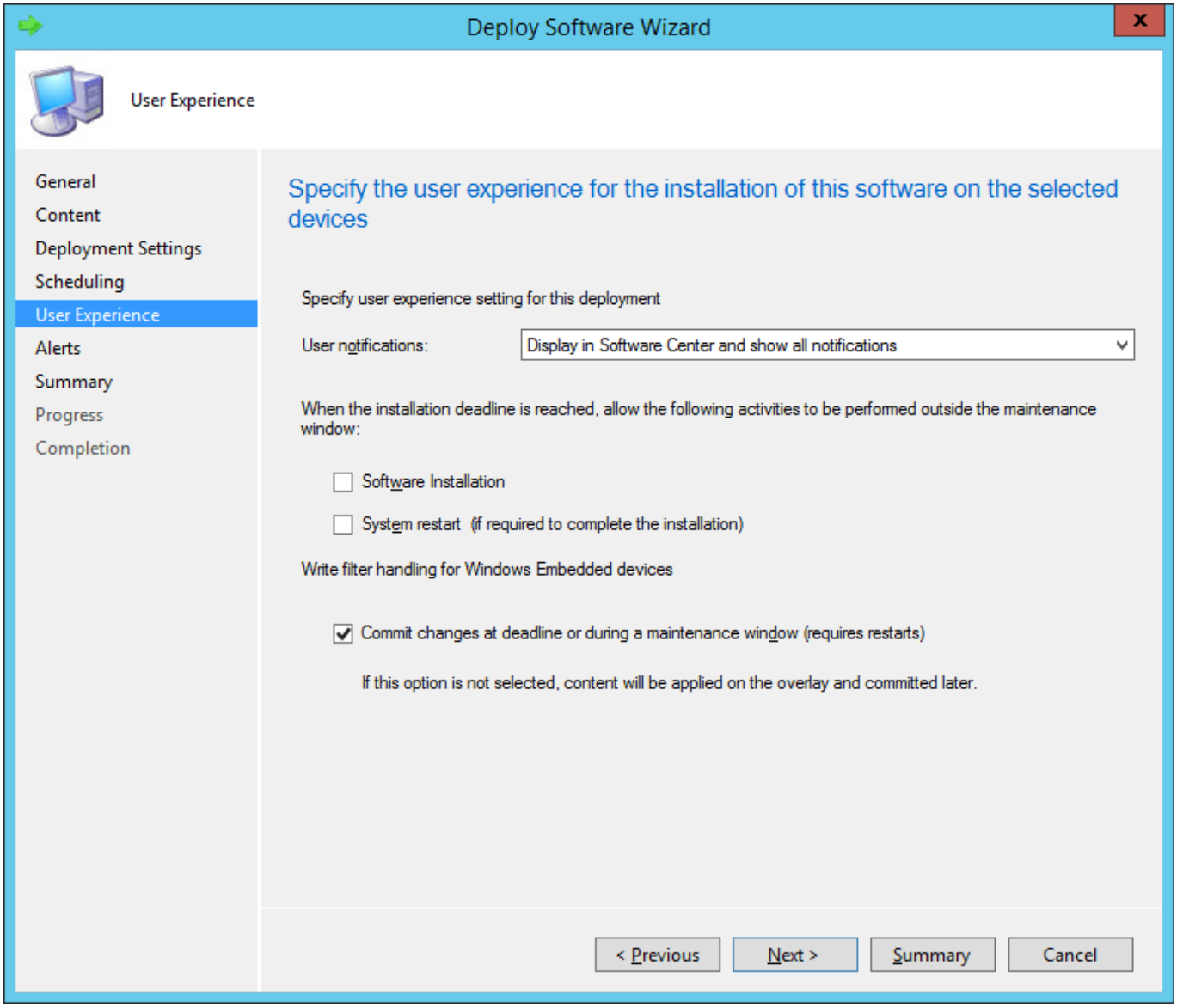

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with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

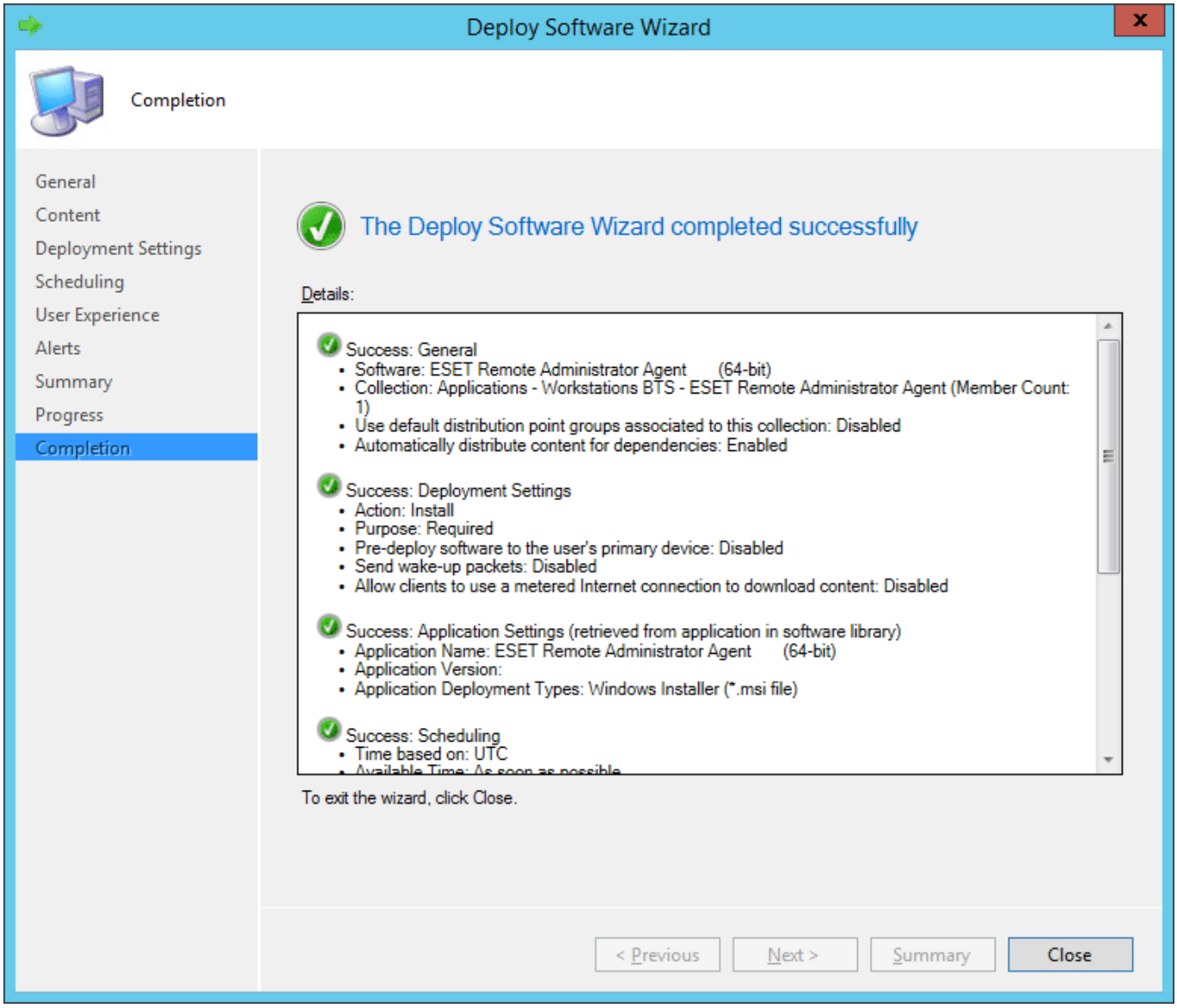

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution 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

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

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

La Remote Deployment Tool de ESET está dedicada a implementar ESET Management Agent solo en ordenadores cliente con sistemas operativos Microsoft Windows compatibles.

Para implementar el ESET Management Agent y el producto de seguridad de ESET utilizando este método, siga los pasos indicados a continuación:

1. Descargue ESET Remote Deployment Tool del sitio web de ESET.

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

3. Ejecute la Herramienta de implementación remota de ESET en el ordenador cliente.

4. Seleccione una de las siguientes opciones de implementación:

    • Active Directory: tendrá que indicar las credenciales de Active Directory. Esta opción incluye una exportación de la estructura de Active Directory para su posterior importación en ESET PROTECT On-Prem.

    • Análisis de red: tendrá que proporcionar rangos de IP para analizar los ordenadores de la red.

    • Importar lista: tendrá que proporcionar una lista de los nombres de host o las direcciones IP.

    • Agregar ordenadores manualmente: tendrá que proporcionar una lista de los nombres de host o las direcciones IP manualmente.

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

Requisitos previos de la Herramienta de implementación remota de ESET

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

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

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

Seleccionar ordenadores en Active Directory

Para continuar con la implementación de ESET Management Agent y el producto de seguridad de ESET desde el capítulo anterior:

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

2. Introduzca el **servidor Active Directory** con la dirección IP o el nombre de host y el **Puerto** a los que quiera conectarse.

3. Introduzca el **Nombre de usuario** y la **Contraseña** para iniciar sesión en el servidor Active Directory. Si marca la casilla situada junto a **Usar las credenciales de usuario actuales**, las credenciales de inicio de sesión se introducirán automáticamente.

4. También puede marcar la casilla situada junto a **Exportar lista de ordenadores para ESET PROTECT** si quiere exportar la estructura de Active Directory para posteriores importaciones a ESET PROTECT On-Prem.

Si un ordenador está en Active Directory, haga clic en **Siguiente** para iniciar sesión automáticamente en el controlador de dominio predeterminado.

5. Marque la casilla situada junto a los ordenadores que quiera agregar y haga clic en **Siguiente**. Marque la casilla de verificación **Incluir subgrupos** para enumerar todos los ordenadores del grupo seleccionado.

6. Se mostrarán los ordenadores seleccionados para la 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).

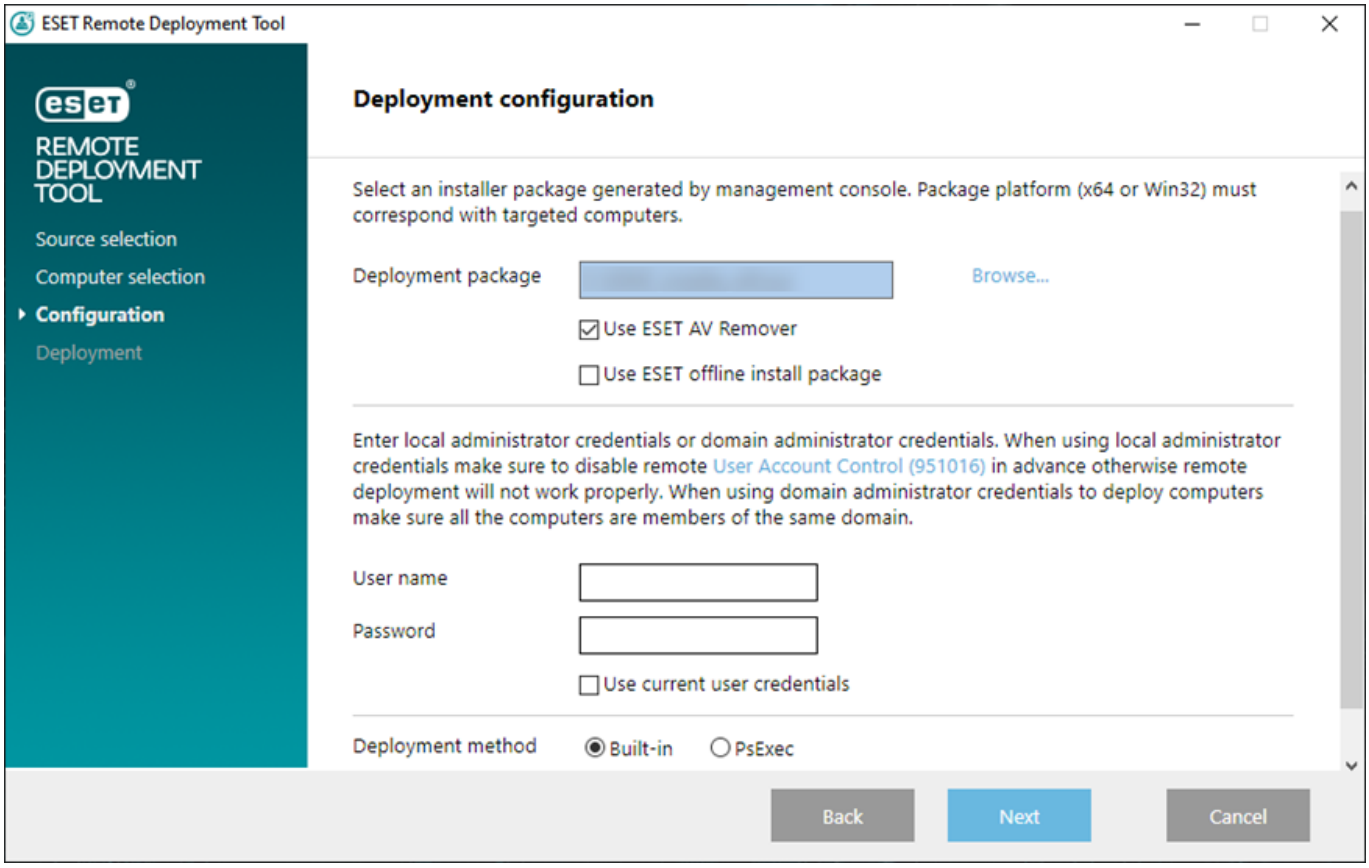
7. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

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

- Si no tiene instalada otras aplicaciones seguridad en el ordenador local, desmarque la casilla situada junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar determinadas aplicaciones.

8. Especifique las credenciales de inicio de sesión de los ordenadores de destino. Si los ordenadores forman parte de un dominio, especifique las **credenciales de administrador del dominio**. Si inicia sesión con **credenciales de administración local**, es necesario desactivar el control de cuentas de usuario remoto en los ordenadores de destino. También puede marcar la casilla situada junto a **Usar las credenciales de usuario actuales**, y las credenciales de inicio de sesión se introducirán automáticamente.

9. El **método de implementación** se utiliza para ejecutar programas en ordenadores remotos. El método **Integrado** es un ajuste predeterminado, y es compatible con los mensajes de error de Windows. **PsExec** es una herramienta externa, alternativa al método integrado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

10. Cuando la instalación comience, se mostrará "Éxito". Haga clic en **Finalizar** para terminar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de los ordenadores que han fallado. Haga clic en **Examinar** junto al campo **Exportar ordenadores fallidos**, seleccione el archivo *.txt* en el que quiere guardar la lista y, a continuación, haga clic en **Exportar ordenadores 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 diversos motivos. Si tiene cualquier problema con la implementación, lea el capítulo Resolución de problemas o Situaciones de ejemplo de implementación de ESET Management Agent verificadas.

Analizar la red local en busca de ordenadores

Para continuar con la implementación de ESET Management Agent y el producto de seguridad de ESET desde el capítulo anterior:

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

2. Introduzca los **Rangos de IP** de la red con el formato *10.100.100.10-10.100.100.250*

3. Seleccione uno de los siguientes **métodos de análisis**:

- **Análisis ping**: busca ordenadores cliente con el comando `ping`.

> Algunos ordenadores cliente de esta red no tienen que enviar una respuesta al comando `ping` porque el cortafuegos bloquea la conexión.

- **Análisis de puerto**: utiliza números de puerto para analizar la red. Consulte los puertos compatibles utilizados para la implementación remota de instancias de ESET Management Agent. El número de puerto predeterminado es el 445.

4. Para buscar ordenadores en la red, haga clic en **Iniciar análisis**.

5. Marque la casilla situada junto a los ordenadores que quiera agregar y haga clic en **Siguiente**.

6. Se mostrarán los ordenadores seleccionados para la 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).

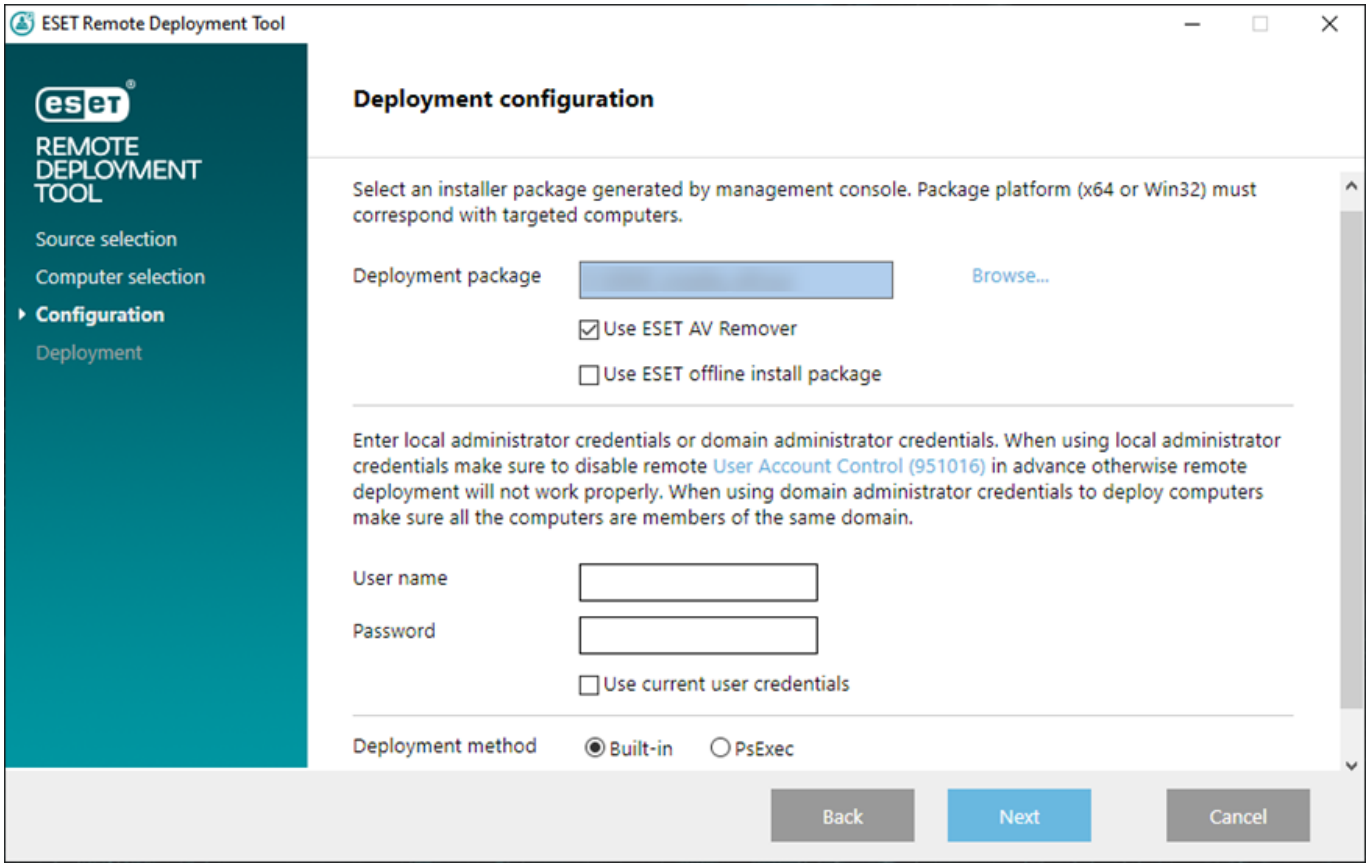
7. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

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

- Si no tiene instalada otras aplicaciones seguridad en el ordenador local, desmarque la casilla situada junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar determinadas aplicaciones.

8. Especifique las credenciales de inicio de sesión de los ordenadores de destino. Si los ordenadores forman parte de un dominio, especifique las **credenciales de administrador del dominio**. Si inicia sesión con **credenciales de administración local**, es necesario desactivar el control de cuentas de usuario remoto en los ordenadores de destino. También puede marcar la casilla situada junto a **Usar las credenciales de usuario actuales**, y las credenciales de inicio de sesión se introducirán automáticamente.

9. El **método de implementación** se utiliza para ejecutar programas en ordenadores remotos. El método **Integrado** es un ajuste predeterminado, y es compatible con los mensajes de error de Windows. **PsExec** es una herramienta externa, alternativa al método integrado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

10. Cuando la instalación comience, se mostrará "Éxito". Haga clic en **Finalizar** para terminar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de los ordenadores que han fallado. Haga clic en **Examinar** junto al campo **Exportar ordenadores fallidos**, seleccione el archivo *.txt* en el que quiere guardar la lista y, a continuación, haga clic en **Exportar ordenadores 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 diversos motivos. Si tiene cualquier problema con la implementación, lea el capítulo Resolución de problemas o Situaciones de ejemplo de implementación de ESET Management Agent verificadas.

Importar una lista de ordenadores

Para continuar con la implementación de ESET Management Agent y el producto de seguridad de ESET desde el capítulo anterior:

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

2. Seleccione una de las siguientes opciones:

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

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

3. Haga clic en **Examinar** y seleccione el archivo que desee cargar; a continuación, haga clic en **Siguiente**.

4. Se mostrarán los ordenadores seleccionados para la 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).

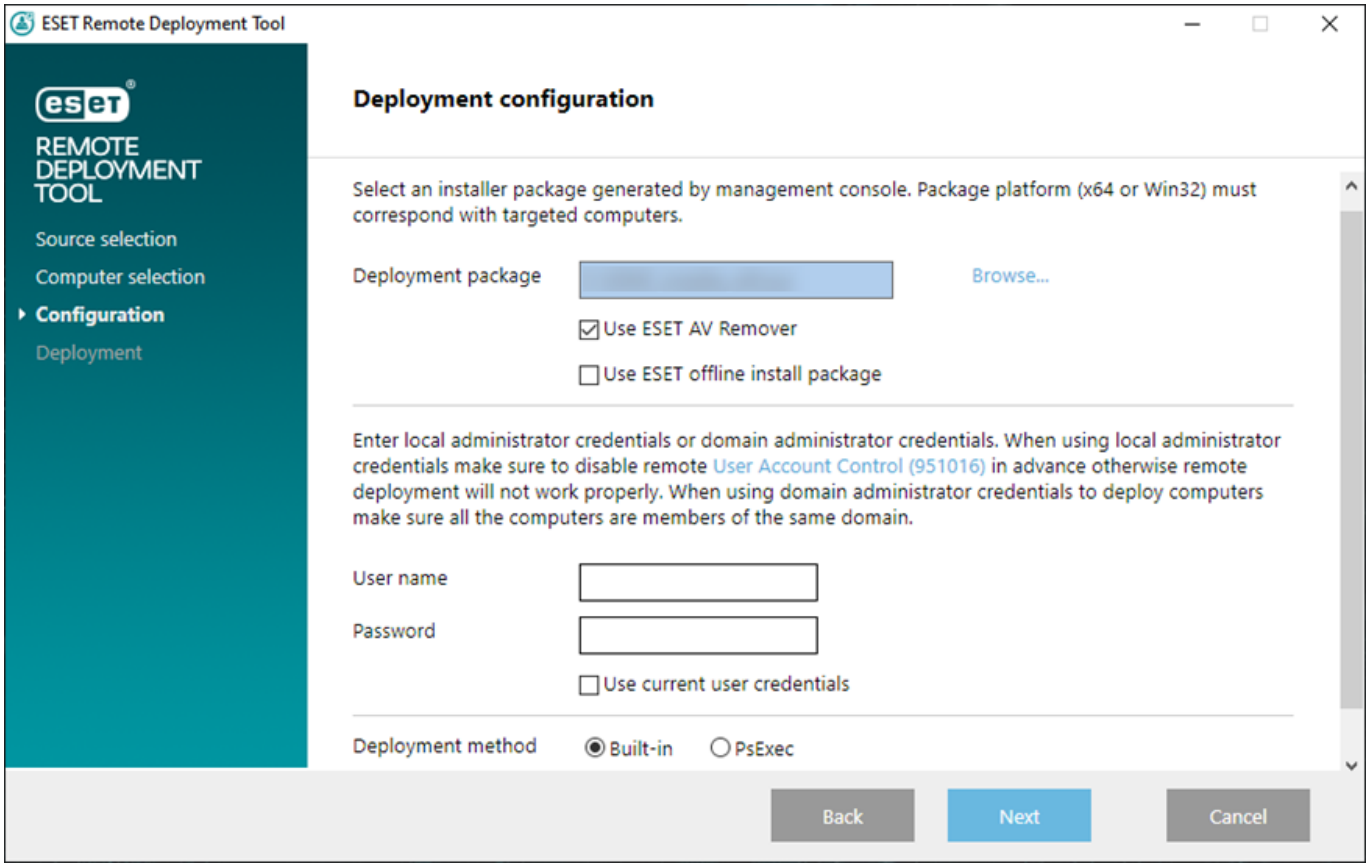
5. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

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

   • Si no tiene instalada otras aplicaciones seguridad en el ordenador local, desmarque la casilla situada junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar determinadas aplicaciones.

6. Especifique las credenciales de inicio de sesión de los ordenadores de destino. Si los ordenadores forman parte de un dominio, especifique las **credenciales de administrador del dominio**. Si inicia sesión con **credenciales de administración local**, es necesario desactivar el control de cuentas de usuario remoto en los ordenadores de destino. También puede marcar la casilla situada junto a **Usar las credenciales de usuario actuales**, y las credenciales de inicio de sesión se introducirán automáticamente.

7. El **método de implementación** se utiliza para ejecutar programas en ordenadores remotos. El método **Integrado** es un ajuste predeterminado, y es compatible con los mensajes de error de Windows. **PsExec** es una herramienta externa, alternativa al método integrado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

8. Cuando la instalación comience, se mostrará "Éxito". Haga clic en **Finalizar** para terminar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de los ordenadores que han fallado. Haga clic en **Examinar** junto al campo **Exportar ordenadores fallidos**, seleccione el archivo *.txt* en el que quiere guardar la lista y, a continuación, haga clic en **Exportar ordenadores 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 diversos motivos. Si tiene cualquier problema con la implementación, lea el capítulo Resolución de problemas o Situaciones de ejemplo de implementación de ESET Management Agent verificadas.

Agregar ordenadores manualmente

Para continuar con la implementación de ESET Management Agent y el producto de seguridad de ESET desde el capítulo anterior:

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

2. Introduzca los nombres de host o las direcciones IP manualmente y, a continuación, haga clic en **Siguiente**. Cada dirección IP o nombre de host debe estar en una línea nueva.

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

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

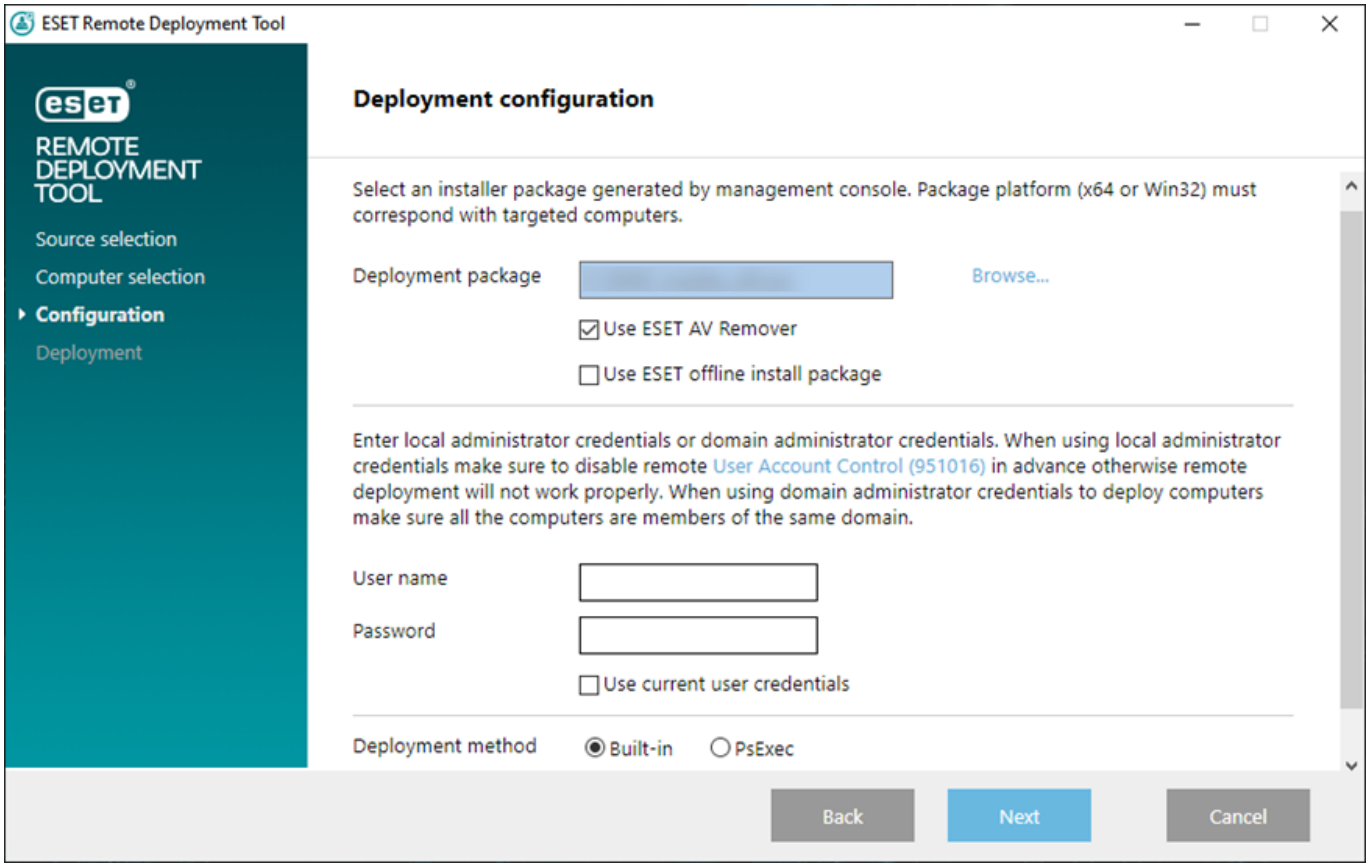
4. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

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

- Si no tiene instalada otras aplicaciones seguridad en el ordenador local, desmarque la casilla situada junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar determinadas aplicaciones.

5. Especifique las credenciales de inicio de sesión de los ordenadores de destino. Si los ordenadores forman parte de un dominio, especifique las **credenciales de administrador del dominio**. Si inicia sesión con **credenciales de administración local**, es necesario desactivar el control de cuentas de usuario remoto en los ordenadores de destino. También puede marcar la casilla situada junto a **Usar las credenciales de usuario actuales**, y las credenciales de inicio de sesión se introducirán automáticamente.

6. El **método de implementación** se utiliza para ejecutar programas en ordenadores remotos. El método **Integrado** es un ajuste predeterminado, y es compatible con los mensajes de error de Windows. **PsExec** es una herramienta externa, alternativa al método integrado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

7. Cuando la instalación comience, se mostrará "Éxito". Haga clic en **Finalizar** para terminar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de los ordenadores que han fallado. Haga clic en **Examinar** junto al campo **Exportar ordenadores fallidos**, seleccione el archivo *.txt* en el que quiere guardar la lista y, a continuación, haga clic en **Exportar ordenadores 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 diversos motivos. Si tiene cualquier problema con la implementación, lea el capítulo Resolución de problemas o Situaciones de ejemplo de implementación de ESET Management Agent verificadas.

ESET Remote Deployment Tool: resolución de problemas

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

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

La implementación puede fallar con diversos mensajes de error y debido a diversos motivos indicados en la siguiente tabla:

Mensaje de error	Posibles causas
No se ha encontrado la ruta de acceso de red (código de error 0x35)	• El cliente no está accesible en la red, el cortafuegos bloquea la comunicación • Los puertos de entrada 135, 137, 138, 139 y 445 no están abiertos en el cortafuegos en el cliente o en el cortafuegos de Windows: no se utiliza la excepción que permite el uso compartido de archivos e impresoras en la entrada • El nombre de host del cliente no se pudo resolver, utilice nombres de ordenadores FQDN válidos
Acceso denegado (código de error 0x5) **El nombre de usuario o la contraseña son incorrectos** (código de error 0x52e)	• Al realizar la implementación desde un servidor unido a un dominio en un cliente unido a dicho dominio, utilice credenciales de un usuario que sea miembro del grupo de administradores de dominio en formato **Dominio\Admin de dominio** • Al realizar la implementación desde un servidor en un cliente que no esté en el mismo dominio, desactive los filtros de control de cuentas de usuario remotos en el ordenador de destino. • Al realizar la implementación desde un servidor en un cliente que no esté en el mismo dominio, utilice credenciales de un usuario local que sea miembro del grupo de administradores en formato Admin. El nombre del ordenador de destino se anexará automáticamente al inicio de sesión. • No existe una contraseña para la cuenta de administrador • Derechos de acceso insuficientes • El uso compartido administrativo ADMIN$ no está disponible • El uso compartido administrativo IPC$ no está disponible • El uso compartido simple de archivos está activado
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 bits o 32 bits) en ESET PROTECT Web Console
El periodo de tiempo de espera de semáforo ha finalizado	El cliente no puede acceder al recurso compartido de red con el paquete de implementación porque SMB 1.0 está desactivado en el recurso compartido.

Siga los pasos de solución de problemas de acuerdo con la posible causa:

Posible causa	Pasos de resolución de problemas
El cliente no está accesible en la red	Haga ping al cliente desde el ESET PROTECT Server; si obtiene respuesta, trate de iniciar sesión en la máquina cliente de forma remota (por ejemplo, a través del escritorio remoto).
El cortafuegos bloquea la comunicación	Compruebe la configuración del cortafuegos en el servidor y el cliente, así como cualquier otro cortafuegos que exista entre estas dos máquinas (si corresponde). Tras una implementación correcta, los puertos 2222 y 2223 no están abiertos en el cortafuegos. Asegúrese de que estos puertos estén abiertos en el firewall entre los dos equipos (cliente y servidor).
El nombre de host del cliente no se pudo resolver	Las posibles soluciones a los problemas de DNS pueden ser, entre otras: • Utilizar el comando `nslookup` de la dirección IP y el nombre de host del servidor o los clientes que tienen problemas de implementación del agente. Los resultados deben coincidir con la información de la máquina. Por ejemplo, un `nslookup` de un nombre de host debe resolver a la dirección IP y mostrarse un comando `ipconfig` en el host en cuestión. El comando `nslookup` se tendrá que ejecutar en los clientes y el servidor. • Examine manualmente los registros DNS en busca de duplicados.
No existe una contraseña para la cuenta de administrador	Establezca la contraseña correcta para la cuenta de administrador (no utilice una contraseña en blanco).
Derechos de acceso insuficientes	Pruebe a utilizar las credenciales de administrador de dominio al crear una tarea de implementación del agente. Si la máquina cliente está en un grupo de trabajo, utilice la cuenta de administrador local en ese ordenador en particular. La cuenta de usuario del Administrador debe estar activada para ejecutar la tarea de implementación del agente. Puede crear un usuario local que sea miembro del grupo de administradores o activar la cuenta de administrador local integrada. Para activar la cuenta de usuario del administrador: 1.Abra el símbolo de sistema administrativo 2.Escribir el siguiente comando: `net user administrator /active:yes`
El uso compartido del recurso administrativo ADMIN$ no está 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 uso compartido del recurso administrativo IPC$ no está disponible	Compruebe que el servidor pueda acceder a IPC$ con el siguiente comando desde el símbolo del sistema del servidor: `net use \\clientname\IPC$` donde `clientname` es el nombre del ordenador de destino.
El uso compartido simple de archivos está activado	Si está recibiendo el mensaje de error **Acceso denegado** y su entorno es mixto (contiene un dominio y un grupo de trabajo), desactive **Uso compartido simple de archivos** o **Asistente para uso compartido** en todas las máquinas que tengan problemas con la implementación del agente. Por ejemplo, en Windows 11 haga lo siguiente: • Haga clic en **Inicio**, escriba `Explorador de archivos` en el cuadro **Buscar** y, a continuación, haga clic en **Opciones del explorador de archivos**. Haga clic en la ficha **Ver** y, en el cuadro de **Configuración avanzada**, desplácese por la lista y cancele la selección de la casilla de verificación junto a **Asistente para uso compartido**.

Protección del agente

ESET Management Agent se protege mediante un mecanismo de autodefensa integrado. Esta función ofrece las siguientes ventajas:

- Protección contra modificación de las entradas del registro de ESET Management Agent (HIPS)

- Los archivos que pertenecen a ESET Management Agent no pueden modificarse, sustituirse, eliminarse ni alterarse (HIPS)
- El proceso de ESET Management Agent no puede cerrarse
- El servicio de ESET Management Agent no se puede detener, pausar, desactivar, desinstalar ni poner en riesgo de ningún otro modo

Parte de la protección la cubre la función HIPS incluida en su producto de ESET.

Para garantizar la protección total de ESET Management Agent, HIPS debe estar activado en un ordenador cliente.

Configuración de la protección por contraseña

Además de la autodefensa, puede proteger mediante contraseña el acceso a ESET Management Agent (solo disponible para Windows). Para configurar una contraseña de ESET Management Agent debe crear la correspondiente política para ESET Management ERA Agent.

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

Configuración de ESET Management Agent

Puede configurar los ajustes específicos de ESET Management Agent mediante una política de ESET Management Agent.

Existen políticas predefinidas para ESET Management Agent. Por ejemplo, **Conexión**: conectar cada (intervalo de conexión del agente) o **Informe de aplicaciones**: informar de todas las aplicaciones instaladas (no solo de las aplicaciones de ESET). Para obtener más información sobre cómo aplicar una política basada en la ubicación, lea el ejemplo.

Haga clic en **Políticas** y despliegue **Políticas integradas > Agente de ESET Management** para modificar una política existente o crear una nueva.

Conexión

- **Los servidores se conectan a**: haga clic en Modificar lista de servidores para agregar los detalles de conexión de ESET PROTECT Server (nombre de host/IP y un número de puerto). Pueden especificarse varias instancias de ESET PROTECT Server. Esto puede resultar útil si, por ejemplo, ha cambiado la dirección IP de su ESET PROTECT Server o está realizando una migración.
- **Límite de datos**: elija el número máximo de bytes para enviar datos.
- **Intervalo de conexión**: elija un intervalo regular y especifique un valor temporal para el intervalo de conexión (también puede utilizar una expresión CRON).
- **Certificado**: puede administrar los certificados de igual de ESET Management Agent. Haga clic en **Cambiar certificado** y seleccione el certificado de ESET Management Agent que debe utilizar ESET Management Agent. Para obtener más información, consulte Certificados de igual.

Actualizaciones

• **Intervalo de actualización**: intervalo con el que se recibirán las actualizaciones. Seleccione un intervalo regular y configure los ajustes (también puede utilizar una expresión CRON).

• **Servidor de actualizaciones**: el servidor de actualizaciones desde el que ESET Management Agent recibe actualizaciones de los módulos.

• **Tipo de actualización**: seleccione el tipo de actualización que desea recibir. Elija entre actualizaciones periódicas o previas a su lanzamiento. No se recomienda seleccionar las actualizaciones de prueba para sistemas de producción, pues entraña ciertos riesgos.

• **Activar actualización automática:** esta opción se aplica a ESET Management Agent 8.1 y versiones posteriores. De forma predeterminada, ESET Management Agent se actualiza automáticamente a la versión compatible más reciente. Puede desactivar esta opción para desactivar la actualización automática de ESET Management Agent.

Configuración

La configuración protegida por contraseña es una función de protección de ESET Management Agent (disponible solo en Windows). Haga clic en **Establecer** junto a **Configuración protegida por contraseña** para activar la protección por contraseña de la configuración de ESET Management Agent.

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

Configuración avanzada

• **Proxy HTTP**: utilice un servidor proxy para facilitar el tráfico de Internet hacia los clientes de su red y la replicación del agente en ESET PROTECT Server.

o**Tipo de configuración del proxy**

■**Proxy global**: utilice un servidor proxy para la replicación del agente y para almacenar en caché los servicios de ESET (por ejemplo, actualizaciones).

■**Un proxy distinto por servicio**: utilice un proxy para la replicación del agente y otro para almacenar en caché los servicios de ESET (por ejemplo, actualizaciones).

o**Proxy global**: esta opción solo está disponible si la selecciona en **Tipo de configuración del proxy**. Haga clic en **Modificar** y configure los ajustes de su proxy.

Las dos opciones que se indican a continuación solo están disponibles si selecciona **Un proxy distinto por servicio**. También puede utilizar solo uno de los ajustes del proxy; por ejemplo, configure solo **Servicios de ESET** y deje **Replicación** desactivado. Marque o desmarque la casilla **Usar conexión directa si el proxy HTTP no está disponible** para activar o desactivar esta opción de reserva.

o**Replicación (para ESET Management Server)**: configure los ajustes de conexión para un proxy que conecta el agente con el servidor.

- **Servicios de ESET**: configure los ajustes de conexión para un proxy que almacenará en caché los servicios de ESET.

• **Llamada de activación**: ESET PROTECT Server puede ejecutar una replicación instantánea de ESET Management Agent en un equipo cliente a través de EPNS. Esto es útil cuando no quiere esperar al intervalo regular en el que el ESET Management Agent se conecta al ESET PROTECT Server. Por ejemplo, cuando desea que una tarea se ejecute de inmediato en los clientes o si desea que una política se aplique directamente.

• **Compatibilidad**: para permitir que el agente de ESET Management gestione los productos de ESET de la versión 5 y anteriores se debe establecer un puerto de escucha específico. Además, los productos de ESET deben estar configurados para reportar a este puerto y la dirección de ESET PROTECT Server debe ser **localhost**.

• **Sistema operativo**: utilice los conmutadores de alternancia para reportar determinada información o determinados problemas del ordenador cliente. Por ejemplo, active **Notificar aplicaciones instaladas que no sean de ESET** para activar la creación de informes de las aplicaciones de terceros instaladas.

• **Repositorio**: la ubicación del repositorio en el que se almacenan todos los archivos de instalación.

El repositorio predeterminado es **AUTOSELECT**.

• **Programa para la mejora del producto**: active o desactive la transmisión de informes de bloqueo y datos de telemetría anónimos a ESET.

• **Registro**: establezca el nivel de detalle del registro para determinar la cantidad de información que se recogerá y registrará de **Trazar** (datos meramente informativos) a **Fatal** (la información más importante). El archivo de registro de ESET Management Agent más reciente se encuentra en un ordenador cliente:

Asignar

Especifique los clientes que recibirán esta política. Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione el ordenador en el que quiera aplicar una política y haga clic en **Aceptar**.

Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**.

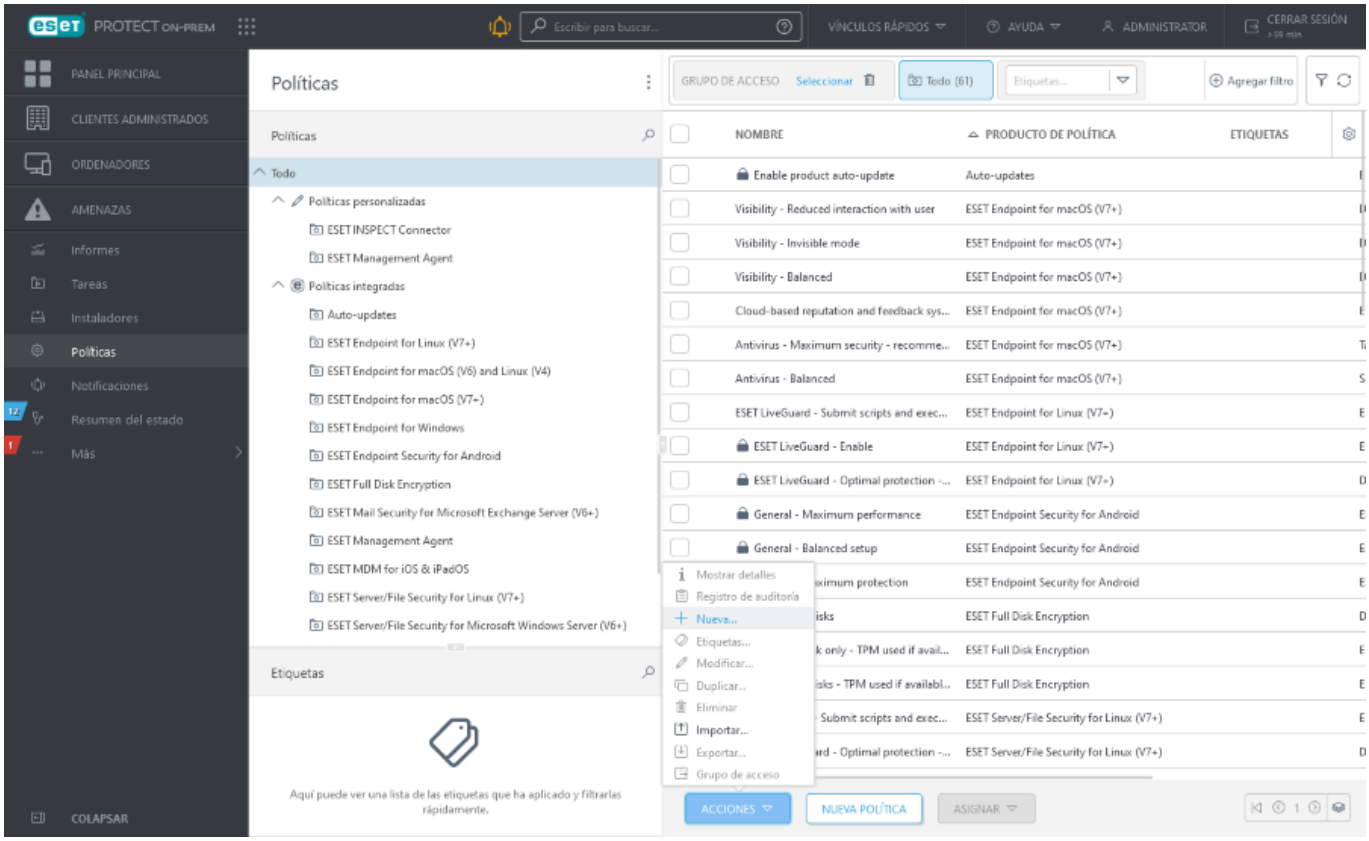
Puede solicitar la configuración del agente en un ordenador administrado para ver la configuración de política del agente aplicada: Haga clic en **Ordenadores**, haga clic en un ordenador > **Detalles** > **Configuración** > Solicitar configuración.

Crear una política para el intervalo de conexión de ESET

Management Agent

En este ejemplo vamos a crear una nueva política para el intervalo de conexión de ESET Management Agent. Este valor se debe modificar en función del tamaño de su infraestructura utilizando políticas después de instalar ESET PROTECT On-Prem e implementar los ESET Management Agent y los productos de punto de acceso de ESET en las máquinas cliente.

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

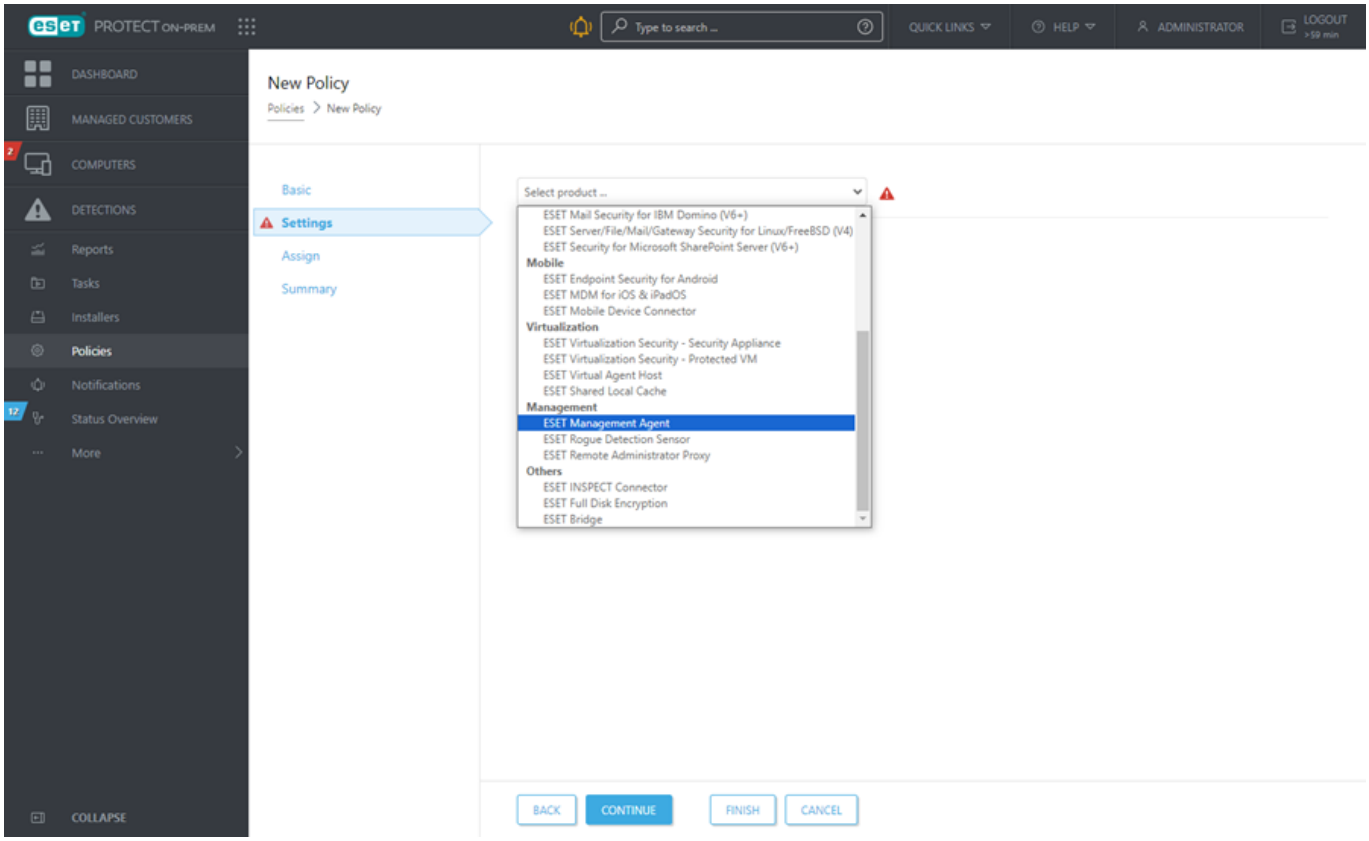


Básico

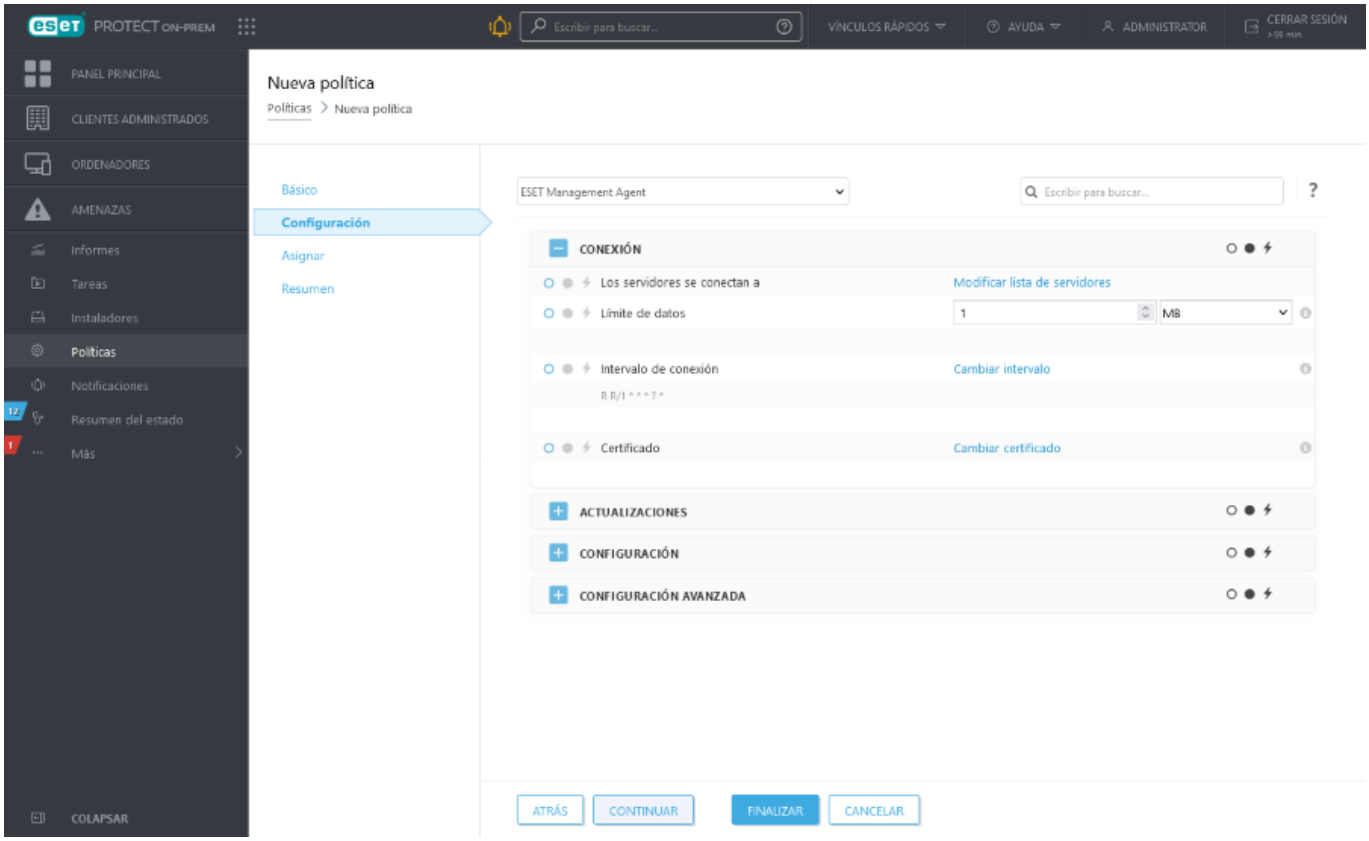
Introduzca un **nombre** para la nueva política (por ejemplo, "Intervalo de conexión del agente"). El campo **Descripción** es opcional.

Configuración

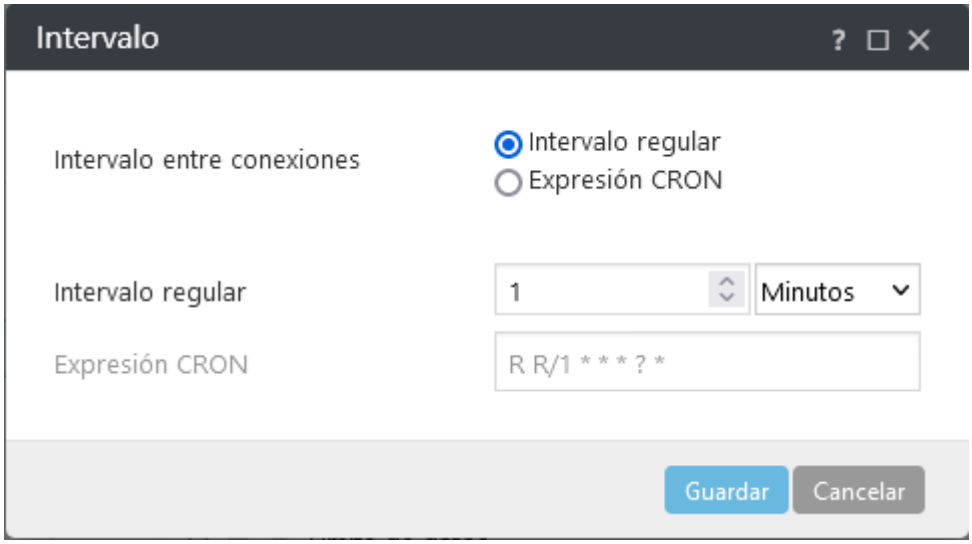
Seleccione **ESET Management Agent** en el menú desplegable **Producto**.



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

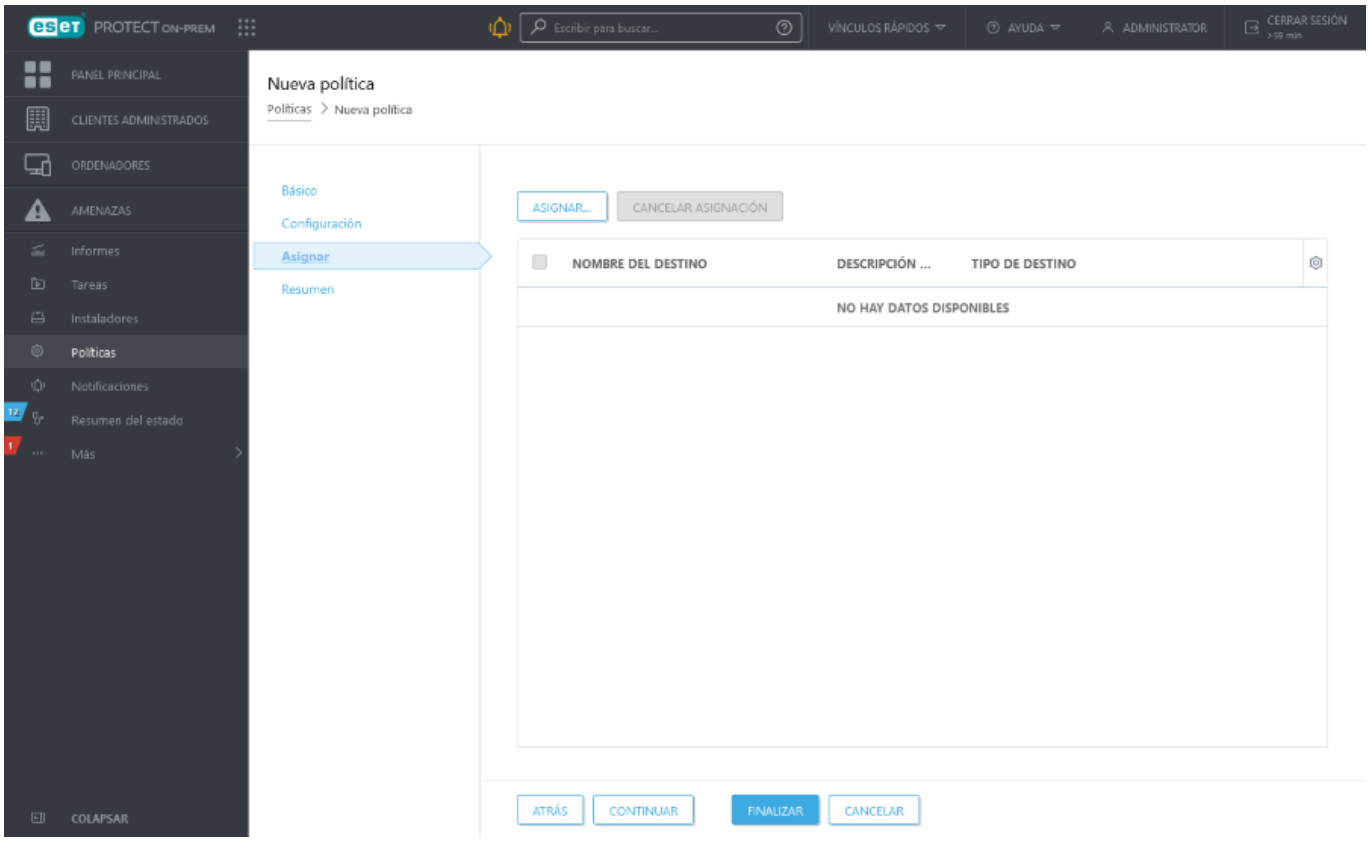


En el campo **Intervalo regular**, cambie el valor al intervalo que prefiera (60 segundos es el intervalo de replicación predeterminado de ESET Management Agent) y haga clic en **Guardar**.



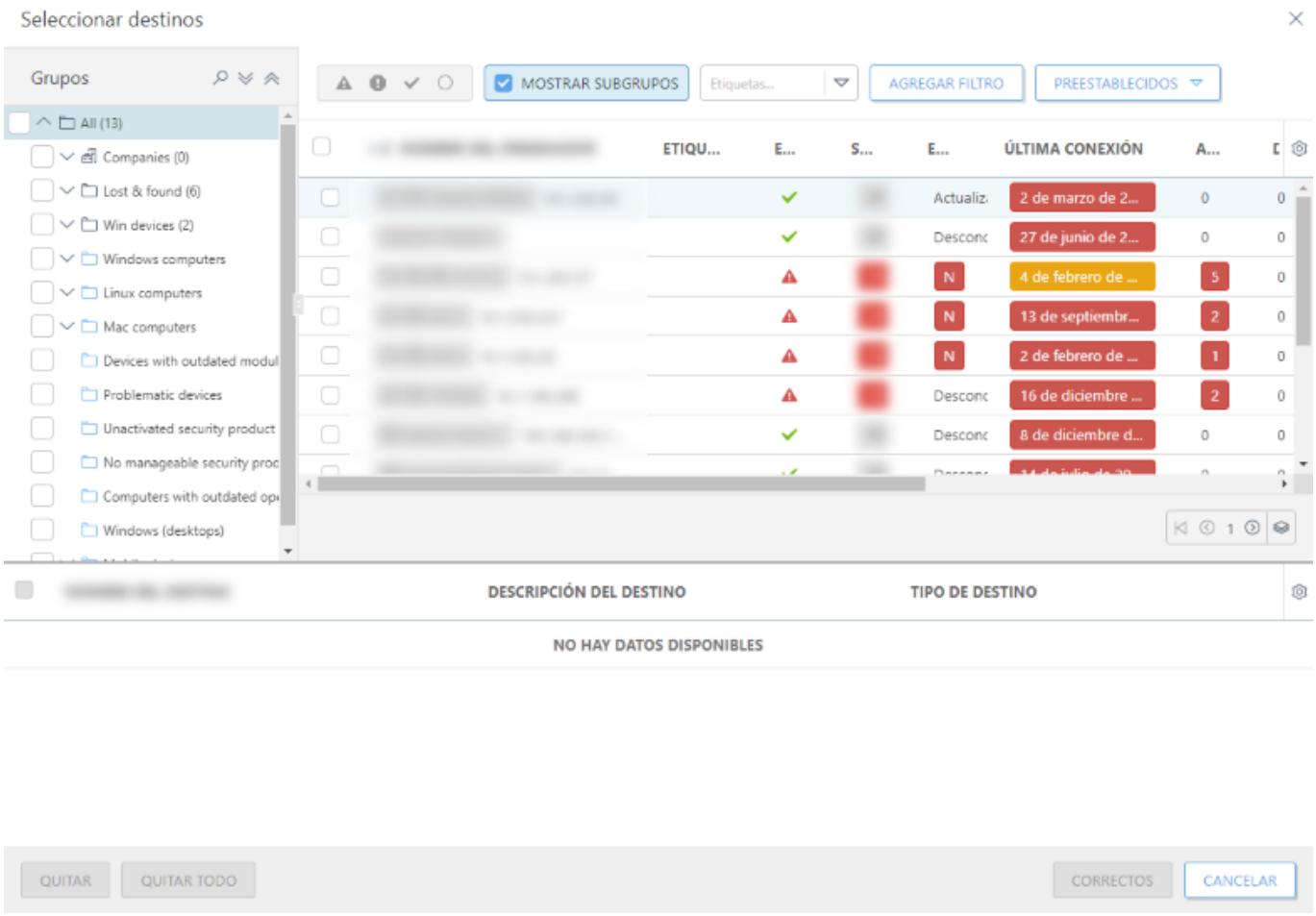
Asignar

Especifique los clientes (ordenadores individuales/dispositivos móviles o grupos enteros) que vayan a ser los destinatarios de esta política.



Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione los ordenadores o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**. La política se aplica a los destinos después de su siguiente conexión con ESET PROTECT Server (en función del intervalo de conexión del agente).

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

Crear una directiva para que ESET Management Agent se conecte al nuevo ESET PROTECT Server

Esta política le permite cambiar el comportamiento de ESET Management Agent modificando su configuración. La tarea indicada a continuación resulta especialmente útil al migrar máquinas cliente a un nuevo ESET PROTECT Server.

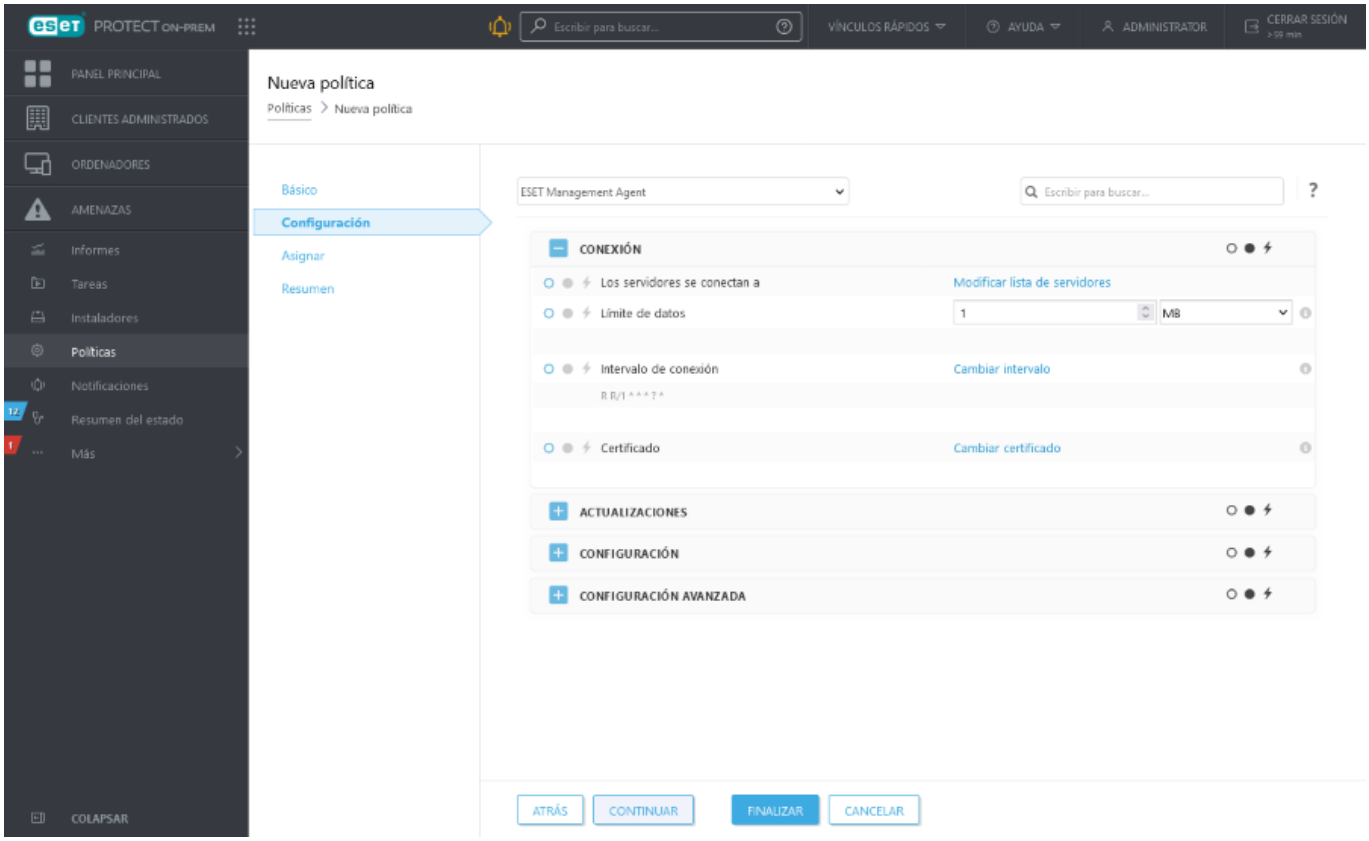
Cree una política nueva para configurar la dirección IP del nuevo ESET PROTECT Server y asigne la política a todos los ordenadores cliente. Seleccione **Políticas** > Crear **nueva**.

Básico

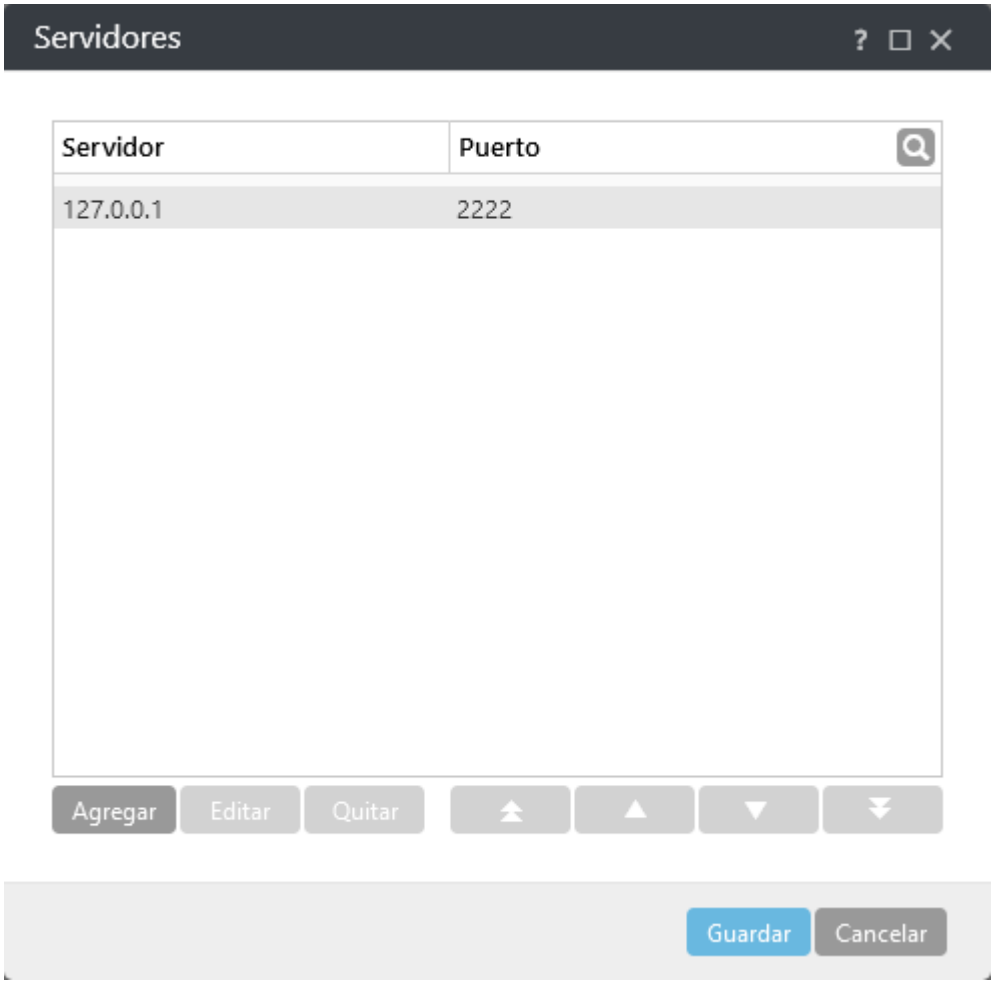
Escriba el **Nombre** de la nueva directiva. El campo **Descripción** es opcional.

Configuración

Seleccione **ESET Management Agent** en el menú desplegable, despliegue **Conexión** y haga clic en **Modificar lista de servidores** junto a **Servidores a los que conectar**.



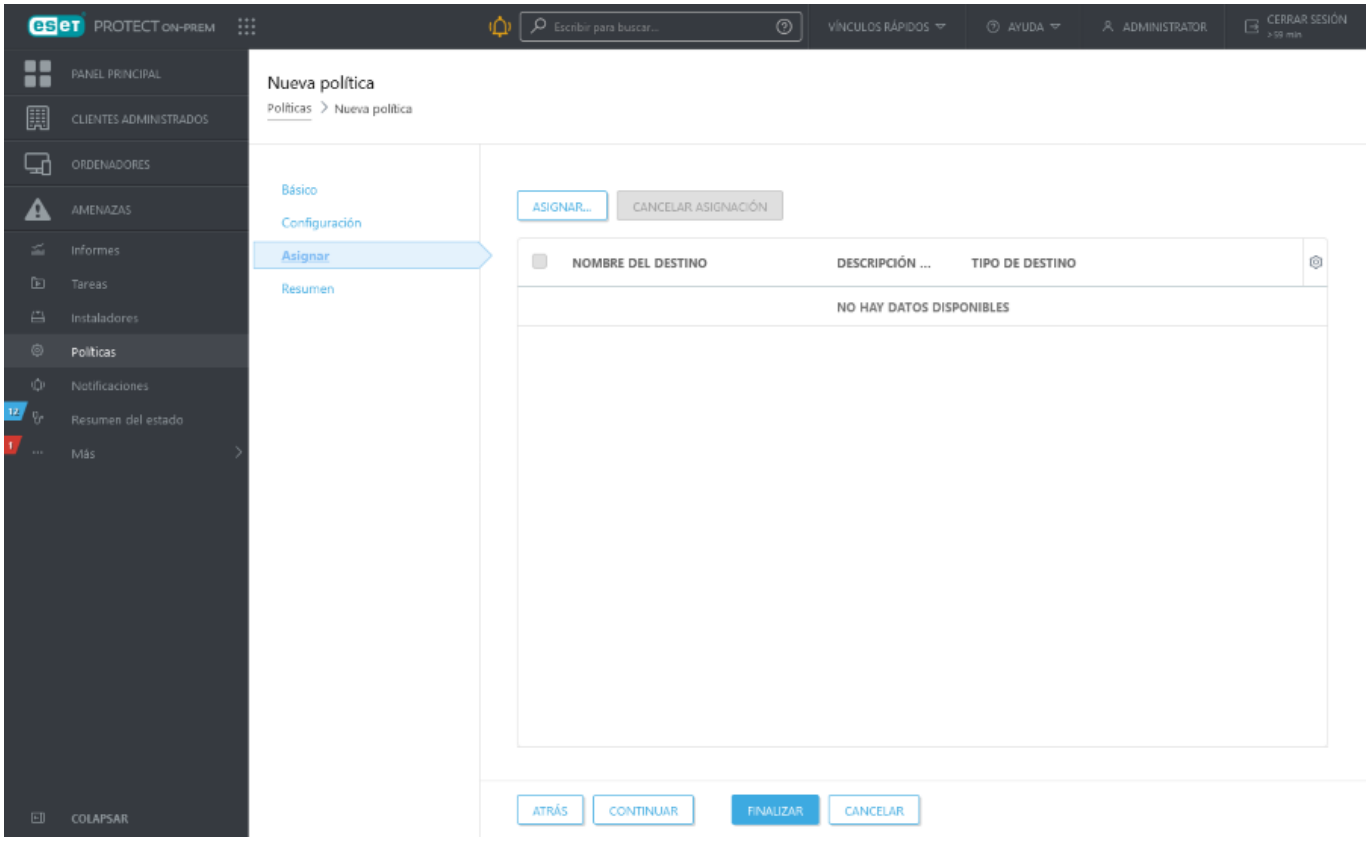
Se abrirá una ventana con una lista de direcciones de ESET PROTECT Server a las que ESET Management Agent puede conectarse. Haga clic en **Agregar** y escriba la dirección IP de su nuevo ESET PROTECT Server en el campo **Host**. Si está usando un puerto distinto del puerto 2222 predeterminado de ESET PROTECT Server, especifique su número de puerto personalizado.



Si tiene varias entradas en la lista, utilice los botones de flecha para modificar la prioridad de las instancias de ESET PROTECT Server. 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**.

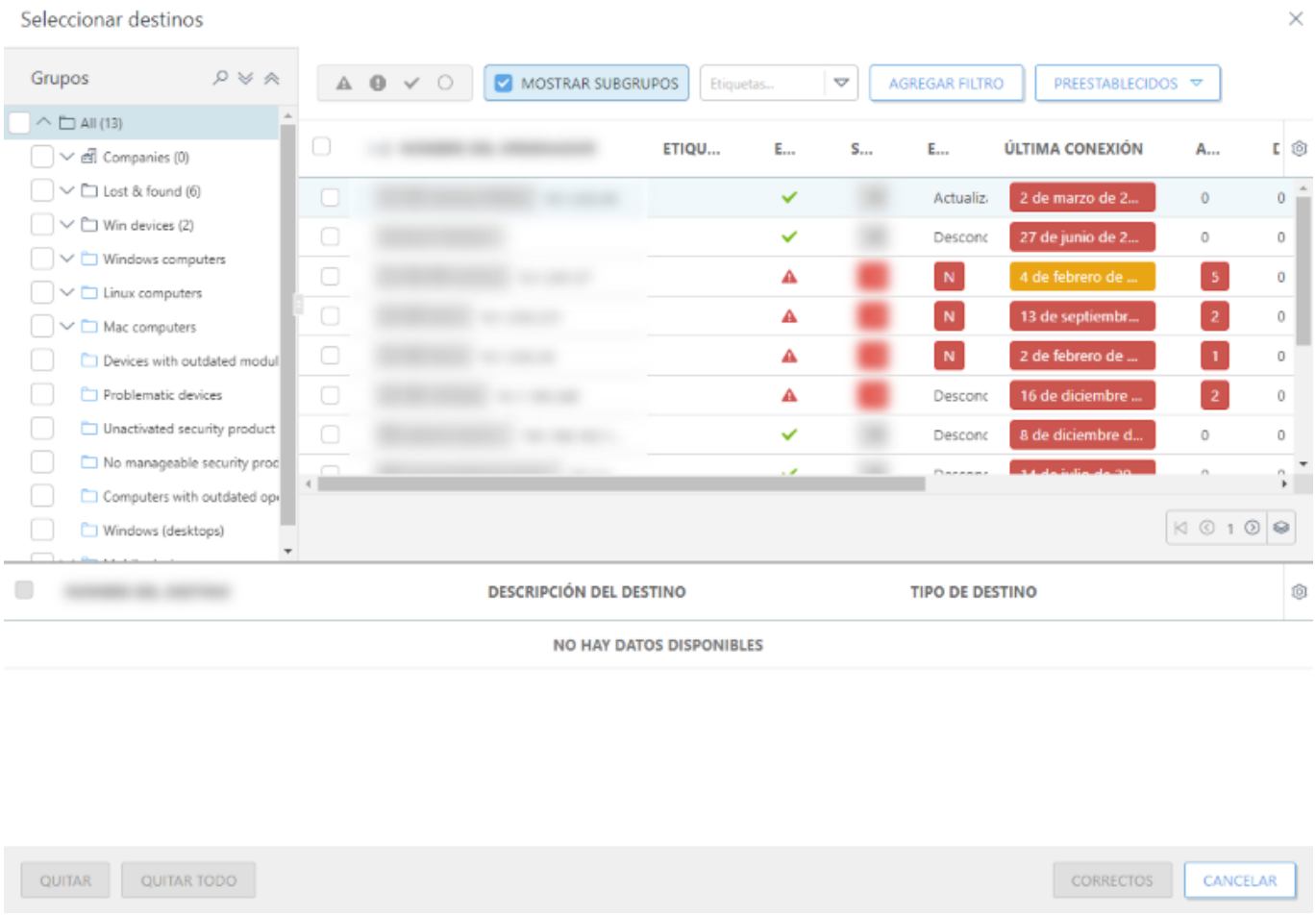
Asignar

Especifique los clientes (ordenadores individuales/dispositivos móviles o grupos enteros) que vayan a ser los destinatarios de esta política.



Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione los ordenadores o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**. La política se aplica a los destinos después de su siguiente conexión con ESET PROTECT Server (en función del intervalo de conexión del agente).

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

Crear una directiva para activar la protección por contraseña de ESET Management Agent

Siga los pasos indicados a continuación para crear una directiva nueva que aplicará una contraseña para proteger ESET Management Agent. Cuando se usa **Configuración de la protección por contraseña** ESET Management Agent no se puede desinstalar ni reparar sin una contraseña. Consulte Protección del agente para obtener más información.

Básico

Escriba el **Nombre** de esta directiva. El campo **Descripción** es opcional.

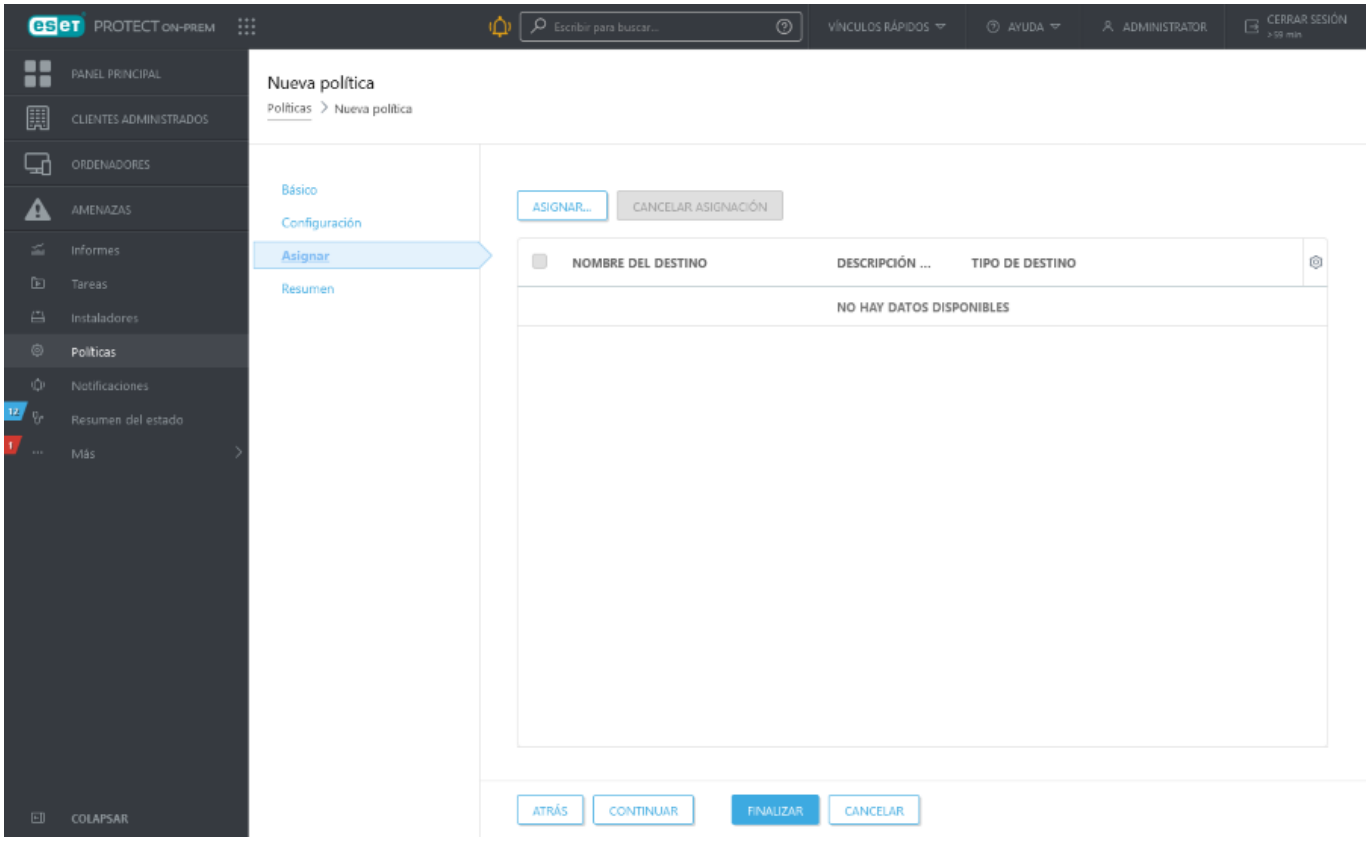
Configuración

Seleccione **ESET Management Agent** en la lista desplegable, despliegue **Configuración**, haga clic en **Establecer** junto a **Configuración de la protección por contraseña** y escriba la contraseña. Si alguien intenta desinstalar o reparar ESET Management Agent en un ordenador cliente, se le pedirá una contraseña.

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

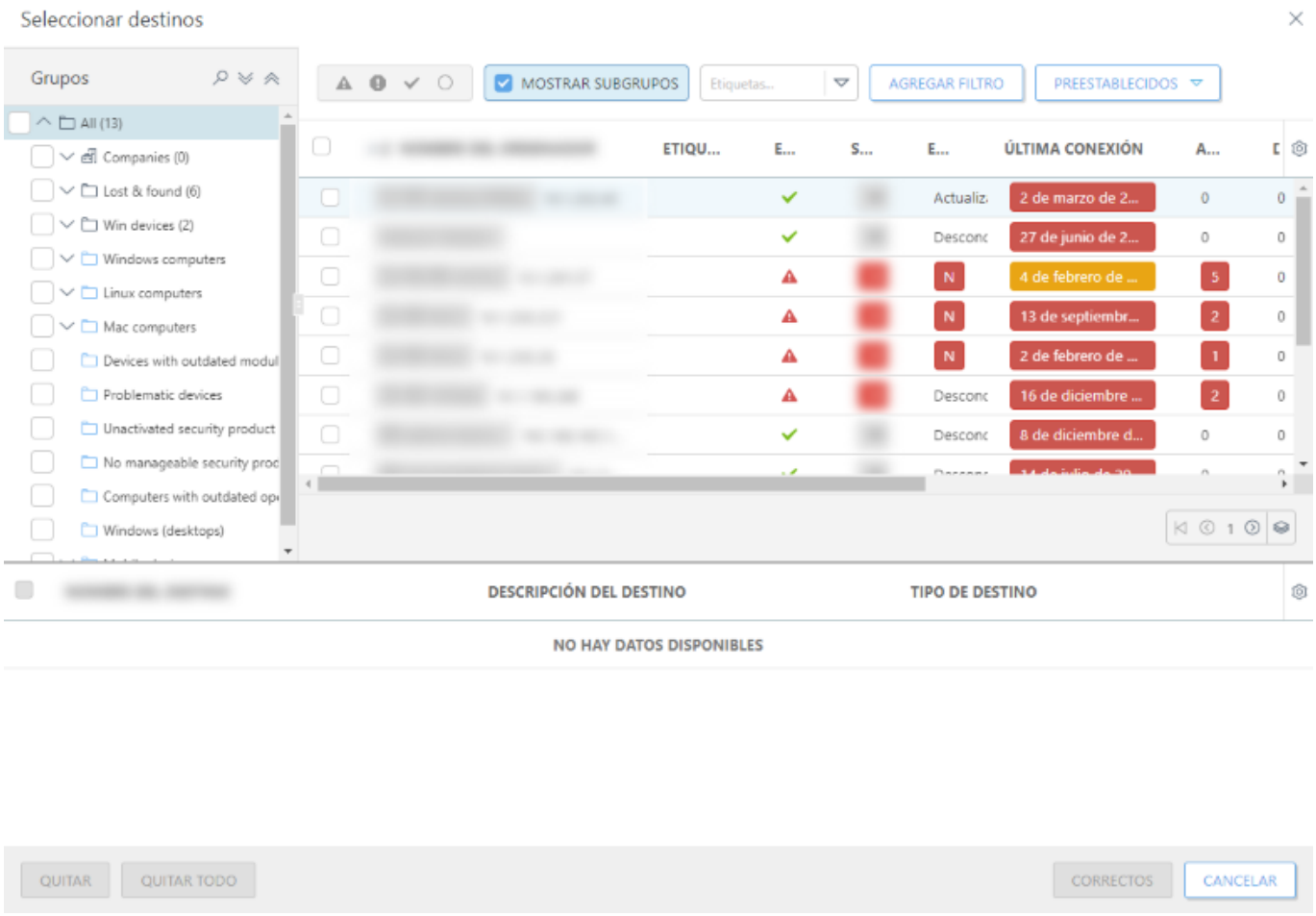
Asignar

Especifique los clientes (ordenadores individuales/dispositivos móviles o grupos enteros) que vayan a ser los destinatarios de esta política.



Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione los ordenadores o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**. La política se aplica a los destinos después de su siguiente conexión con ESET PROTECT Server (en función del intervalo de conexión del agente).

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

Resolución de problemas - Conexión con el agente

Cuando parezca que un ordenador cliente no se conecta con ESET PROTECT Server, se recomienda realizar los procedimientos de resolución de problemas del ESET Management Agent de forma local en el ordenador cliente.

De forma predeterminada, ESET Management Agent se sincroniza con ESET PROTECT Server cada minuto. Puede modificar este ajuste creando una nueva directiva para el intervalo de conexión con ESET Management Agent.

Consulte el archivo de registro más reciente de ESET Management Agent. 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 ESET Management Agent se encuentra en ejecución.

• **software-install.log**: protocolo de texto de la última tarea de instalación remota realizada por ESET Management Agent.

• **trace.log**: un informe detallado de toda la actividad de ESET Management Agent, incluidos los posibles errores registrados.

> Para habilitar el registro completo del ESET Management Agent en el archivo *trace.log*, cree un archivo ficticio llamado *traceAll* sin extensión en la misma carpeta que un *trace.log* y, a continuación, reinicie el ordenador (para reiniciar el servicio ESET Management Agent).

• **status.html**: una tabla en la que se muestra el estado actual de las comunicaciones (sincronización) de ESET Management Agent con ESET PROTECT Server. El registro también contiene la configuración del proxy HTTP, una lista de políticas aplicadas (incluidas las exclusiones aplicadas) y la lista Grupos dinámicos a la que el dispositivo pertenece.

> Le recomendamos que lea el artículo de nuestra base de conocimiento sobre cómo utilizar el archivo status.html para la resolución de problemas de conexión con el agente.

Los problemas más habituales que pueden impedir que ESET Management Agent se conecte con ESET PROTECT Server son los siguientes:

• 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 ESET PROTECT Server no está configurado para recibir conexiones en el puerto 2222.

• El DNS no funciona correctamente, o los puertos están bloqueados por un cortafuegos. Consulte la lista de puertos utilizados por ESET PROTECT On-Prem, o consulte nuestro artículo de la base de conocimiento ¿Qué direcciones y puertos del cortafuegos de terceros debo abrir para garantizar la compatibilidad con todas las funciones de mi producto de 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.

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

Resolución de problemas - Implementación del agente

Durante la implementación de ESET Management Agent pueden surgir problemas. Si la implementación falla, los motivos pueden ser diversos. Esta sección le ayudará a:

- Averiguar qué ha causado que la implementación de ESET Management Agent falle

- Detectar posibles causas de acuerdo con la tabla de abajo
- Resolver el problema y realizar una implementación con éxito

Windows

1. Para averiguar por qué ha fallado la implementación del agente, vaya a **Informes** > **Automatización**, seleccione **Información sobre tareas de implementación de agente en los últimos 30 días**.
Se mostrará una tabla con la información de implementación. La columna **Progreso** muestra los mensajes de error que indican por qué ha fallado la implementación del agente.

Si necesita aún más detalles, puede cambiar la cantidad de información del registro de seguimiento de ESET PROTECT Server. Vaya a **Más** > Configuración > **Configuración avanzada** > **Registro** y seleccione **Error** en el menú desplegable. Ejecute la implementación del agente de nuevo y, cuando falle, revise las últimas entradas al final del archivo de registro de seguimiento de ESET PROTECT Server. El informe incluirá sugerencias sobre cómo resolver el problema.

El archivo más reciente se puede encontrar aquí:

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

> Para habilitar el registro completo del ESET Management Agent en el archivo *trace.log*, cree un archivo ficticio llamado *traceAll* sin extensión en la misma carpeta que un *trace.log* y, a continuación, reinicie el ordenador (para reiniciar el servicio ESET Management Agent).
> En caso de surgir problemas de conexión con ESET Management Agent, consulte Resolución de problemas - Conexión con el agente para obtener más información.

2. La tabla que aparece a continuación contiene diversos motivos por los que puede fallar la implementación del agente:

Mensaje de error	Causa(s) posible(s)
No se pudo conectar	• El cliente no está accesible en la red, el cortafuegos bloquea la comunicación • Los puertos de entrada 135, 137, 138, 139 y 445 no están abiertos en el cortafuegos en el cliente o en el cortafuegos de Windows: no se utiliza la excepción que permite el uso compartido de archivos e impresoras en la entrada • El nombre de cliente del cliente no se pudo resolver, utilice nombres de ordenadores FQDN válidos
Acceso denegado	• Al realizar la implementación desde un servidor vinculado a un dominio en un cliente vinculado a dicho dominio, utilice credenciales de un usuario que sea miembro del grupo de administradores de dominio en formato: **Dominio\Admin de dominio** • Al realizar una implementación desde un servidor unido a un dominio en un cliente unido a dicho dominio, puede elevar temporalmente el servicio ESET PROTECT Server de servicio de red a servicio ejecutado en la cuenta de administrador de dominio. • Al realizar la implementación desde un servidor en un cliente que no esté en el mismo dominio, desactive los filtros de control de cuentas de usuario remotos en el ordenador de destino. • Al realizar la implementación desde un servidor en un cliente que se encuentra en otro dominio, utilice las credenciales de un usuario local que sea miembro del grupo de administradores en el formato: **Admin**. El nombre del ordenador de destino se anexará automáticamente al inicio de sesión. • No existe una contraseña para la cuenta de administrador • Derechos de acceso insuficientes • El uso compartido del recurso administrativo *ADMIN$* no está disponible • El uso compartido del recurso administrativo *IPC$* no está disponible • El uso compartido de archivos sencillo está activado
No se encontró el paquete en el repositorio	• El enlace al repositorio es incorrecto • El repositorio no está disponible • El repositorio no contiene el paquete necesario
Error 1603	• Compruebe el archivo *ra-agent-install.log*. Está disponible en las siguientes rutas de acceso: *C:\Usuarios\%user%\AppData\Local\Temp\ra-agent-install.log* del ordenador de destino. • Si el error continúa, lea el artículo de nuestra base de conocimiento.

3. Siga los pasos de solución de problemas de acuerdo con la posible causa:

- **El cliente no está accesible en la red**: haga ping al cliente desde ESET PROTECT Server; si obtiene respuesta, trate de iniciar sesión en la máquina cliente de forma remota (por ejemplo, a través del escritorio remoto).

- **El cortafuegos bloquea la comunicación**: compruebe la configuración del cortafuegos en el servidor y el

cliente, así como cualquier otro cortafuegos que exista entre estas dos máquinas (si corresponde).

- **El nombre de host del cliente no se pudo resolver**: las posibles soluciones a los problemas de DNS pueden incluir, pero no están limitadas a:

  - Utilizar el comando `nslookup` de la dirección IP y el nombre de host del servidor o los clientes que tienen problemas de implementación del agente. Los resultados deben coincidir con la información de la máquina. Por ejemplo, un `nslookup` de un nombre de host debe resolver a la dirección IP y mostrarse un comando `ipconfig` en el host en cuestión. El comando `nslookup` tendrá que ejecutarse en los clientes y el servidor.

  - Examine manualmente los registros DNS en busca de 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 existe una contraseña para la cuenta de administrador**: configure una contraseña adecuada para la cuenta de administrador (no utilice una contraseña en blanco).

- **Derechos de acceso insuficientes**: pruebe a utilizar las credenciales de administrador de dominio al crear una tarea de implementación del agente. Si la máquina cliente está en un grupo de trabajo, utilice la cuenta de administrador local en ese ordenador en particular.

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

- **Para activar** la cuenta de usuario del administrador:

  1. Abra el símbolo de sistema administrativo

  2. Escribir 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**: compruebe que el servidor pueda acceder a *IPC$* con el comando que se indica a continuación desde el símbolo del sistema del servidor.

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

- **El uso compartido simple de archivos está activado**: si está recibiendo el mensaje de error **Acceso denegado** y su entorno es mixto (contiene un dominio y un grupo de trabajo), desactive **Uso compartido simple de archivos** o **Asistente para uso compartido** en todas las máquinas que tengan problemas con la implementación del agente. Por ejemplo, en Windows 11 haga lo siguiente:

  - Haga clic en **Inicio**, escriba `Explorador de archivos` en el cuadro **Buscar** y, a continuación, haga clic en **Opciones del explorador de archivos**. Haga clic en la ficha **Ver** y, en el cuadro de **Configuración avanzada**, desplácese por la lista y cancele la selección de la casilla de verificación junto a **Asistente para**

uso compartido.

• **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 habitualmente cuando no hay conexión con el repositorio de ESET PROTECT On-Prem. Compruebe su conexión a Internet.

Linux y macOS

Si la implementación del agente no funciona en Linux o macOS, el problema habitualmente está relacionado con SSH. Controle el equipo cliente y asegúrese de que el daemon SSH se esté ejecutando. Una vez solucionado, ejecute la implementación del agente de nuevo.

Situaciones de ejemplo de la implementación de ESET Management Agent

Esta sección contiene cuatro situaciones verificadas de la implementación de ESET PROTECT On-Prem.

1.Implementación desde un dispositivo ESET PROTECT Server o un ESET PROTECT Server Linux en destinos Windows que no están unidos a un dominio.

2.Implementación desde un ESET PROTECT Server Windows desde un origen Windows que no está unido a un dominio en destinos Windows que no están unidos al dominio.

3.Implementación desde un dispositivo ESET PROTECT Server o un ESET PROTECT Server Linux en destinos Windows que están unidos a un dominio.

4.Implementación desde un ESET PROTECT Server Windows desde un origen Windows que está unido a un dominio en destinos Windows que están unidos al dominio.

Situaciones de ejemplo de implementación de ESET Management Agent en destinos que no están unidos a un dominio

En las siguientes instrucciones se cubren estas situaciones:

• Implementación desde un dispositivo ESET PROTECT Server o un ESET PROTECT Server Linux en destinos Windows **que no están unidos a un dominio**.

• Implementación desde un ESET PROTECT Server Windows desde un origen Windows que no está unido a un dominio en destinos Windows **que no están unidos al dominio**.

Condiciones previas:

- Misma red local.
- Nombres FQDN operativos, p. ej.: desktop-win7.test.local se asigna a 192.168.1.20 y viceversa.
- Instalación limpia del sistema operativo desde MSDN con valores predeterminados.

Destinos:

Windows 10 Enterprise

1. Cree un usuario con contraseña que sea miembro del grupo Administradores, por ejemplo, **Admin**.

   a.Ejecute **Microsoft Management Console** abriendo **Ejecutar**, escribiendo "`mmc`" en el campo y haciendo clic en **Aceptar**.

   b.Agregue el **complemento Usuarios y grupos locales** desde **Archivo** > **Agregar o quitar complemento**. Agregue un usuario nuevo a la carpeta **Usuarios** e introduzca en los campos la información necesaria (no olvide incluir la contraseña). En la sección **Grupos**, abra las **Propiedades** del grupo **Administradores** y agregue al grupo el nuevo usuario creado haciendo clic en el botón **Agregar**. Escriba el nombre de inicio de sesión del usuario que acaba de crear en **Escriba el nombre de objeto para seleccionar** y verifíquelo haciendo clic en el botón **Comprobar nombres**.

2. En el **Centro de redes y recursos compartidos**, cambie el ajuste de red de **Red pública** a **Red privada** haciendo clic en la opción **Red pública** del lado izquierdo de la sección **Ver las redes activas**.

3. Desactive el **Firewall de Windows** en la **Red privada** haciendo clic en **Activar o desactivar el firewall de Windows** y seleccionando **Desactivar firewall de Windows** en la configuración de la ubicación de la **Red de trabajo** o doméstica.

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

5. Desactivar restricciones remotas de User Account Control (UAC):

   a.Abra el **Editor del Registro** escribiendo `regedit` en la consola **Ejecutar** y busque `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

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

   c.Abra el archivo creado y defina los **datos del valor** en **1**.

ESET PROTECT Web Console:

En ESET PROTECT Web Console, cree una nueva tarea del servidor de implementación de agente:

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

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

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 **No hay ningún certificado seleccionado** y seleccione **Certificado del agente**.

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

Situaciones de ejemplo de implementación de ESET Management Agent en destinos que están unidos a un dominio

En las siguientes instrucciones se cubren estas situaciones:

- Implementación desde un dispositivo ESET PROTECT Server o un ESET PROTECT Server Linux en destinos Windows **que están unidos a un dominio**.

- Implementación desde un ESET PROTECT Server Windows desde un origen Windows que está unido a un dominio en destinos Windows **que están unidos al dominio**.

Condiciones previas:

- Misma red local.

- Nombres FQDN operativos, p. ej.: desktop-win10.protect.local se asigna a 10.0.0.2 y viceversa.

- Instalación limpia del sistema operativo desde MSDN con valores predeterminados.

- Dominio `protect.local` creado con nombre de netbios `PROTECT`.

- 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` puede iniciar sesión en todas las máquinas y realizar tareas de administración locales.

- El servicio ESET PROTECT Server de Windows se está ejecutando temporalmente con las credenciales `PROTECT\DomainAdmin`. Tras la implementación, la cuenta de **Servicio de red** es suficiente (no es necesario realizar ningún cambio en el dispositivo virtual ni en Linux).

Destinos:

Windows 10 Enterprise

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

2. Compruebe que la red es una **Red de dominio** en la sección **Ver las redes activas**.

3. Desactive el **Firewall de Windows** en la **Red de dominio** haciendo clic en **Activar o desactivar el firewall de Windows** y seleccionando **Desactivar firewall de Windows** en la **Configuración de ubicación de red de dominio**.

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

ESET PROTECT Web Console:

En ESET PROTECT Web Console, cree una nueva tarea del servidor de implementación de agente:

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

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

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 **No hay ningún 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 ESET PROTECT Web Console. Puede acceder a ESET PROTECT Web Console desde cualquier dispositivo utilizando un navegador compatible. El **Menú principal**está accesible a la izquierda en todo momento, excepto cuando está utilizando un asistente. Haga clic en para desplegar el menú de la parte izquierda de la pantalla; puede contraerlo haciendo clic en **Contraer**.

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

Panel
Clientes administrados
Ordenadores
Detecciones

Informes
Tareas
Instaladores
Políticas
Notificaciones
Resumen del estado
Más

Panel principal

La consola es la página predeterminada que se muestra cuando inicia sesión en ESET PROTECT Web Console por primera vez. Muestra informes predefinidos sobre su red. Puede cambiar entre los tableros utilizando las fichas de la barra de menú superior. Cada tablero se compone de varios informes.

Manipulación de la consola

- **Agregar**: haga clic en el símbolo + situado en la parte superior del encabezado del panel para agregar un panel nuevo. Escriba el nombre de la nueva consola y haga clic en **Agregar consola** para confirmar. Se creará una nueva consola en blanco.

- **Mover**: haga clic en el nombre de una consola y arrástrelo para cambiar su ubicación en relación con otras consolas.

- Puede personalizar sus paneles agregando informes, modificando los existentes, cambiándolos de tamaño, moviéndolos y reorganizándolos.

- 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 MSP pueden hacer clic en **Seleccionar** junto al **cliente MSP** para filtrar la vista de panel para el cliente seleccionado.

Haga clic en el icono del engranaje situado junto a la ventana dinámica de la consola seleccionada para ver las siguientes opciones en el menú desplegable:

Actualizar página	Actualiza las plantillas de informe de esta consola.
Quitar	Quita la consola.
Renombrar	Cambia el nombre de la consola.
Duplicar	Crea una copia de la consola con los mismos parámetros que los del grupo principal del usuario.
Cambiar diseño	Elija el nuevo diseño de esta consola. El cambio quitará las plantillas actuales de la consola.

No puede personalizar estas consolas predeterminadas: **Resumen del estado**, **Resumen de la seguridad** y **ESET LiveGuard**.

En ESET PROTECT On-Prem vienen preconfiguradas las siguientes consolas:

Resumen del estado

La consola **Resumen del estado** es la pantalla predeterminada que ve cuando inicia sesión en ESET PROTECT On-Prem (a menos que establezca otra consola como predeterminada). Muestra información general sobre su red.

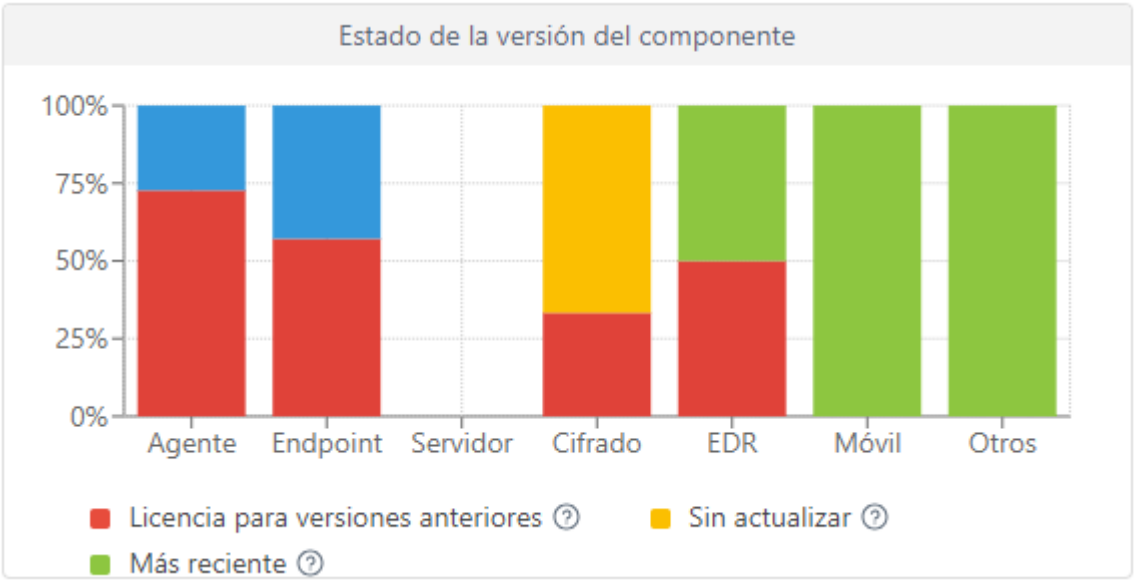
Filtros de dispositivos: muestra el número de dispositivos administrados basándose en el último estado del que se ha informado. Puede hacer clic en cada una de las 4 ventanas dinámicas para abrir una lista filtrada de dispositivos.

Estado del dispositivo: muestra el número de dispositivos administrados basándose en el tipo de producto de seguridad instalado en cada ficha. Si no hay implementado ningún producto de seguridad de ese tipo, en la ficha se mostrará una opción para implementar el paquete instalador correspondiente.

Estados de conexión: muestra la lista de las conexiones más recientes de los dispositivos administrados.

Estado de la versión del componente

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



Haga clic en el gráfico amarillo/rojo que representa los componentes o aplicaciones obsoletos y seleccione **Actualizar los componentes de ESET instalados** para iniciar una actualización. Consulte también la Política sobre el fin de la vida útil 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** (**Obsoleto**): la versión instalada del componente o producto de ESET está obsoleta, pero sigue siendo compatible. Normalmente, hay dos versiones anteriores a la versión más reciente en estado amarillo, a menos que contengan una vulnerabilidad de seguridad detectada recientemente.

- **Verde** (**Correcto**): está instalada la versión más reciente del componente o producto de ESET, o la versión

instalada es la versión más reciente del componente o producto de ESET compatible con la instancia de ESET PROTECT Web Console utilizada.

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

• **Azul** (**En espera**): las actualizaciones automáticas están activadas y la versión más reciente se instalará automáticamente. Más información sobre las actualizaciones automáticas:

- ESET Management Agentes
- Productos de seguridad de ESET

> Si pasa mucho tiempo sin que se actualicen los componentes de ESET, puede actualizarlos manualmente haciendo clic en el gráfico azul y seleccionando **Actualizar componentes de ESET instalados**.
> También puede usar la tarea del cliente Actualización de componentes de ESET PROTECT para actualizar los agentes y la tarea del cliente 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, justo después de una nueva instalación de un producto de ESET).

Estado de administración: muestra el número de **Administrados y protegidos** (dispositivos cliente con ESET Agent y un producto de seguridad instalado), **Administrados** (dispositivos cliente que solo tienen el agente), **No administrados** (dispositivos cliente de la red de los que ESET PROTECT On-Prem tiene constancia pero que no tienen instalado el agente) y **Rogue** (dispositivos cliente de los que ESET PROTECT On-Prem no tiene constancia, pero que Rogue Detection Sensor ha detectado).

Fuente RSS: muestra una fuente RSS de WeLiveSecurity y el Portal de la Base de conocimiento de ESET. Si hace clic en el icono del engranaje en **Fuente RSS**, puede elegir **Desactivar reproducción automática de fuente**, desactivar un origen de fuente concreto o **Desactivar fuente RSS**.

Resumen de incidentes

Esta consola ofrece información general sobre las detecciones sin resolver detectadas en los últimos 7 días, lo que incluye su gravedad, el método de detección, el estado de resolución y los 10 ordenadores/usuarios con más detecciones.

ESET LiveGuard

Si está utilizando ESET LiveGuard Advanced, aquí encontrará una visión general de informes útiles de ESET LiveGuard Advanced. 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.

Ordenadores

Este panel le da una visión general de las máquinas cliente, lo que incluye el estado de la protección, los sistemas operativos y el estado de la actualización.

Estado del rendimiento del servidor

En este panel puede ver información sobre el propio servidor de ESET PROTECT, lo que incluye la carga del servidor, los clientes con problemas, la carga de la CPU y las conexiones de bases de datos.

Detecciones del antivirus

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

Detecciones del cortafuegos

Eventos del cortafuegos de los clientes conectados ordenados en función de su gravedad, del momento de su notificación, etc.

Aplicaciones de ESET

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

Protección en la nube

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

Redimensionar	Haga clic en para ver un informe en modo de pantalla completa.
Actualizar	Actualiza la plantilla del informe.
Descargar	Haga clic en **Descargar** para generar y descargar el informe. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa `;` (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe PDF para ver los valores de texto.
Cambiar	Cambie la plantilla de informe por otra de la lista de plantillas.
Modificar plantilla de informe	Edite una plantilla de informe existente. Se aplican los mismos ajustes y opciones usados al crear una plantilla nueva de informe.
Establecer intervalo de actualización	Configure un intervalo de actualización predeterminado para la plantilla.
Programar	Planificar un informe: puede modificar el desencadenador, la regulación y la entrega del informe de la planificación. Puede encontrar todos los informes planificados en la **ficha Informes programados**.
Quitar	Quita la plantilla de informe de la consola.
Renombrar	Cambia el nombre de la plantilla del informe.
Esta celda	Elija el nuevo diseño de esta consola. El cambio quitará las plantillas actuales de la consola.

Permisos del panel principal

Un usuario debe tener el permiso adecuado para trabajar con paneles. En un panel principal solo pueden utilizarse las plantillas de informes contenidas en un grupo en el que el usuario tenga derechos de acceso. Si el usuario no tiene derechos asignados en **Informes y consola**, no verá ningún dato en la sección Panel principal. De forma predeterminada, el administrador puede ver todos los datos.

- **Leer**: el usuario puede enumerar las plantillas de informes y sus categorías, generar informes basados en plantillas de informes o leer el panel
- **Usar**: el usuario puede modificar el panel con las plantillas de informes disponibles
- **Escribir**: cree, modifique o elimine plantillas y sus categorías

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

Profundizar

Puede utilizar la función de la consola de profundización para examinar datos con mayor detalle. Le permite seleccionar de forma interactiva elementos específicos de un resumen y ver datos detallados sobre ellos. Céntrese en el elemento de su interés "profundizando" desde la información del resumen a fin de obtener más información sobre este tema en particular. Por lo general hay varios niveles a los que puede profundizar.

Existen diferentes opciones de profundización:

- Mostrar **Información detallada**: nombre y descripción del ordenador, nombre del grupo estático, etc. Muestra los datos originales (no agregados) de la fila en la que se ha hecho clic.

- 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 solo hay un número en la columna y hace clic en Expandir columna Ordenador, mostrará todos los detalles de los ordenadores.

- Mostrar **En la página Ordenadores (todos)**: le redirige a la página **Ordenadores** (muestra solo 100 elementos como resultado).

Acciones con un clic

Los informes con información sobre los problemas detectados contienen opciones adicionales de profundización cuando hace clic en el elemento de la tabla o del gráfico:

- "*tarea para resolver la alerta seleccionada*": puede resolver la alerta seleccionando la tarea sugerida, que se ejecutará lo antes posible.

  Si la alerta no se puede resolver a través de una tarea, pero sí a través de una configuración de políticas, se muestran las siguientes opciones:

  - **Administrar políticas**

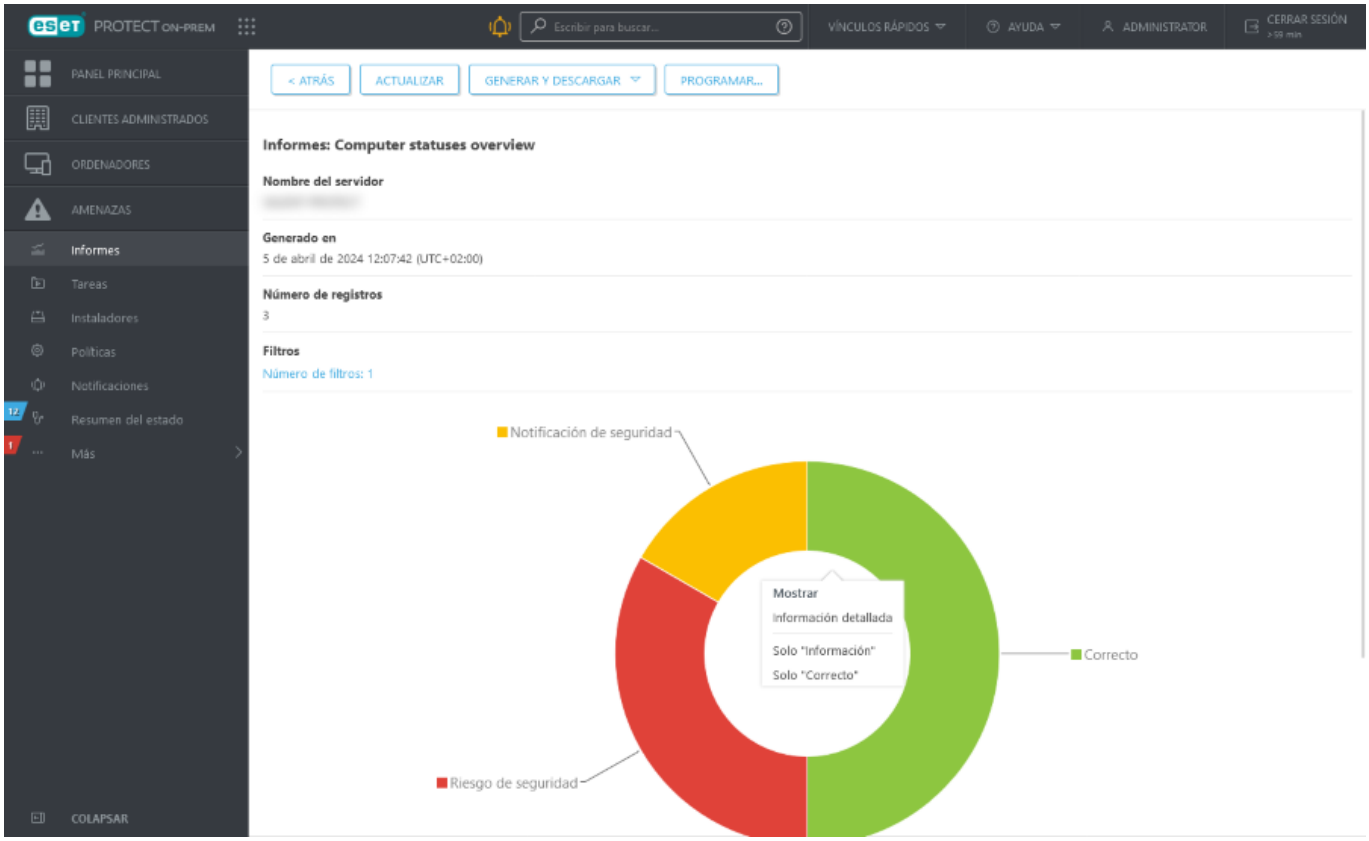
  - **Nueva política**

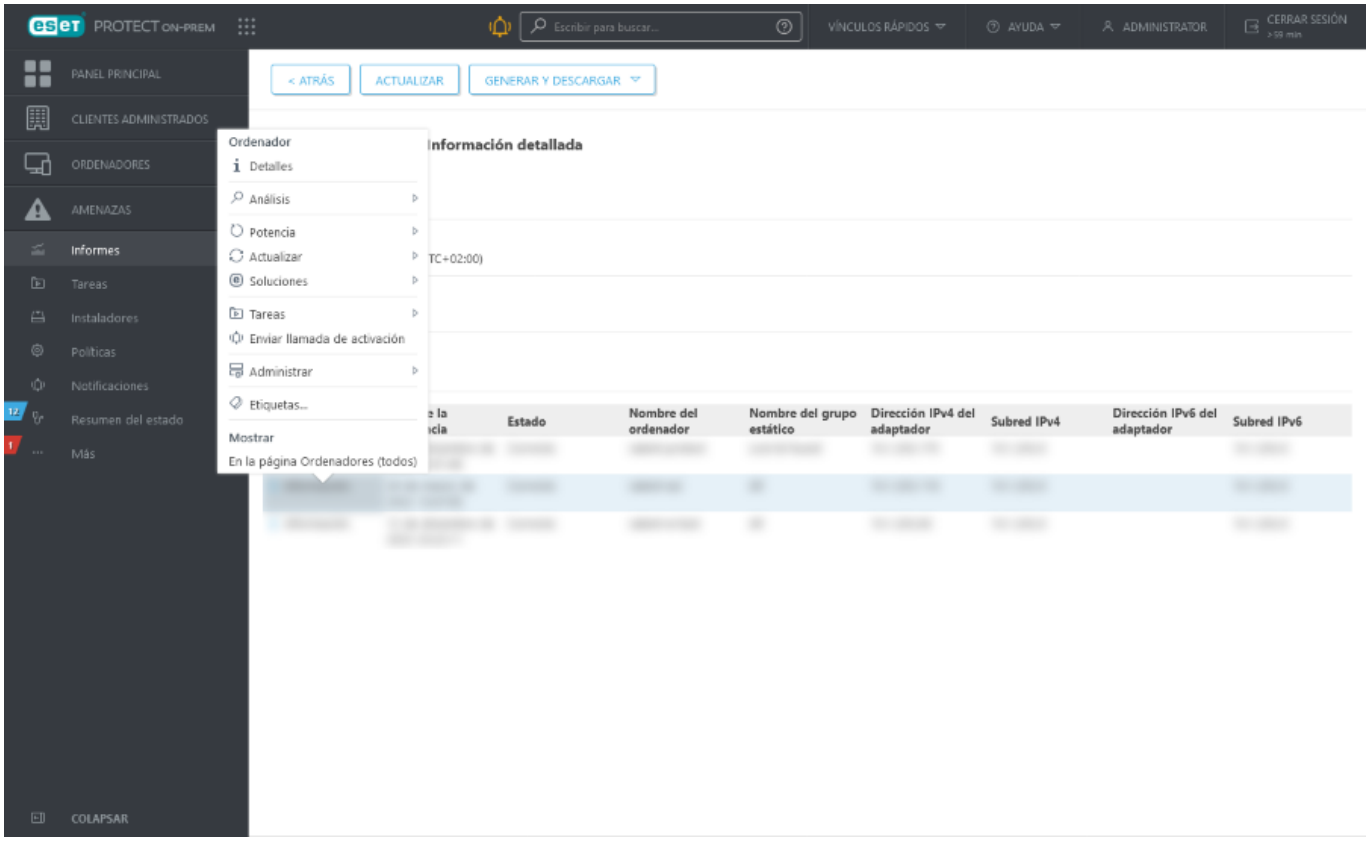
- **Buscar en Internet**: activa la búsqueda en Google de la alerta seleccionada. Puede utilizar esta opción si no

se sugiere ninguna respuesta (tarea o configuración de políticas) para resolver la alerta seleccionada.

> En los resultados que obtenga al profundizar en otros informes solo se mostrarán los primeros 1.000 elementos.

Si desea generar y descargar el informe, haga clic en el botón **Generar y descargar**. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa ; (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe 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 Managed Service Provider (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: se trata de detalles de grupos estáticos porque dichos grupos representan a los clientes en 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 elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Entrar**. Los filtros activos aparecen resaltados en color azul. También puede utilizar los filtros preestablecidos.
- En otras secciones de Web Console:Panel, al programar o generar un informe.

Ordenadores

Todos los dispositivos cliente que se hayan agregado a ESET PROTECT On-Prem se muestran aquí y se dividen en grupos. Cada dispositivo se asigna a un grupo estático. Al hacer clic en un grupo de la lista (a la izquierda) se mostrarán los miembros (clientes) de este grupo en el panel derecho.

Los ordenadores **no administrados** (clientes de la red que no tienen ESET Management Agent instalado) suelen aparecer en el grupo **Perdidos y encontrados**. El estado de un cliente que se muestra en ESET PROTECT Web Console es independiente de los ajustes de los productos de seguridad de ESET en el cliente. Esta es la razón por la que, incluso aunque un estado concreto no se muestre en el cliente, se seguirá informando de él a ESET PROTECT Web Console. Puede arrastrar y colocar clientes para moverlos entre los grupos.

Haga clic en el botón **Agregar dispositivo** y seleccione:

- **Ordenadores**: puede agregar ordenadores al grupo estático seleccionado.
- **Dispositivos móviles**: puede agregar dispositivos móviles al grupo estático seleccionado.
- **Sincronizar mediante servidor de directorios**: puede ejecutar la tarea Sincronización de grupos estáticos.

Haga clic en un dispositivo para abrir un nuevo menú con acciones disponibles para ese dispositivo. También puede marcar la casilla de verificación junto a un dispositivo y hacer clic en el botón **Ordenador** de la barra inferior. El menú **Ordenador** mostrará distintas opciones en función del tipo de dispositivo. Consulte la leyenda de los iconos si desea obtener información detallada sobre los diferentes tipos de iconos y estados. Haga clic en el número de alertas de la columna **Alertas** para ver la lista de alertas en la sección detalles del ordenador.

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

- Amarillo (error): hace entre 2 y 14 días que el ordenador no se conecta.
- Rojo (advertencia): el ordenador no se conecta desde hace más de 14 días.

El icono **Inspect** abre la sección Ordenadores de ESET Inspect On-Prem Web Console. El ESET Inspect On-Prem solo está disponible cuando tiene la licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de ESET Inspect**.

Filtrado de la vista

Hay distintas formas de filtrar la vista:

- Filtro estándar: Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Entrar**. Los filtros activos aparecen resaltados en color azul.
- Puede filtrar por gravedad con los iconos de estado: rojo: **Errores**, amarillo: **Advertencias**; verde: **Correcto**; gris: ordenadores **no administrados**. El icono de gravedad representa el estado actual del

producto de ESET en un ordenador cliente en particular. Puede utilizar una combinación de estos iconos activándolos y desactivándolos. Por ejemplo, para ver solo los ordenadores con advertencias, deje seleccionado solo el icono amarillo (los demás iconos no deben estar seleccionados). Para ver ambos, advertencias y errores, deje solo estos dos iconos activados.

- Haga clic en **Agregar filtro > Categoría de producto** y, en el menú desplegable, seleccione los tipos de dispositivos que desee ver.

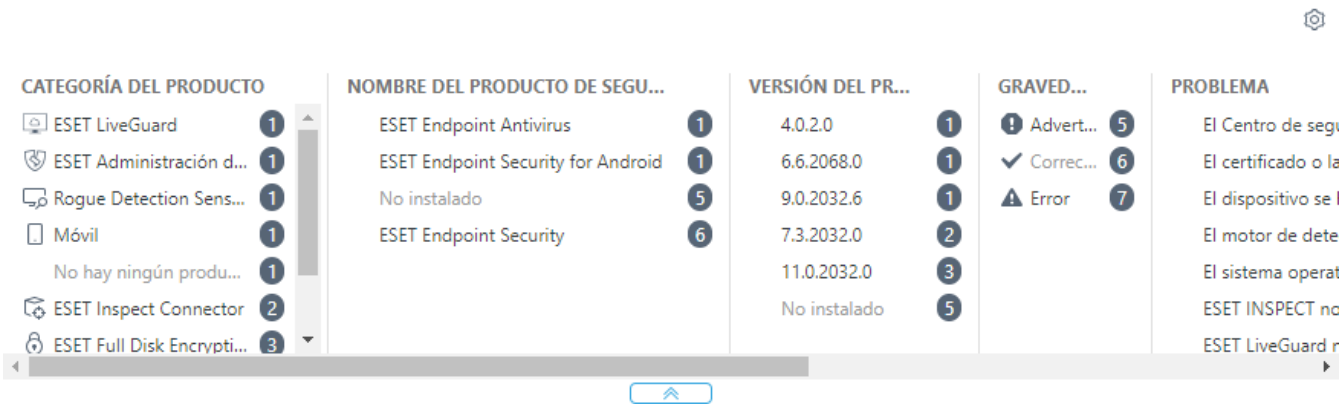
  - **Protegido por ESET** (protegido por un producto ESET): Escritorio, Móvil, Servidor, Servidor de correo electrónico, Servidor de puerta de enlace, Servidor de colaboración, Servidor de archivos.

  - **ESET PROTECT On-Prem** (componentes individuales de ESET PROTECT): ESET Management Agent, Rogue Detection Sensor, ESET PROTECT Server.

  - **Otros**: ESET LiveGuard, ESET Inspect Connector, ESET Inspect Server, ESET Full Disk Encryption, ESET Bridge, Virtual Security Appliance, Shared Local Cache.

- Casilla **Mostrar subgrupos**: muestre subgrupos del grupo seleccionado.

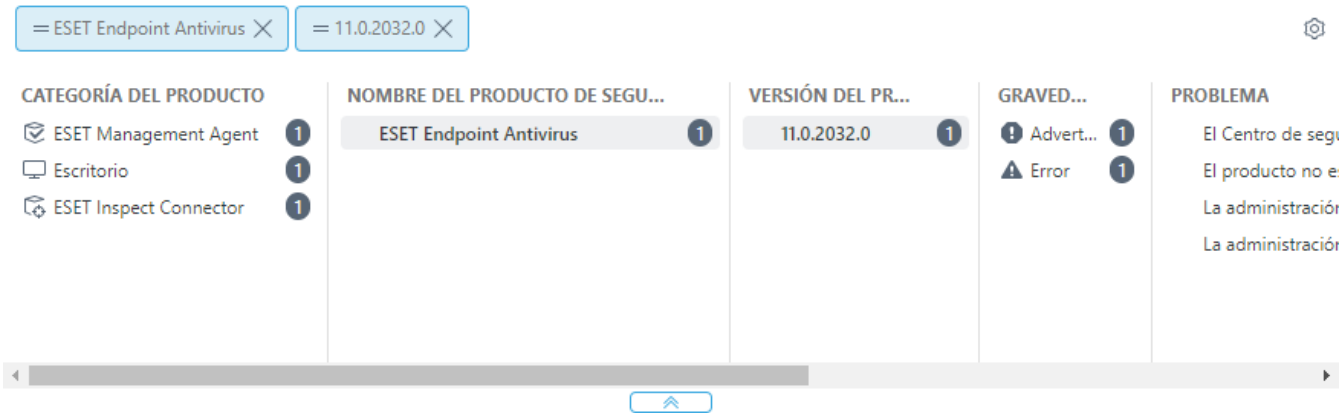
- Puede ver los **Filtros avanzados** como un panel de filtros expansible en la pantalla **Ordenadores**.



Los filtros avanzados muestran una vista previa en tiempo real de los valores de distintos filtros y el número exacto de resultados de su selección.

Al filtrar grandes conjuntos de ordenadores, los filtros avanzados muestran qué valores de filtro devolverán un número administrable de resultados, lo que le permitirá encontrar los dispositivos correctos 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 alternar entre el filtrado de un valor **igual** y **no igual**.



Haga clic en el icono del engranaje en una columna para ordenar los valores de la columna o haga clic en el icono del engranaje situado en la parte superior de los filtros avanzados. Use el asistente para ajustar (agregar, quitar y reordenar) las columnas mostradas. También puede utilizar la opción de arrastrar y colocar para ajustar las columnas. Haga clic en **Restablecer** para restablecer las columnas de la tabla a su estado predeterminado (las columnas disponibles predeterminadas en orden predeterminado).

Solo puede utilizar filtros avanzados con grupos estáticos. Los grupos dinámicos no son compatibles con los filtros avanzados.

- Utilice Grupos dinámicos o Informes para disfrutar de opciones de filtrado más avanzadas.
- Para buscar los ordenadores marcados como Maestro para clonación, haga clic en **Agregar filtro** > seleccione **Maestro para clonación** > marque la casilla de verificación situada junto al filtro **Maestro para clonación**.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. 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 ordenador

Para encontrar los detalles de un ordenador, seleccione un ordenador cliente en un grupo estático o dinámico y haga clic en **Detalles** o haga clic en el nombre del ordenador para mostrar el panel lateral Vista previa del ordenador en el lateral derecho.

El icono **Inspect** abre la sección Ordenadores de ESET Inspect On-Prem Web Console. El ESET Inspect On-Prem solo está disponible cuando tiene la licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de ESET Inspect**.

La ventana de información consta de los siguientes elementos:

Información general:

Ordenador

- Haga clic en el icono de edición para cambiar el nombre o la descripción del ordenador. Puede seleccionar **Permitir nombres duplicados** si ya hay otro ordenador administrado con el mismo nombre.
- Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
- **FQDN**: nombre de dominio completamente cualificado del ordenador

> Si sus ordenadores cliente y ESET PROTECT Server se ejecutan en Active Directory, puede automatizar la acción de rellenar los campos **Nombre** y **Descripción** con la tarea Sincronización de grupos estáticos.

- **Grupo principal**: cambie el grupo estático principal del ordenador.
- **IP**: la dirección IP del equipo.
- **Recuento de políticas aplicadas**: haga clic en el número para ver la lista de las políticas aplicadas.
- **Miembro de grupos dinámicos**: la lista de grupos dinámicos en los que estaba presente el ordenador cliente durante la replicación más reciente.

Hardware

Esta ventana dinámica contiene una lista de parámetros clave del hardware, información sobre el sistema operativo e identificadores únicos. Haga clic en la ventana dinámica para ver la ficha **Detalles - Hardware**. Consulte también el inventario de hardware.

Alertas

- **Alertas**: vínculo a una lista de problemas del ordenador.
- **Número de detecciones sin resolver**: recuento de detecciones sin resolver. 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 ordenador se conectó hace menos de 10 minutos. La información de **Última conexión** se resalta para indicar que el ordenador no está conectado:
  - Amarillo (error): hace entre 2 y 14 días que el ordenador no se conecta.
  - Rojo (advertencia): el ordenador no se conecta desde hace más de 14 días.
- **Hora del último inicio**: fecha y hora del último inicio del dispositivo administrado. El ordenador administrado debe ejecutar ESET Management Agente 10.0 o una versión posterior para ver **Hora del último inicio**. Las versiones anteriores del agente indican **n/a**.
- **Hora del último análisis**: información sobre la hora del último análisis.

- **Motor de detección**: versión del motor de detección del dispositivo de destino.
- **Actualizado**: el estado de actualización.

Productos y licencias

Lista de componentes de ESET instalados en el ordenador. Haga clic en la ventana dinámica para ver la ficha **Detalles - Productos y licencias**.

Cifrado

La ventana dinámica de cifrado solo es visible en estaciones de trabajo compatibles con ESET Full Disk Encryption.

- Haga clic en **Cifrar ordenador** para iniciar el asistente de Activar cifrado.
- Cuando el cifrado esté activado, haga clic en **Administrar** para administrar las opciones de cifrado.
- Si el usuario no puede iniciar sesión con su contraseña o si no se puede acceder a los datos cifrados de la estación de trabajo debido a un problema técnico, el administrador podrá iniciar el proceso de recuperación de cifrado.

ESET LiveGuard Advanced

En la ventana se proporciona información básica sobre el servicio. Puede tener dos estados de ventana:

- Blanco: el estado predeterminado. Con ESET LiveGuard Advanced activado y funcionando, el estado de la ventana sigue siendo Blanco.
- Amarillo: si hay un problema con el servicio ESET LiveGuard Advanced, la ventana se vuelve amarilla y muestra información sobre el problema.

> Necesita la licencia de ESET LiveGuard Advanced para activar ESET LiveGuard Advanced.

Acciones disponibles:

- **Activar**: haga clic en **Activar** para configurar la tarea de activación y la política del producto ESET LiveGuard Advanced en el equipo actual. También puede hacer clic en un ordenador o en el icono del engranaje situado junto a un grupo estático y seleccione **Soluciones** > **Activar ESET LiveGuard**. En la ventana de configuración, seleccione el nivel de protección y haga clic en **Activar ESET LiveGuard**:
  - **Protección óptima (recomendada)**: los archivos en riesgo, incluidos los tipos de documentos que admiten macros, se enviarán a un servidor seguro de ESET para el escaneo automatizado y el análisis del comportamiento. El acceso a los archivos está limitado hasta que se hayan evaluados como seguros.
  - **Protección básica**:ESET LiveGuard Advanced analizará un conjunto limitado de archivos.
- Archivos enviados: lista de todos los archivos enviados a los servidores de ESET.

Después de activar ESET LiveGuard Advanced:

- El panel de ESET LiveGuard mostrará los informes mejorados de ESET LiveGuard Advanced de su red administrada.

• Cada dispositivo con ESET LiveGuard Advanced tendrá el reputación y el Sistema de reputación ESET LiveGrid® y el Sistema de respuesta ESET LiveGrid® activados. Consulte las políticas de su dispositivo.

Usuarios

• **Usuarios que han iniciado sesión** (solo ordenadores): dominio y nombre de usuario de los usuarios que han iniciado sesión en el dispositivo.

• **Usuarios asignados**

oHaga clic en **Agregar usuario** para asignar un usuario desde Usuarios del ordenador a este dispositivo.

U ordenador solo se puede asignarse a un máximo de 200 usuarios en una operación.

oHaga clic en el icono de la papelera para cancelar la asignación del usuario actual.

oHaga clic en el nombre de usuario del usuario asignado para ver los datos de su cuenta.

Ubicación

La ventana dinámica solo está disponible para dispositivos móviles. Puede localizar dispositivos de la Apple Business Manager de iOS (ABM) solo cuando está activado el Modo perdido.

Virtualización

La ventana dinámica aparece después de marcar el ordenador como equipo principal para clonar y muestra la configuración de VDI. Haga clic en el icono del engranaje para cambiar la configuración de VDI.

En la parte inferior se muestran los siguientes botones:

• Haga clic en el botón **Aislamiento de red** para ejecutar las tareas del cliente de aislamiento de la red en el ordenador:

o Aislar de la red

o Finalizar aislamiento de la red

• El botón **Virtualización** se utiliza para configurar el ordenador para la clonación. Es obligatorio cuando se clonan ordenadores o se cambia el hardware de los ordenadores.

oMarcar como maestro para clonación

o**Desactivar la detección de hardware**: desactive la detección de los cambios de hardware de forma permanente. Esta acción es irreversible.

o**Cancelar selección como equipo principal para clonar**: quite el indicador de equipo principal. Tras aplicar esta opción, cada nueva clonación del equipo generará una pregunta.

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

Configuración:

Ficha **Configuración**: contiene la lista de configuraciones de los productos de ESET instalados (ESET Management Agent, ESET Endpoint, etc.). Las acciones disponibles son:

- Haga clic en **Solicitar configuración** para crear una tarea que obligue a ESET Management Agent a recopilar todas las configuraciones de los productos administrados. Una vez enviada la tarea a ESET Management Agent, se ejecuta inmediatamente, y los resultados se envían a ESET PROTECT Server en la siguiente conexión. Esto le permitirá ver la lista de todas las configuraciones de los productos administrados.

- Abra una configuración mediante un menú contextual y conviértala en una política. Haga clic en una configuración para verla en el visor.

- Cuando abra la configuración, puede convertirla en una política. Haga clic en **Convertir en política**: la configuración actual se transferirá al asistente de políticas y podrá modificar y guardar la configuración como nueva política.

- Descargue una configuración con fines diagnósticos y de asistencia. Haga clic en una configuración seleccionada y haga clic en **Descargar para diagnóstico** en el menú desplegable.

Ficha **Políticas aplicadas**: lista de las políticas aplicadas al dispositivo. Si ha aplicado una política para un producto de ESET o una función del producto de ESET que no están instalados en el ordenador, la política mostrada estará no disponible.

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 las políticas bloqueadas (no editables): políticas integradas específicas (por ejemplo, la política de actualizaciones automáticas o las políticas ESET LiveGuard) o políticas para las que el usuario tiene permiso de **Lectura**, pero no de **Escritura**.

Haga clic en **Administrar políticas** para administrar, modificar, asignar o eliminar una política. Las políticas se aplican en función de su orden (columna **Orden de políticas**). Para cambiar la prioridad de la aplicación de políticas, marque la casilla de verificación situada junto a una política y haga clic en los botones **Aplicar antes** o **Aplicar más tarde**.

Pestaña **Exclusiones aplicadas**: lista de las exclusiones aplicadas al dispositivo.

Registros (solo ordenadores)

- **SysInspector**: haga clic en **Solicitar registro (solo Windows)** para ejecutar la tarea Solicitud de registro de SysInspector en los clientes seleccionados. Una vez completada la tarea, se muestra una nueva entrada en la lista de registros de ESET SysInspector. Haga clic en uno de los registros de la lista para explorarlo.

- **Log Collector**: haga clic en **Ejecutar Log Collector** para ejecutar la tarea Log Collector. Una vez completada la tarea, se agrega una nueva entrada a la lista de registros. Haga clic en uno de los registros de la lista para descargarlo.
- **Registros de diagnóstico**: haga clic en **Diagnóstico** > **Activar** para iniciar el Modo de diagnóstico en el equipo actual. El Modo de diagnóstico hará que el cliente envíe todos los registros a ESET PROTECT Server. Podrá examinar todos los registros en un plazo de 24 horas. Los registros se clasifican en cinco categorías: **Registro de correo no deseado**, **Registro de cortafuegos**, **Registro de HIPS**, **Registro de control de dispositivos** y **Registro de control web**. Haga clic en **Diagnóstico** > **Volver a enviar todos los registros** para volver a enviar todos los registros del agente en la siguiente replicación. Haga clic en **Diagnóstico** > **Desactivar** para detener el modo de diagnóstico.

El límite de tamaño de archivo para la entrega de registro por dispositivo es de 200 MB. Puede acceder a los registros desde Web Console en **Detalles** > sección **Registros**. Si los registros que ha recopilado la tarea superan los 200 MB, se producirá un error en la tarea. Si se produce un error en la tarea, puede:
- Recopilar los registros localmente en el dispositivo.
- Cambiar el nivel de detalle de los registros y repetir la tarea:
  - En el caso de destinos Windows, utilice el parámetro `/Targets:EraAgLogs` para recopilar solo los registros de ESET Management Agent.
  - En el caso de destinos Linux/macOS, utilice el parámetro `--no-productlogs` para excluir los registros del producto de seguridad de ESET instalado.

Ejecuciones de tareas

Una lista de tareas ejecutadas. Puede filtrar la vista para limitar los resultados, ver detalles de la tarea, editar, duplicar, eliminar o ejecutar/ejecutar de nuevo la tarea.

Aplicaciones instaladas:

Muestra una lista de los programas instalados en un cliente, con información detallada como la versión, el tamaño, el 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 de Agent.

Si administra dispositivos Android y ha aplicado una política para permitir las excepciones de la aplicación (**Control de la aplicación** > **Activar control de la aplicación** > **Activar el 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 eliminarla.

- Se le pedirá que introduzca **Parámetros de desinstalación**. Son parámetros opcionales de la línea de comandos para el instalador (paquete de instalación). Los parámetros de desinstalación son exclusivos para cada instalador de software. Puede encontrar más información en la documentación de cada producto.

- Marque la casilla de verificación situada junto a **Reiniciar automáticamente cuando sea necesario** para

forzar un reinicio automático del ordenador cliente tras la instalación. También puede dejar esta opción sin seleccionar y reiniciar manualmente el ordenador cliente. Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste.

Cuando desinstale el agente de ESET Management del ordenador cliente, ESET PROTECT On-Prem dejará de administrar el dispositivo:
• El producto de seguridad de ESET puede conservar algunos ajustes después de la desinstalación del agente de ESET Management.
• Si ESET Management Agent está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar el producto (con cambios). Se recomienda restablecer algunos ajustes que no se deseen mantener (por ejemplo, la protección con contraseña) a los valores predeterminados mediante una política antes de quitar el dispositivo de la administración.
• Asimismo se abandonarán todas las tareas que se estén ejecutando en el agente. Es posible que los estados de ejecución **En ejecución**, **Finalizado** o **Con error** de esta tarea no se muestren con precisión en ESET PROTECT Web Console en función de la replicación de los datos.
• Tras la desinstalación del agente puede gestionar el producto de seguridad mediante eShell o la EGUI integrada.

Si hay una actualización disponible para el producto de ESET, puede actualizar el producto de ESET haciendo clic en el botón **Actualizar productos de ESET**.

• ESET PROTECT On-Prem admite la actualización automática de las instancias de ESET Management Agent en ordenadores administrados.
• Los dispositivos iOS envían la lista de software instalado a ESET PROTECT On-Prem una vez al día. El usuarios no puede forzar la actualización de la lista.

Alertas

Muestra una lista de alertas y sus detalles: Problema, Estado, Producto, Cuándo ocurrió, Gravedad, etc. Puede accederse directamente a esta lista desde la sección **Ordenadores** haciendo clic en el recuento de alertas de la columna **Alertas**. Puede administrar la alertas a través de acciones con un clic.

Preguntas (solo ordenadores)

La lista de preguntas relacionadas con la clonación está en la ficha **Preguntas**. Obtenga más información sobre resolución de problemas para ordenadores cambiados o clonados.

Detecciones y cuarentena

• **Detecciones**: se muestran todos los tipos de detecciones, pero puede filtrarlas por **Categoría de detección**: **Antivirus**, Archivos bloqueados, ESET Inspect, **Cortafuegos**, **HIPS** y **Protección web**.

• **Cuarentena**: una lista de detecciones en cuarentena con detalles como el nombre de la detección, el tipo

de la detección, el nombre del objeto, el tamaño, la primera aparición, el recuento, el motivo del usuario, etc.

- **Archivos enviados**: una lista de todos los archivos enviados a los servidores de ESET.

··· Detalles

• **Básico**: información sobre el 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 sin sonido, cómo se administra, cuándo se actualizó por última vez y el número de políticas aplicadas.

• **Hardware**: información sobre el hardware, el fabricante y modelo, la CPU, la RAM, el almacenamiento (lo que incluye la capacidad y el espacio libre) y los periféricos del ordenador e información sobre redes (IPv4, IPv6, subred, adaptador de red, etc.). Consulte también el inventario de hardware.

• **Productos y licencias**: versión del motor de detección actual, versiones de los productos de seguridad de ESET instalados y licencias utilizadas.

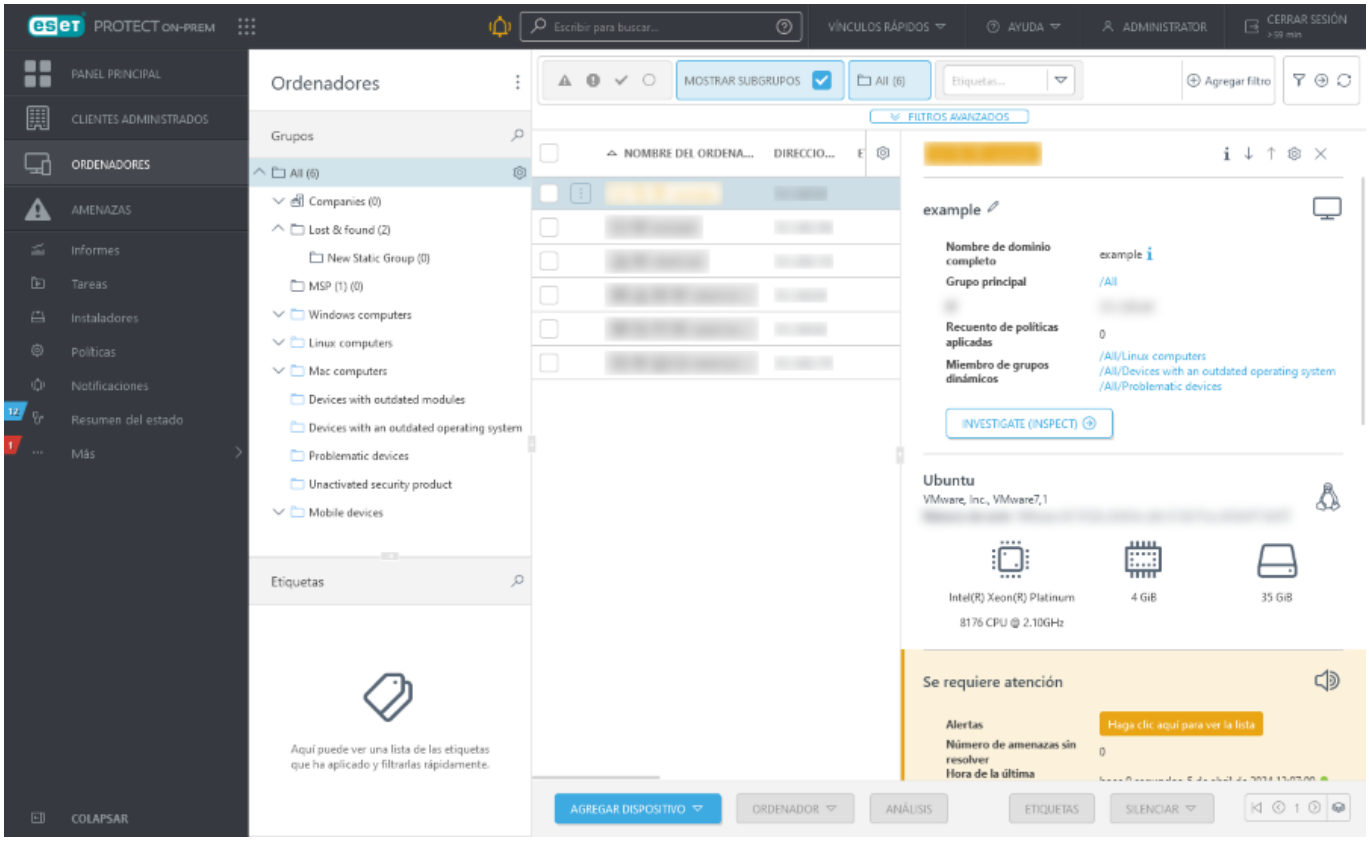
• **Cifrado:** si utiliza ESET Full Disk Encryption, consulte la información general sobre el estado de cifrado del disco.

Vista previa del ordenador

En **Ordenadores**, haga clic en el nombre de un ordenador para mostrar el panel lateral Vista previa del ordenador en el lateral derecho. El panel lateral Vista previa del ordenador contiene la información más importante sobre el ordenador seleccionado.

Manipulación de la vista previa del ordenador:

- **Mostrar detalles**: abra el menú Detalles del ordenador
- **Siguiente**: muestra el siguiente dispositivo en el panel lateral Vista previa del ordenador.
- **Anterior**: muestra el dispositivo anterior en el panel lateral Vista previa del ordenador.
- **Administrar el contenido de Detalles del ordenador**: puede gestionar qué secciones del panel lateral de vista previa del ordenador se muestran y en qué orden.
- **Cerrar**: cierra el panel lateral Vista previa del ordenador.



Quitar ordenador de administración

Para quitar un dispositivo de la administración, haga clic en **Ordenadores**, seleccione un dispositivo y haga clic en **Administrar** > **Quitar**. En un cuadro de diálogo se mostrarán los pasos necesarios para quitar el ordenador seleccionado de la administración.

Cuando pase al siguiente paso, asegúrese de haber completado el paso anterior con éxito. Esto es básico para que la eliminación de los dispositivos se realice de forma correcta.

1. **Restablecer configuración de Endpoint**: haga clic en **Administrar políticas** y quite todas las políticas aplicadas para permitir la administración de dispositivos locales. Consulte **Reglas de eliminación de políticas** en la sección **Políticas**. Si se ha establecido una contraseña para acceder a la configuración del producto Endpoint, cree una política nueva para eliminarla (seleccione la opción de definir una contraseña pero sin introducir ninguna). Para ordenadores cifrados con ESET Full Disk Encryption, siga los pasos de descifrado.

2. **Detener administración del ordenador**: ejecuta una tarea Detener administración o desinstale ESET Management Agent o el producto de seguridad ESET localmente en el ordenador. De esta forma se suspende la conexión entre el ordenador y ESET PROTECT On-Prem.

3. **Quitar ordenador de la base de datos**: una vez que se haya asegurado de que el ordenador ya no se conecta a ESET PROTECT On-Prem, puede quitarlo de la lista de dispositivos administrados.

Marque la casilla **Quiero desactivar los productos de ESET instalados** para quitar la licencia de todos los productos de ESET instalados en el ordenador seleccionado. Consulte también la información sobre la desactivación de los productos empresariales de ESET.

Grupos

Los grupos pueden entenderse como carpetas en las que se categorizan ordenadores y otros objetos.

Para los ordenadores y dispositivos, puede usar plantillas de grupos y grupos predefinidos o crear nuevos grupos y plantillas de grupos. Los ordenadores cliente se pueden agregar a los grupos. Esto le ayuda a mantener los ordenadores estructurados y dispuestos a su gusto. Puede agregar ordenadores a un grupo estático.

Los grupos estáticos se administran manualmente, mientras que los grupos dinámicos se organizan automáticamente en función de criterios específicos de una plantilla. Cuando los ordenadores están incluidos en grupos, puede asignar políticas, tareas o ajustes a estos grupos. Posteriormente, la política, la tarea o el ajuste se aplican a todos los miembros del grupo. Existen dos tipos de grupos de clientes:

Grupos estáticos

Los grupos estáticos son grupos de ordenadores cliente seleccionados y otros objetos. Sus miembros son estáticos y solo se pueden añadir o eliminar manualmente, no en función de criterios dinámicos. Cada objeto solo puede estar presente en un grupo estático. Un grupo estático solo puede eliminarse si no contiene objetos.

Grupos dinámicos

Los grupos dinámicos son grupos de dispositivos (no otros objetos, como tareas o políticas) que se han convertido en miembros del grupo al cumplir unos criterios específicos. Si el dispositivo cliente no cumple esos criterios, se eliminará del grupo. Los ordenadores que cumplen los criterios se añaden automáticamente al grupo (de ahí que se les llame "dinámicos").

Haga clic en el icono del engranaje que aparece junto al nombre del grupo para ver las acciones de grupo y los detalles de grupo disponibles.

Los ordenadores que son miembros del grupo aparecen en el panel de la derecha.

Acciones de grupo

Diríjase a **Ordenadores** y seleccione el grupo que desee administrar. Haga clic en el icono del engranaje que aparece junto al nombre del grupo y seleccione Mover. Se mostrará un menú con las siguientes opciones:

Acción de grupo	Descripción de la acción de grupo	Grupos estáticos	Grupos dinámicos
Mostrar detalles	Ofrece información general sobre el grupo seleccionado.	✔	✔
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.	✔	✔
Nuevo grupo estático	El grupo seleccionado pasa a ser el grupo principal predeterminado, pero se puede cambiar más tarde si se crea un nuevo grupo estático.	✔	x
Nuevo grupo dinámico	El grupo seleccionado pasa a ser el grupo principal predeterminado, pero se puede cambiar más tarde si se crea un nuevo grupo dinámico.	✔	✔
Nueva notificación	Crea una nueva notificación.	x	✔
Agregar nuevo	Agrega un nuevo dispositivo.	✔	x

Acción de grupo	Descripción de la acción de grupo	Grupos estáticos	Grupos dinámicos
Tareas	Seleccione las tareas del cliente que se ejecutarán en los dispositivos de este grupo: **Análisis**: ejecuta la tarea Análisis a petición en todos los clientes del grupo seleccionado. **Actualización**: • **Actualizar módulos**: ejecuta la tarea Actualización de módulos (se inicia una actualización de forma manual). • **Actualizar productos de ESET**: ejecute la tarea Instalación del software en ordenadores con productos de seguridad de ESET sin actualizar. • **Actualización del sistema operativo**: ejecute la tarea Actualización del sistema operativo en ordenadores del grupo seleccionado. **Móvil**: consulte Acciones Antirrobo para obtener más información. • **Inscribir de nuevo**: vuelva a inscribir un dispositivo móvil. • **Buscar**: solicita las coordenadas GPS de su dispositivo móvil. • **Bloquear**: el dispositivo se bloqueará cuando se detecte actividad sospechosa o esté marcado como desaparecido. • **Desbloquear**: el dispositivo se desbloqueará. • **Borrar el código de acceso**: quite el código de acceso de un dispositivo iOS/iPadOS. • **Modo sirena/perdido**: activa una potente sirena de forma remota, la sirena sonará aunque el dispositivo esté en silencio. • **Restablecimiento de fábrica**: todos los datos almacenados en el dispositivo se borrarán de forma permanente. **Ejecutar tarea**: seleccione una o más tareas del cliente y ejecútelas en el dispositivo seleccionado. **Nueva tarea**: cree una nueva tarea del cliente. Seleccione una tarea y configure la aceleración (opcional) para esta tarea. La tarea se pone en la cola de acuerdo con los parámetros de la tarea. Esta opción desencadena inmediatamente una tarea existente que usted selecciona de una lista de tareas disponibles. El desencadenador no está disponible para esta tarea, ya que se ejecuta inmediatamente. **Tareas recientes** - Lista de las tareas del cliente recientes de todos los grupos y ordenadores.	✔	✔
Soluciones	**Activar ESET Inspect On-Prem**: haga clic en junto a un grupo estático y seleccione **Soluciones** > **Activar ESET Inspect On-Prem** para activar y habilitar ESET Inspect On-Prem en el ordenador. **Habilitar ESET LiveGuard** –Haga clic en un ordenador o en el icono del engranaje situado junto a un grupo estático y seleccione **Soluciones** > **Activar ESET LiveGuard** para activar 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 del grupo seleccionado.	✔	x
Administrar políticas	Administre las políticas asignadas al grupo seleccionado.	✔	✔
Modificar...	Permite realizar modificaciones en el grupo seleccionado. Se aplican los mismos ajustes que cuando se crea un grupo nuevo (estático o dinámico).	✔	✔
Mover	Seleccione un grupo y muévalo como un subgrupo de otro grupo.	✔	✔
Eliminar	Elimina el grupo seleccionado.	✔	✔
Aplicar antes **Aplicar más tarde**	Cambie el nivel de prioridad de un grupo dinámico.	x	✔
Importar	Importar una lista (normalmente un archivo de texto) de ordenadores como miembros del grupo seleccionado. Si ya existen los ordenadores miembros de este grupo, el conflicto se resolverá según la acción seleccionada.	✔	x
Exportar	Exportar los miembros del grupo (y los subgrupos, si se seleccionan) a una lista (archivo *.txt*). Esta lista se puede utilizar para revisarla o importarla después.	✔	x

Detalles de grupo

Cuando seleccione la acción de grupo **Mostrar detalles**, podrá ver información general del grupo seleccionado:

Información general:

En **Información general** puede modificar la configuración del grupo haciendo clic en o en **Agregar descripción**. Puede ver información sobre la colocación del grupo, su **Grupo principal** y sus **Grupos secundarios**. Si el grupo seleccionado es un Grupo dinámico, también puede ver la operación y las reglas según las que se evalúan los ordenadores y se asignan al grupo.

Tareas

Puede ver y modificar las tareas del cliente asignadas al grupo.

Políticas

Puede asignar una política existente al grupo o crear una nueva política. Puede ver y modificar las políticas asignadas al grupo.

> Solo puede ver las políticas asignadas al grupo seleccionado. No puede ver las políticas aplicadas a ordenadores concretos del grupo.

Las políticas se aplican en función de su orden (columna **Orden de políticas**). Para cambiar la prioridad de la aplicación de políticas, marque la casilla de verificación situada junto a una política y haga clic en los botones **Aplicar antes** o **Aplicar más tarde**.

Alertas

La lista de alertas de los ordenadores del grupo. Puede administrar la alertas a través de acciones con un clic.

Exclusiones

La 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
- Servir de grupos principales de los usuarios

Grupo de inicio – El grupo de inicio 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 derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "Department_1" como **grupo de inicio** de la tarea del cliente.

Si el grupo de inicio preseleccionado no cumple sus expectativas, puede seleccionar uno manualmente.

Los grupos estáticos solo se pueden crear manualmente. Los dispositivos pueden moverse a los grupos manualmente. Cada ordenador o dispositivo móvil solo puede pertenecer a un grupo estático. La administración de los grupos estáticos está disponible mediante acciones de grupo.

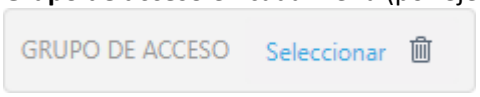
Hay dos grupos estáticos predeterminados:

- **Todo**: este es un grupo principal para todos los dispositivos de la red de ESET PROTECT Server. Todos los objetos creados por el administrador están (de forma predeterminada) en este grupo. Siempre se muestra, y su nombre no puede cambiarse. El acceso a este grupo otorga a los usuarios acceso a todos los subgrupos; por lo tanto, debe distribuirse con cuidado.
- **Perdidos y encontrados**: un grupo secundario del grupo **Todo**. Los nuevos ordenadores que se conectan a ESET PROTECT Server por primera vez se muestran automáticamente en este grupo. Es posible cambiar el nombre del grupo y copiar el grupo, pero no se puede eliminar ni mover.

Para mover un ordenador a otro grupo estático, haga clic en el ordenador, seleccione **Administrar** > **Mover a grupo**, seleccione el grupo estático de destino y haga clic en **Aceptar**.

Un grupo estático solo puede eliminarse si:
- El usuario tiene permiso de escritura en este grupo
- El grupo está vacío

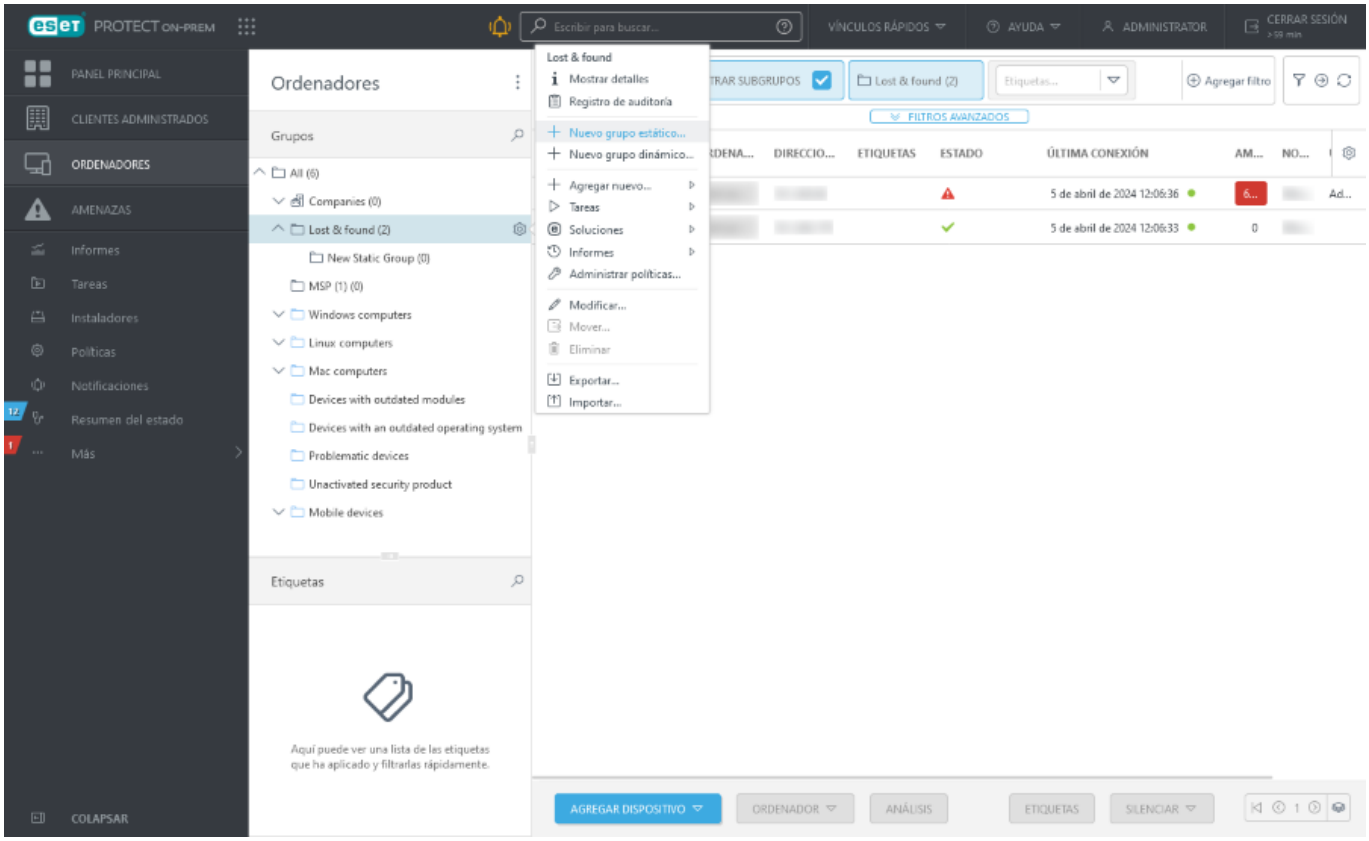
Si quedan objetos en el grupo estático, la operación de eliminación fallará. Hay un botón de filtrado de **Grupo de acceso** en cada menú (por ejemplo, **Instaladores**) con objetos.



Haga clic en **Seleccionar** para elegir un grupo estático: a continuación, solo los objetos contenidos en este grupo se mostrarán en la vista. Con esta vista filtrada, el usuario puede manipular fácilmente los objetos de un grupo.

Cree un grupo estático nuevo

Para crear un nuevo grupo estático, haga clic en **Ordenadores**, seleccione el icono del engranaje junto a un grupo estático y seleccione **Nuevo grupo estático**.



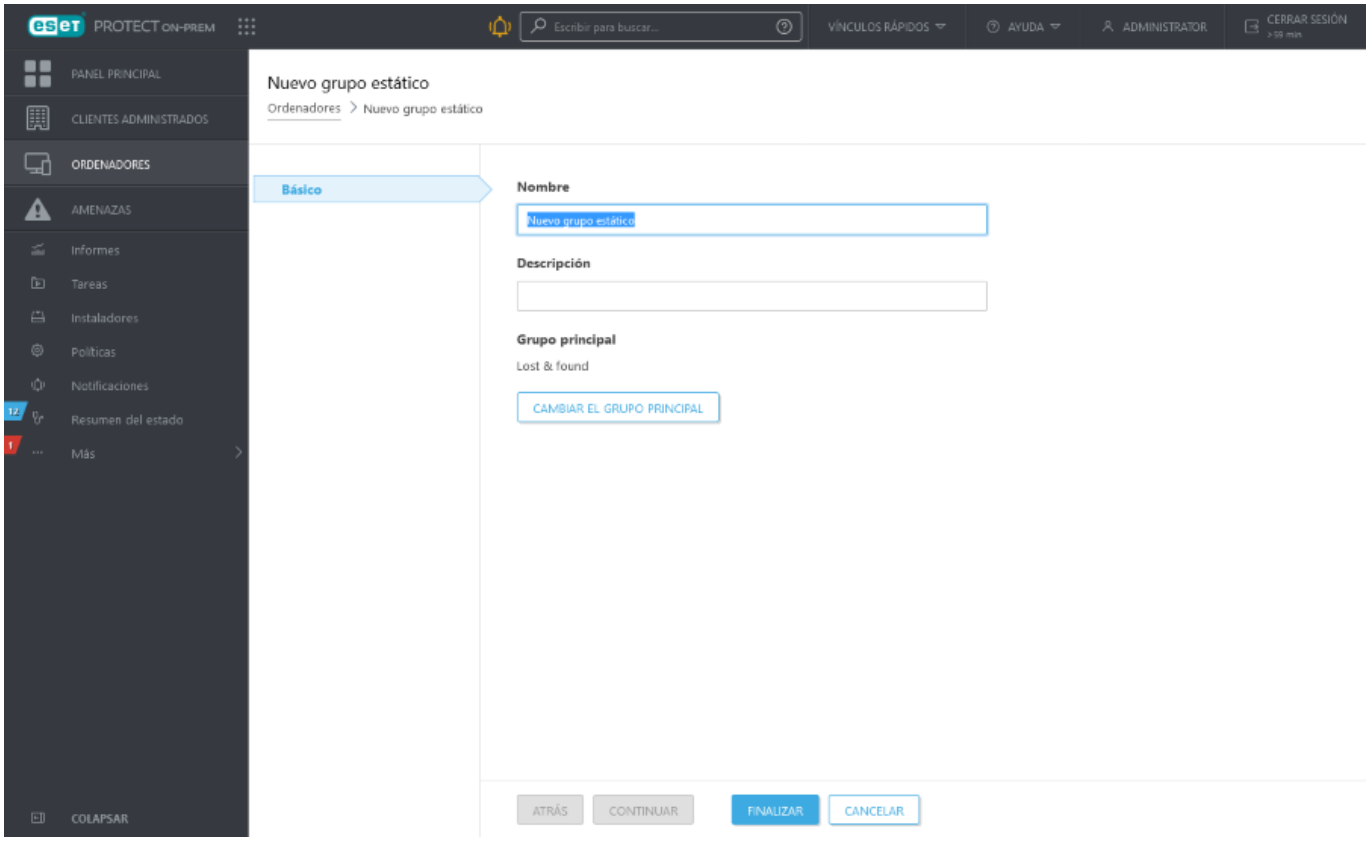
Básico

Introduzca un **nombre** y una **descripción** del grupo nuevo.

- También puede cambiar el **Grupo principal**. De forma predeterminada el grupo principal es el grupo que seleccionó cuando comenzó a crear el nuevo grupo estático. Si desea cambiar el grupo principal, haga clic en **Cambiar el grupo principal** y seleccione un grupo principal en el árbol.

- El grupo principal del nuevo grupo estático debe ser un grupo estático. No es posible incluir un grupo estático en un grupo dinámico.

Haga clic en **Finalizar** para crear un nuevo grupo estático.



Importar clientes desde Active Directory

Para importar clientes desde AD, cree una nueva tarea del servidor. Sincronización de grupos estáticos.

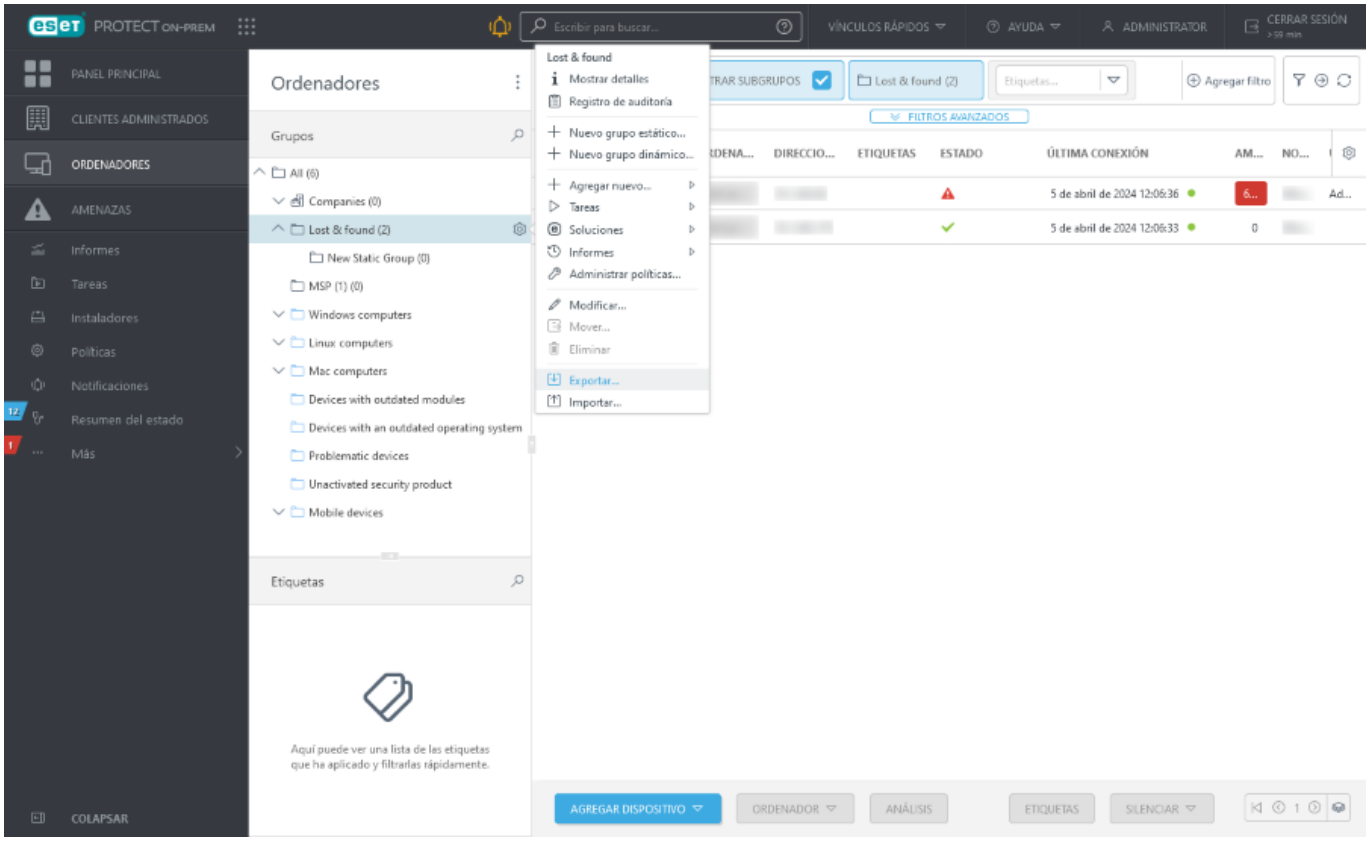
Seleccione el grupo al que quiere agregar los ordenadores nuevos desde el AD. También puede seleccionar los objetos del AD que desea sincronizar y qué hacer con los duplicados. Introduzca los ajustes de conexión del servidor del AD y establezca el modo de sincronización en **Active Directory/Open Directory/LDAP**.

Exportar grupos estáticos

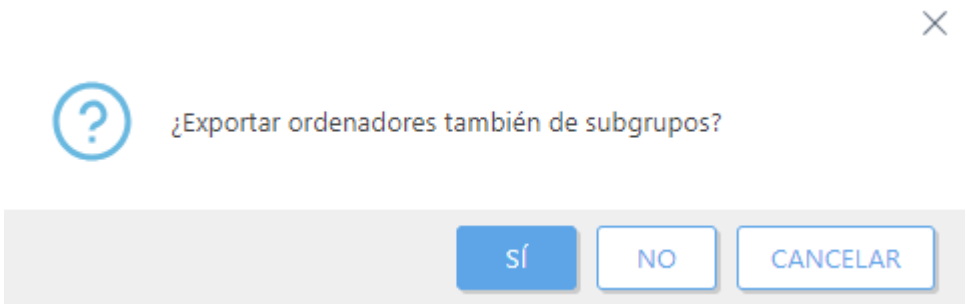
Exportar una lista de ordenadores que estén en la estructura de ESET PROTECT On-Prem es sencillo. Puede exportar la lista y almacenarla como una copia de seguridad para poder importarla de nuevo en el futuro, por ejemplo, si desea restaurar la estructura del grupo.

Los grupos estáticos deben contener al menos un ordenador, no se pueden exportar grupos vacíos.

1. Vaya a **Ordenadores** y seleccione el grupo estático que desee exportar.
2. Haga clic en el icono del engranaje y seleccione **Exportar**.



3. Si el grupo estático seleccionado contiene subgrupos con ordenadores, también puede exportar los ordenadores de los subgrupos.

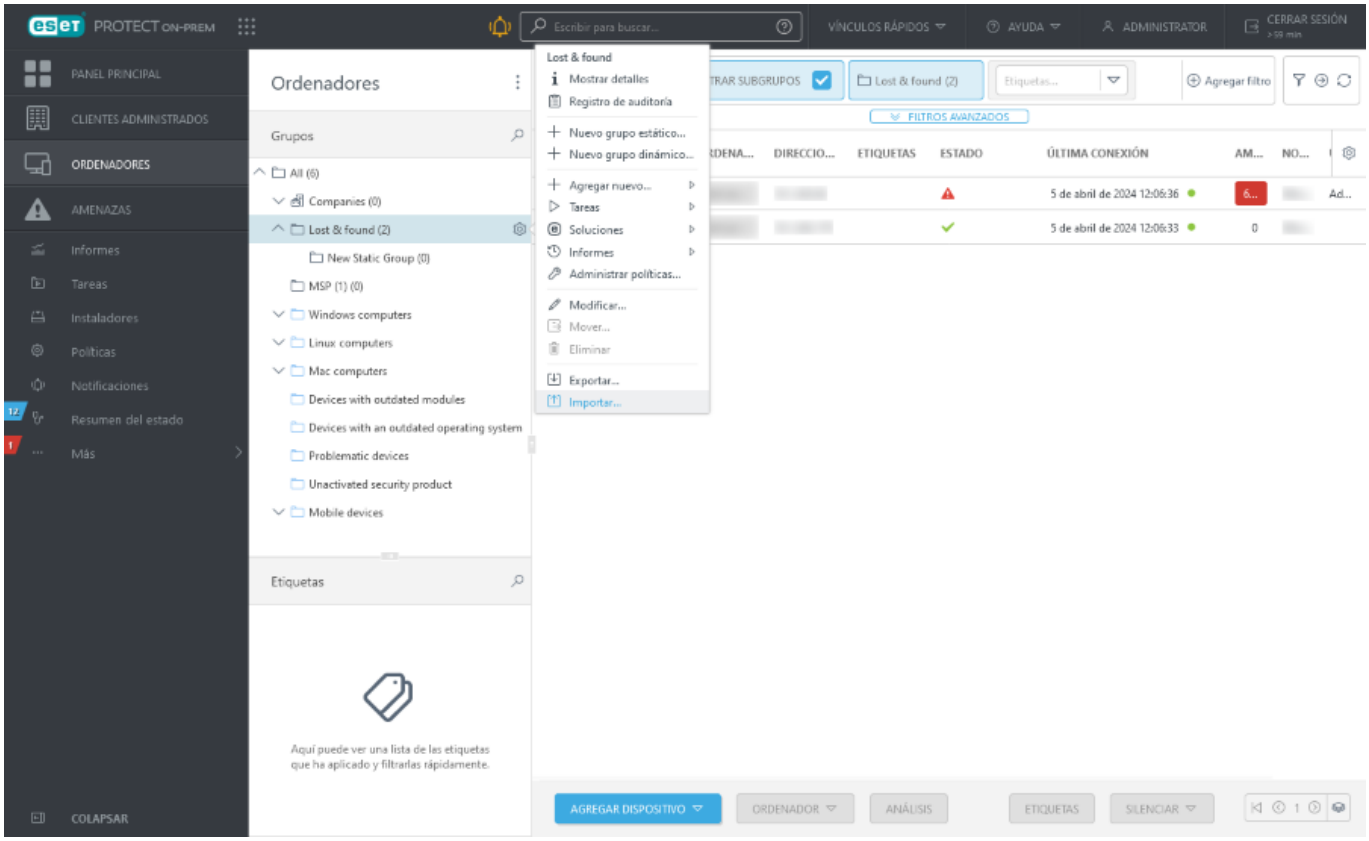


4. El archivo se guardará en formato *.txt*.

> los grupos dinámicos no se pueden exportar porque estos grupos son solo enlaces a ordenadores de acuerdo a los criterios definidos en las plantillas de grupos dinámicos.

Importar grupos estáticos

Los archivos exportados desde grupos estáticos se pueden importar de nuevo a ESET PROTECT Web Console e incluirlos en la estructura de grupos existentes.



1. Haga clic en **Ordenadores** y seleccione cualquier grupo estático.

2. Haga clic en el icono del engranaje y seleccione **Importar**.

3. Haga clic en **Examinar** y diríjase al archivo *.txt*. Cada línea del archivo debe contener una ruta de acceso completa al nombre del ordenador o la 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 el grupo estático existe y los ordenadores del archivo *.txt* ya existen en este grupo, esos ordenadores se omiten y no se importan. Se mostrará un aviso.

- **Mover los dispositivos existentes si aún no existen en las rutas importadas. Siempre que sea posible, mantenga solo dispositivos administrados en la misma ruta.**: si el grupo estático ya existe y los ordenadores del archivo *.txt* ya existen en este grupo, es necesario mover los ordenadores a otros grupos estáticos antes de la importación, y después de la importación se trasladan de nuevo a sus grupos originales desde donde se han 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 ordenador original se muestra con la información completa y el duplicado se

muestra solo con su nombre de ordenador.

6. Haga clic en **Importar** para importar el grupo estático y los ordenadores.

Árbol de grupos estáticos para ESET Business Account/ESET MSP Administrator

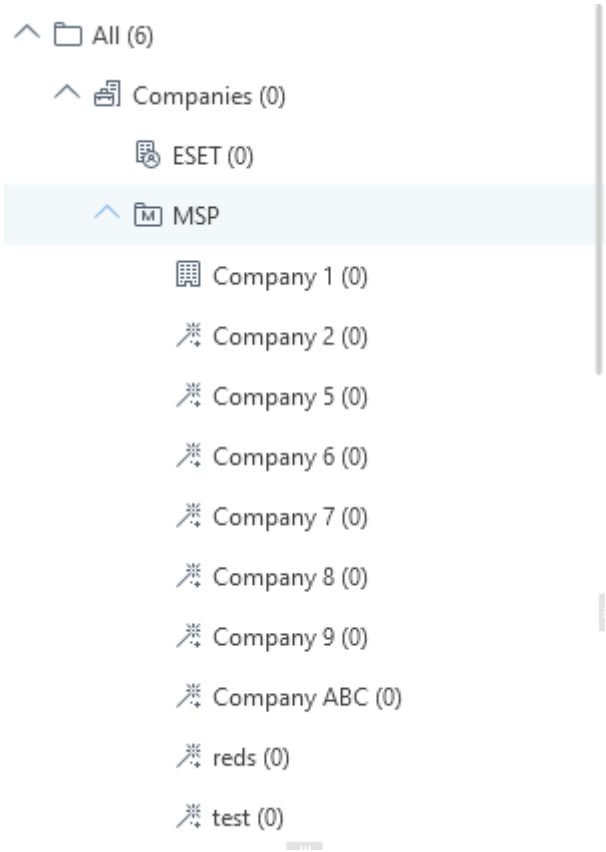
Si importa licencias desde ESET Business Account, la estructura de la empresa ESET Business Account (incluidos los sitios) aparece en el árbol de grupo estático (una nueva función de la versión 9.1 de ESET PROTECT On-Prem).

Si importa licencias desde ESET MSP Administrator, la estructura ESET MSP Administrator aparece en el árbol de grupo estático. Más información sobre ESET PROTECT On-Prem para proveedores de servicios administrados.

Estructura de árbol de grupos estáticos para ESET Business Account/ESET MSP Administrator

Puede ver la estructura de árbol de grupos estáticos para ESET Business Account/ESET MSP Administrator de **Ordenadores** en el árbol de grupos estáticos ubicado en **Todos** > **Empresas**.

> Le recomendamos que utilice una cuenta en línea (ESET Business Account o ESET MSP Administrator; consulte también Introducción a ESET Business Account) y la sincronice con ESET PROTECT On-Prem para aprovechar todo el potencial de ESET PROTECT On-Prem.
> Si activó ESET PROTECT On-Prem con una clave de licencia o una licencia sin conexión y no sincronizó las licencias de ESET Business Account o ESET MSP Administrator, no verá ESET Business Account ni ESET MSP Administrator en la estructura de árbol de grupos estáticos.



En **Empresas** puede ver uno o más árboles de ESET Business Account o ESET MSP Administrator, en función de las cuentas sincronizadas en Administración de licencias.

Si tiene una cuenta de ESET MSP Administrator, consulte los detalles sobre la estructura de las entidades en los MSP.

Sincronización del sitio de ESET Business Account

Si tiene sitios de ESET Business Account, ESET PROTECT On-Prem los sincroniza automáticamente con el árbol de Grupo estático y asigna licencias de cada sitio al Grupo estático de sitio correspondiente (marcado con el icono) en la empresa de ESET Business Account .

- Se recomienda utilizar el sitio de grupos estáticos creado automáticamente para administrar los sitios (en lugar de crear los grupos estáticos manualmente).
- Debe crear administradores de sitios y asignar sus permisos manualmente. Seleccione el grupo estático del sitio correspondiente como grupo de inicio de cada administrador del sitio y asigne al administrador un conjunto de permisos con el mismo grupo de inicio.

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 inicio (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 de sitio solo puede ver su sitio y sus objetos (por ejemplo, licencias).

Si sincroniza un sitio en la estructura de árbol de grupos estáticos 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 de grupos estáticos y elimina el sitio en ESET Business Account, su icono en ESET PROTECT On-Prem cambiará a .

Objetos compartidos

La estructura de árbol de grupos estáticos de ESET Business Account o ESET MSP Administrator contiene grupos estáticos dedicados adicionales denominados **Objetos compartidos**.

Puede utilizar **Objetos compartidos** para compartir objetos de Web Console (políticas, plantillas de grupos dinámicos, etc.) con 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 Web Console. 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 de **Uso** de **Objetos compartidos**.

- Asegúrese de que no se asigne el permiso de **Escritura** de **Objetos compartidos** a usuarios limitados para evitar que los editen. El permiso de **Uso** es suficiente.
- No puede almacenar ordenadores en **Objetos compartidos**. Los **Objetos compartidos** no están visibles en **Grupos** en **Ordenadores**.

Grupos dinámicos

Los grupos dinámicos pueden considerarse filtros basados en el estado del ordenador. Un ordenador podría corresponder a más de un filtro y, por lo tanto, asignarse a más de un grupo dinámico. Esto diferencia a los grupos dinámicos de los grupos estáticos, puesto que un cliente individual no puede pertenecer a más de un grupo estático.

Los grupos dinámicos son grupos de clientes seleccionados con base en condiciones específicas. Para que un ordenador se convierta en miembro de un grupo dinámico concreto, debe cumplir las condiciones definidas en una plantilla de grupo dinámico. Cada plantilla está compuesta por una o varias Reglas. Durante la creación de una nueva plantilla puede especificar estas reglas. Si un ordenador cliente no cumple los criterios, se quita del

grupo. Si cumple las condiciones definidas, se añadirá al grupo.

Se realiza una evaluación de los clientes para incluirlos en grupos dinámicos cada vez que se registran en ESET PROTECT On-Prem. Cuando un dispositivo cumple los valores especificados en una plantilla de grupos dinámicos, se asigna automáticamente a este grupo. Los ordenadores se filtran en el lado del agente, por lo que no es necesario transferir información adicional al servidor. El agente decide por sí solo a qué grupos dinámicos pertenece un cliente y solamente notifica al servidor su decisión.

> **i** Si el dispositivo cliente no está conectado (por ejemplo, si está apagado), su pertenencia a los grupos dinámicos no se actualizará. Cuando el dispositivo vuelva a conectarse, se actualizará su pertenencia a los grupos dinámicos.

Después de instalar ESET PROTECT On-Prem existen varios grupos dinámicos predefinidos a su disposición. También puede crear grupos dinámicos personalizados. Existen dos formas de hacerlo:

- Crear una plantilla primero y luego crear un grupo dinámico.
- Crear una plantilla nueva al crear un nuevo grupo dinámico.

Puede utilizar grupos dinámicos en otras partes de ESET PROTECT On-Prem. Es posible asignarles políticas (consulte cómo se aplican las políticas) o preparar una tarea para todos los ordenadores del grupo.

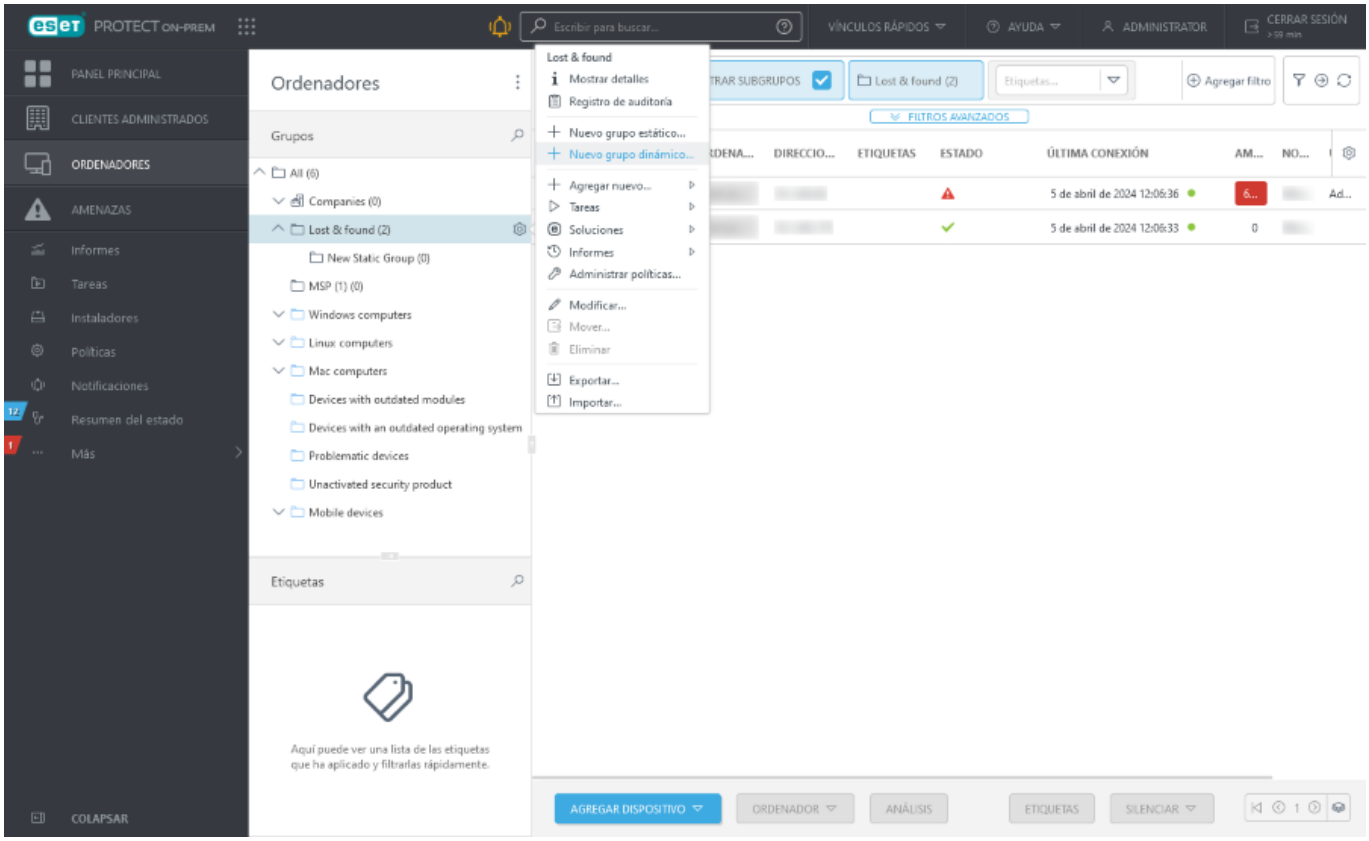
Los grupos dinámicos pueden estar dentro (bajo) de grupos estáticos o en grupos dinámicos. Sin embargo, el grupo estático no puede estar dentro de un grupo dinámico. Todos los grupos dinámicos que estén debajo de un determinado grupo estático solo filtran los dispositivos de ese grupo estático. Si un grupo dinámico está dentro de otro grupo dinámico, filtra los resultados del grupo dinámico superior. Cuando el grupo se crea, se puede mover con libertad por el árbol.

La administración de los grupos dinámicos está disponible mediante acciones de grupo.

Crear un grupo dinámico nuevo

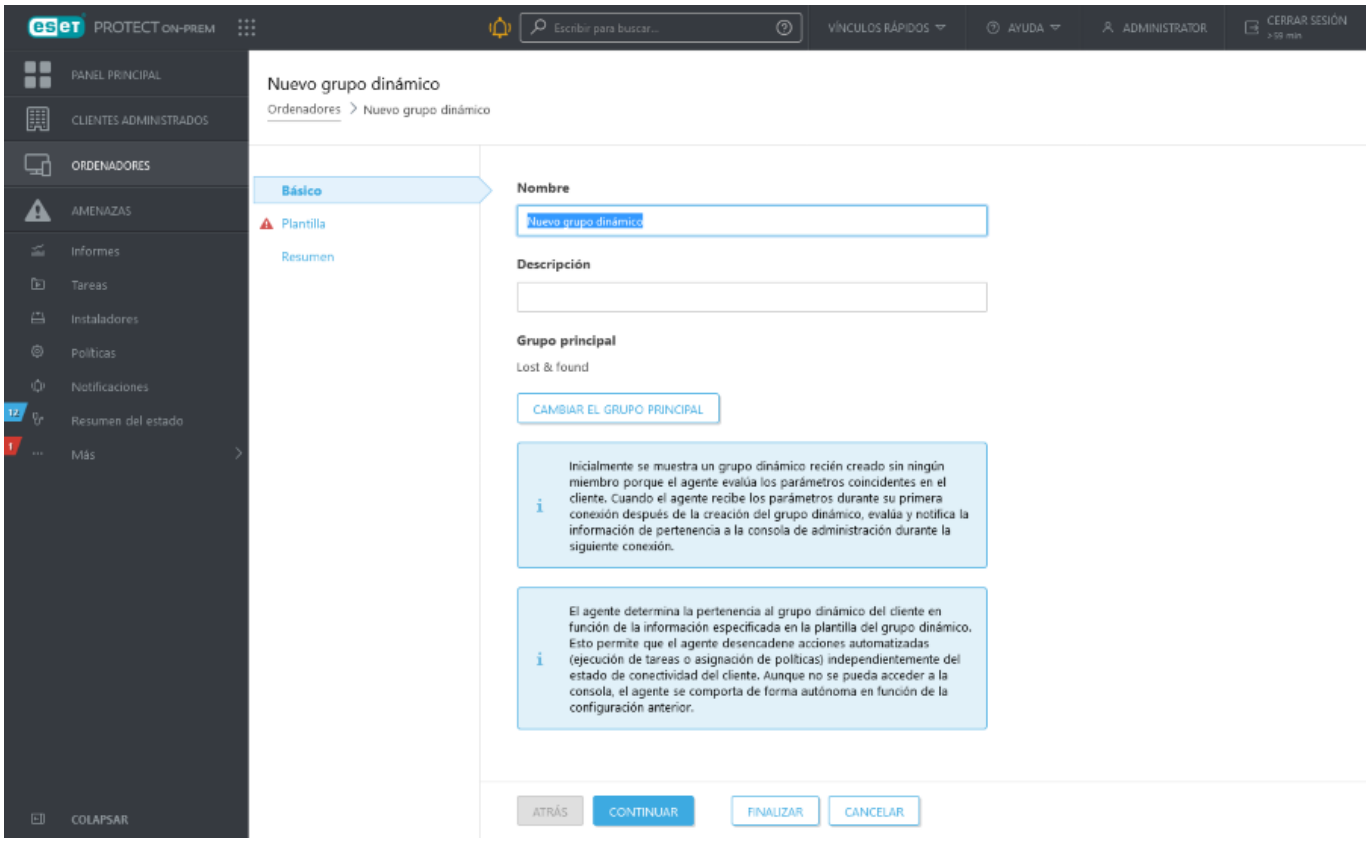
Siga estos pasos para crear un grupo dinámico nuevo.

1. Haga clic en **Ordenadores**, seleccione el icono del engranaje junto a cualquier grupo y seleccione **Nuevo grupo dinámico**. Aparecerá un Asistente para nuevo grupo dinámico.



2. Escriba el nombre y la descripción de la nueva plantilla.

3. Puede cambiar el grupo principal haciendo clic en **Cambiar el grupo principal**.



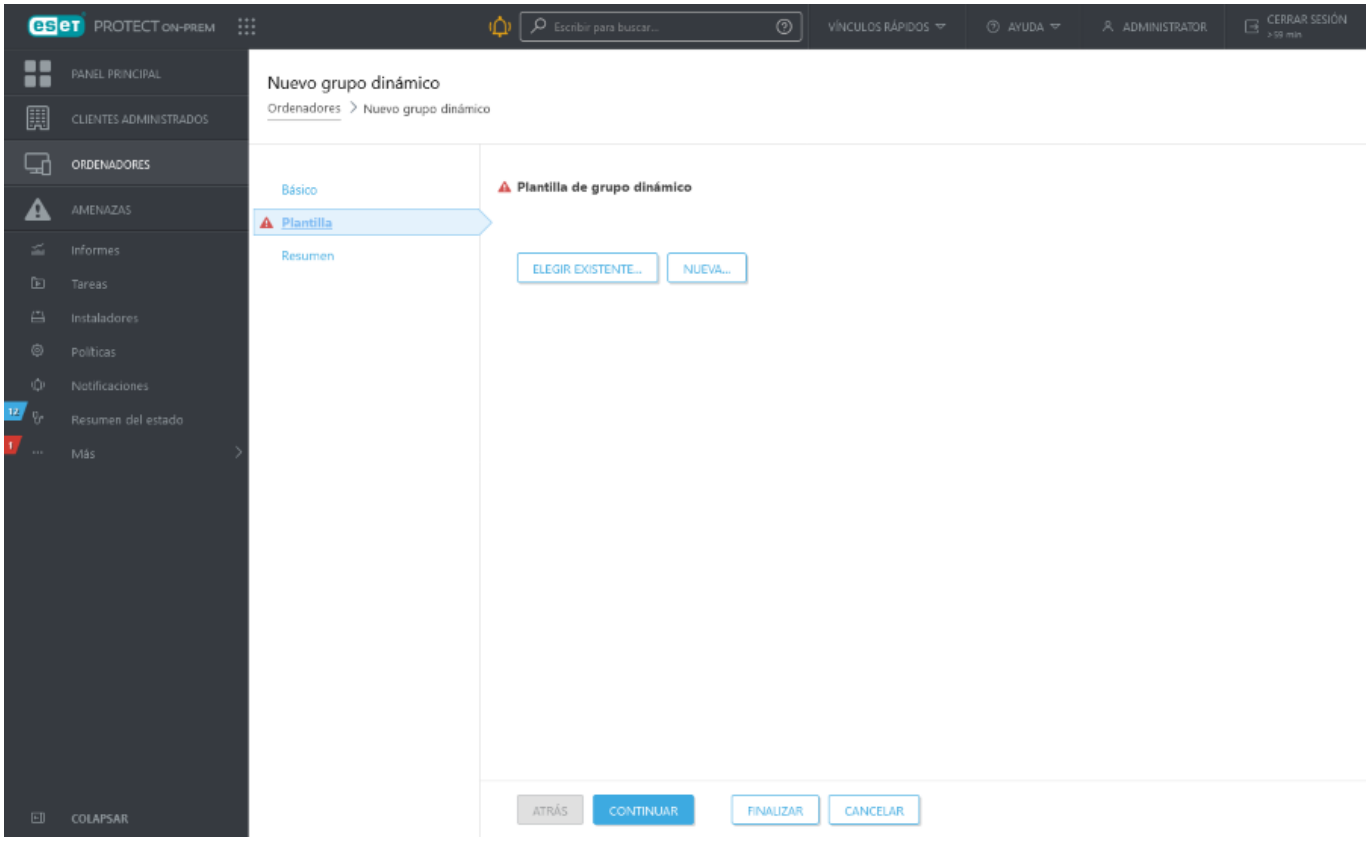
4. Haga clic en **Plantilla**. Todos los grupos dinámicos se crean a partir de una plantilla que define la forma en la que el grupo filtra los ordenadores cliente. A partir de una plantilla se puede crear un número de grupos dinámicos ilimitado.

Una plantilla es un objeto estático almacenado en un grupo estático. Los usuarios deben tener los permisos adecuados para poder acceder a las plantillas. Un usuario necesita permisos para poder trabajar con plantillas de grupos dinámicos. Todas las plantillas predefinidas se encuentran en el grupo estático **Todo** y, de manera predeterminada, solo están disponibles para el administrador. Al resto de usuarios se les tendrán que asignar permisos adicionales. Por ello, los usuarios podrían no ver o utilizar las plantillas predeterminadas. Las plantillas pueden moverse a un grupo en el que los usuarios tengan permisos. Para duplicar una plantilla, el usuario debe tener asignados permisos de **Uso** (para plantillas de grupo dinámico) para el grupo en el que está la plantilla de origen y permisos de **Escritura** para el grupo de inicio del usuario (donde se almacenará el duplicado). Consulte el ejemplo de duplicación de objetos.

- Si quiere crear el grupo desde una plantilla predefinida o desde una plantilla que ya haya creado, haga clic en **Elegir existente** y seleccione en la lista la plantilla correspondiente.

- Si no ha creado todavía ninguna plantilla, y no hay ninguna predefinida en la lista que le convenga, haga clic en **Nuevo** y siga los pasos para crear una plantilla nueva.

Para conocer más casos de uso sobre cómo crear un nuevo grupo dinámico a partir de una plantilla de grupo dinámico con reglas, consulte los ejemplos.



5. Haga clic en **Resumen**. El nuevo grupo aparecerá bajo el grupo principal.

Mover grupo estático o dinámico

Un grupo dinámico puede ser miembro de cualquier otro grupo, incluidos los estáticos. Un grupo estático no se puede mover a un grupo dinámico. Tampoco es posible mover grupos estáticos predefinidos (por ejemplo, el grupo estático **Perdidos y encontrados**) a ningún otro grupo. Los demás grupos se pueden mover libremente.

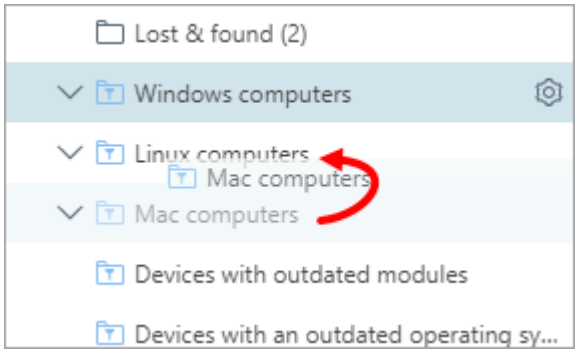
Haga clic en el icono del engranaje que aparece junto al nombre del grupo y seleccione **Mover**. Se mostrará

una ventana que muestra la estructura de árbol del grupo. Seleccione el grupo destino (estático o dinámico) al que desea mover el grupo seleccionado. El grupo destino se convertirá en el grupo principal. También puede mover grupos arrastrando y soltando un grupo en el grupo destino que desee.

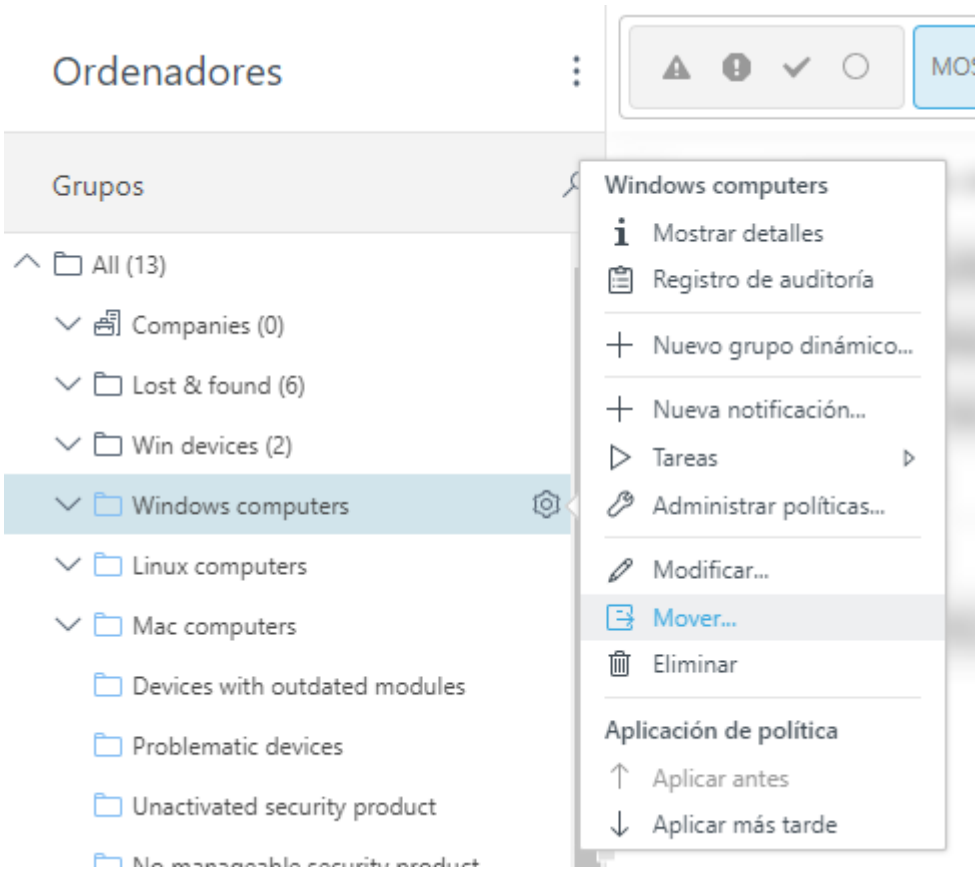
> El grupo dinámico en una nueva posición comienza a filtrar los ordenadores (según la plantilla) sin ninguna relación con su ubicación anterior.

Un grupo se puede mover de tres formas:

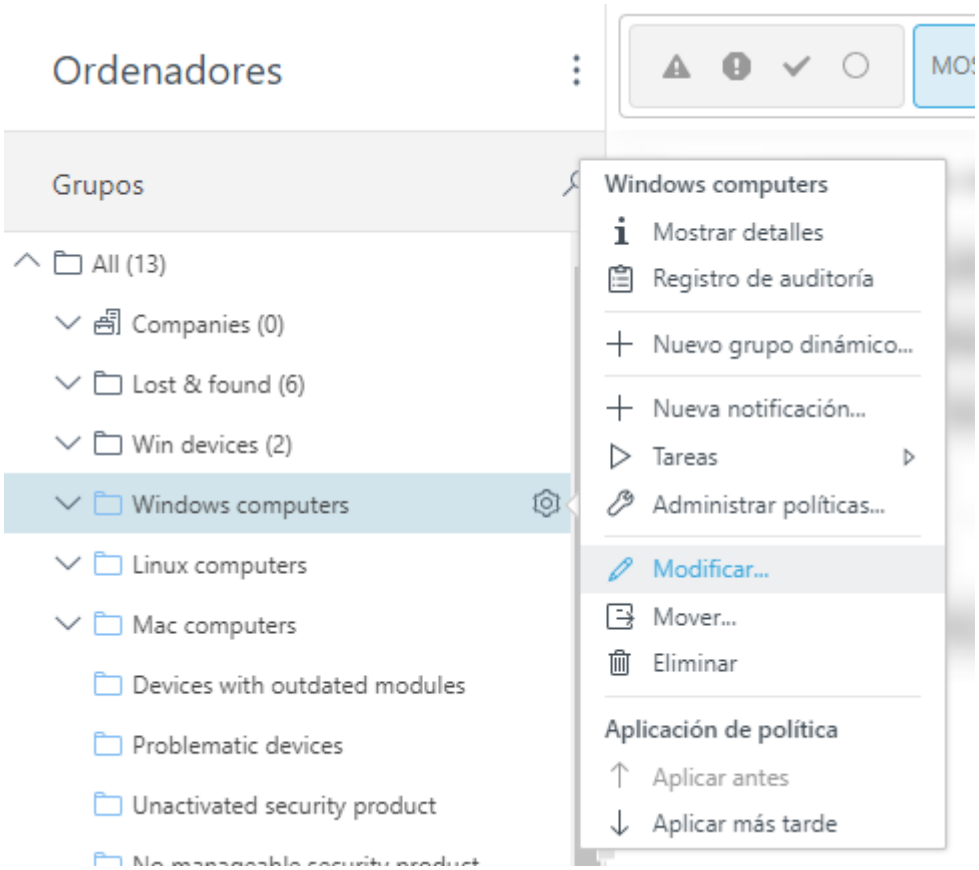
- **Arrastrar y soltar**: haga clic y mantenga pulsado el grupo que desea mover y suéltelo encima del grupo principal nuevo.



- Haga clic en el icono del engranaje > **Mover** > seleccione un grupo principal nuevo de la lista y haga clic en **Aceptar**.

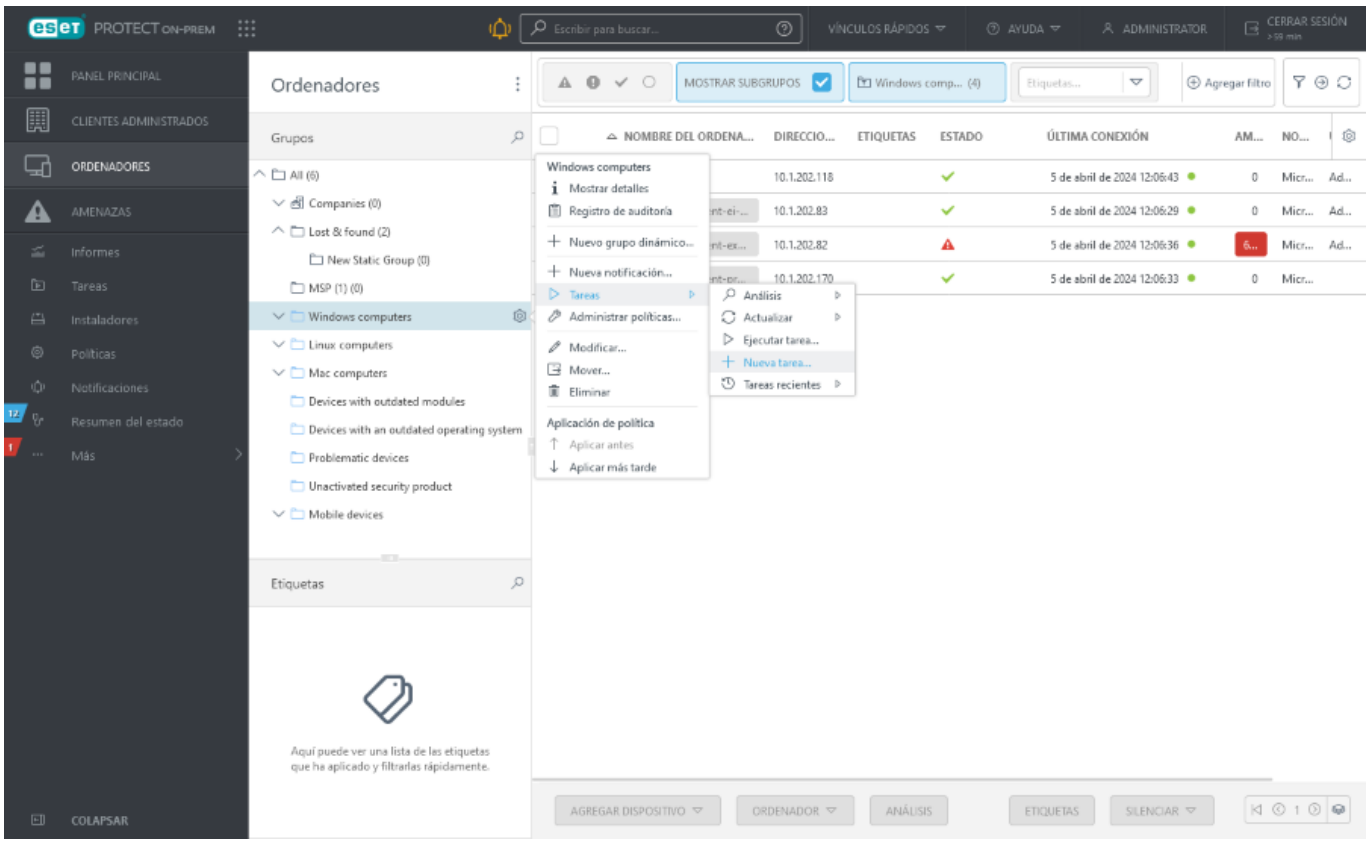


- Haga clic en el icono del engranaje > **Modificar >** seleccione **Cambiar el grupo principal**. Seleccione un grupo principal nuevo de la lista y haga clic en **Aceptar**.



Asignar una tarea del cliente a un grupo

Haga clic en **Ordenadores**, seleccione **Grupo estático** o **Grupo dinámico** y haga clic en el icono del engranaje > **Tareas** > **Nueva tarea**. Se abrirá la ventana del Asistente para nueva tarea del cliente.

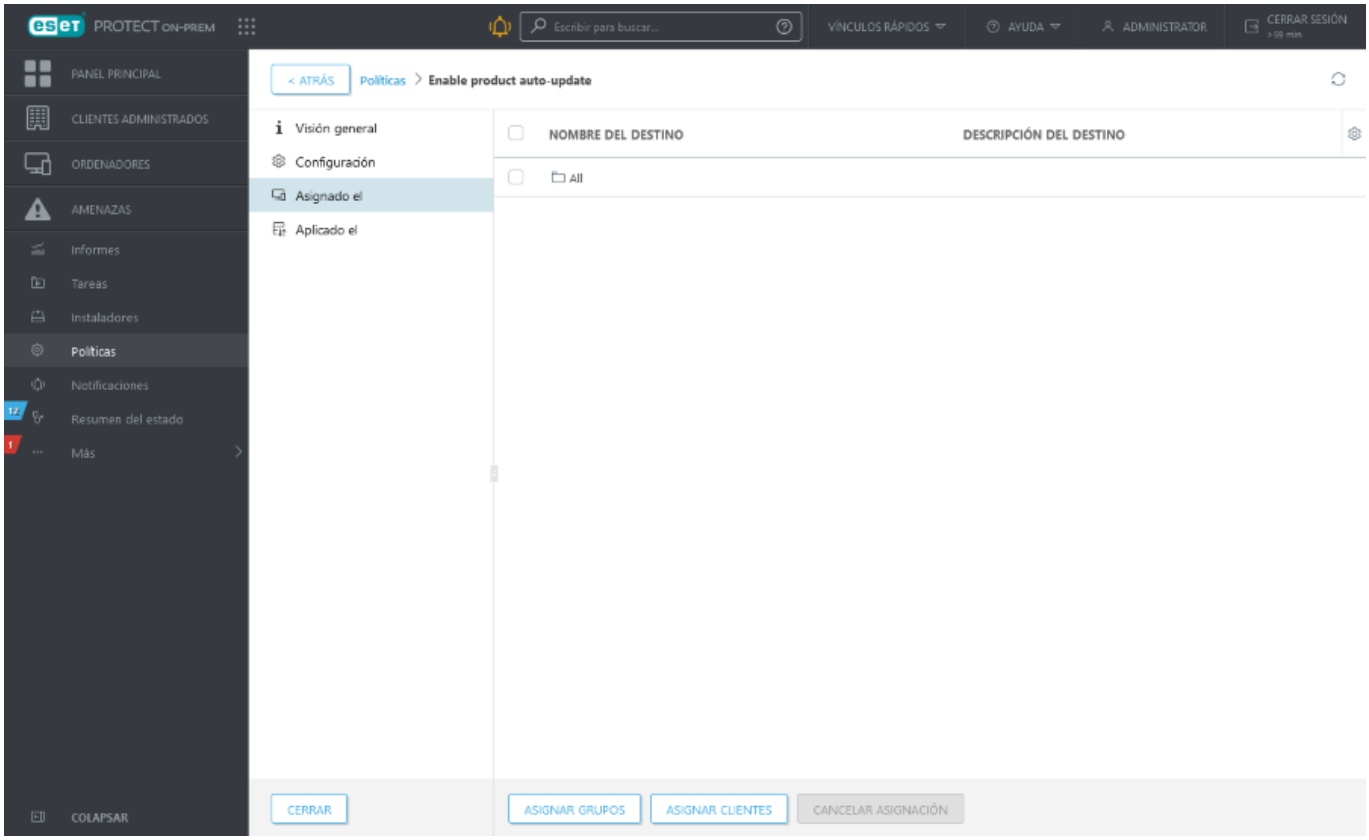


Asignar una política a un grupo

Después de crear una política, puede asignarla a un **grupo estático** o **dinámico**. Hay dos formas de asignar una política:

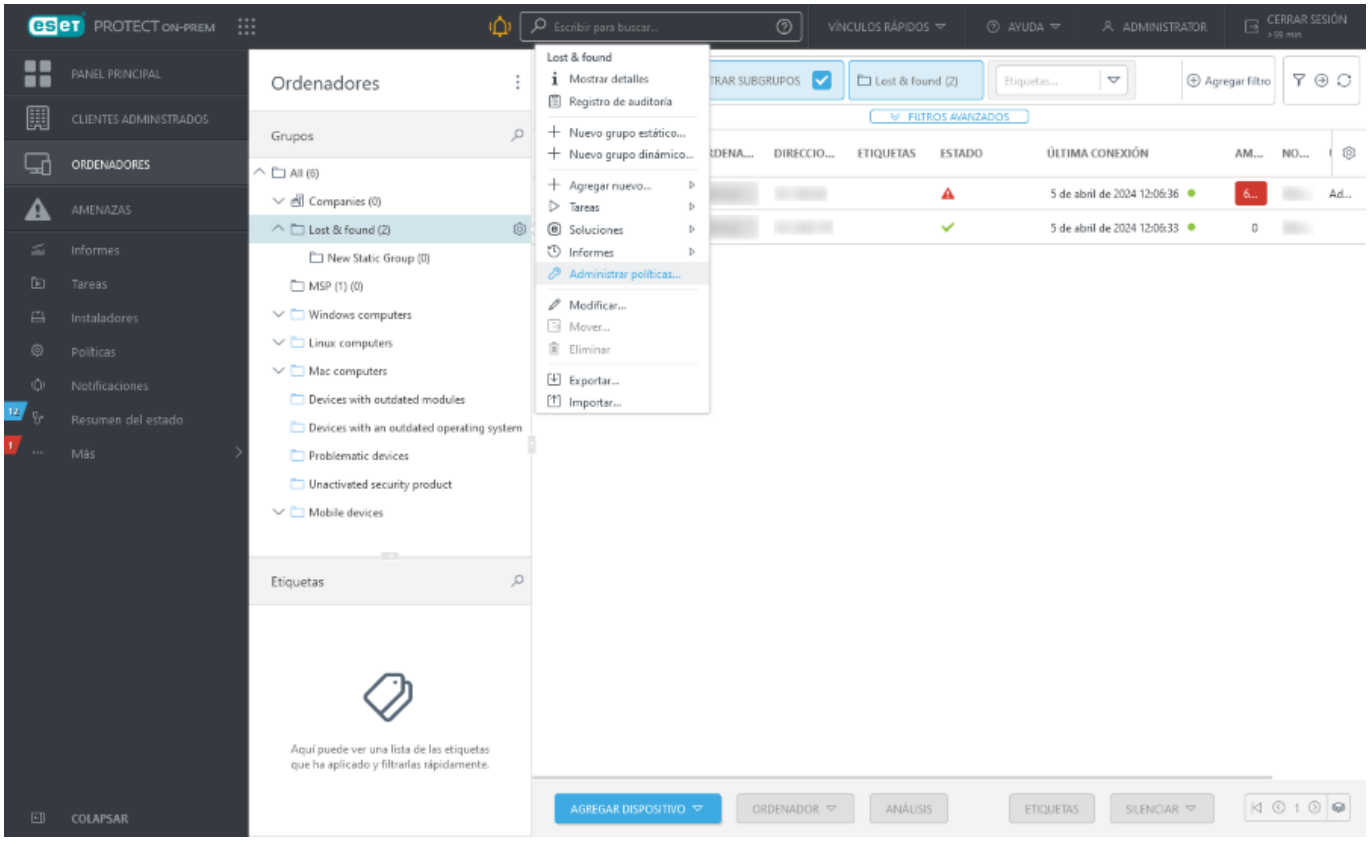
Método I.

En **Políticas**, seleccione una política y haga clic en **Acciones** > **Mostrar detalles** > **Asignado el** > **Asignar grupos**. Seleccione un grupo estático o dinámico en la lista (puede seleccionar más grupos) y haga clic en **Aceptar**.



Método II.

1. Haga clic en **Ordenadores**, haga clic en el icono del engranaje junto al nombre del grupo y seleccione **Administrar políticas**.



2. En la ventana **Orden de aplicación de directiva** haga clic en **Agregar directiva**.

3. Marque la casilla de verificación situada junto a la política que desea asignar a este grupo y haga clic en **Aceptar**.

4. Haga clic en **Cerrar**.

Para ver qué políticas están asignadas a un grupo determinado, seleccione ese grupo y haga clic en la ficha **Políticas** para ver una lista de políticas asignadas al grupo.

Para ver qué grupos están asignados a una política concreta, seleccione la política y haga clic en **Mostrar detalles** > **Aplicada a**.

> para obtener más información acerca de las políticas, consulte el capítulo Políticas.

Detecciones

En la sección **Detecciones** se muestra una descripción general de las detecciones encontradas en los dispositivos administrados.

La estructura del grupo se muestra a la izquierda. Puede examinar los grupos y ver las detecciones encontradas en miembros de un grupo determinado. Para ver todas las detecciones encontradas en los clientes asignados a grupos de su cuenta, seleccione el grupo **Todo** 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

Existen dos tipos de detecciones en función de su estado:

- **Detecciones activas**: las detecciones activas son detecciones que aún no se han desinfectado. Para desinfectar la detección, ejecute un **Análisis exhaustivo** con desinfección activada en la carpeta que contiene la detección. La tarea de análisis debe finalizar correctamente para desinfectar la detección y dejar de tener detecciones. Si el usuario no resuelve una detección activa durante las 24 horas posteriores a su detección, pierde el estado de **Activa**, pero se mantiene sin resolver.

- **Detecciones resueltas**: son detecciones marcadas por un usuario como resueltas; sin embargo, aún no se han analizado con **Análisis exhaustivo**. Los dispositivos con detecciones marcadas como resueltas se mostrarán en la lista de resultados filtrados hasta que se realice el análisis.

El estado **Detección gestionada** indica si un producto de seguridad de ESET realizó una acción contra una detección (en función del tipo de detección y los ajustes de nivel de desinfección):

- **Sí**: el producto de seguridad de ESET realizó una acción contra la detección (eliminar, desinfectar o poner en cuarentena).

- **No**: el producto de seguridad de ESET no realizó ninguna acción contra la detección.

Puede utilizar **Detección gestionada** como filtro en Informes, Notificaciones y Plantillas de grupos dinámicos.

No todas las detecciones encontradas en los dispositivos cliente se mueven a la cuarentena. Entre las detecciones que no se mueven a la cuarentena se incluyen las siguientes:
- Detecciones que no se pueden eliminar
- Detecciones sospechosas por su comportamiento, pero no identificadas como malware, por ejemplo, las PUA.

Durante la limpieza de la base de datos, los elementos de Detecciones que corresponden a los registros de incidentes desinfectados también se eliminan (sea cual sea el estado de la detección). De forma predeterminada, el periodo de limpieza de registros de incidentes (y detecciones) está establecido en 6 meses. Puede cambiar el intervalo en **Más** > Configuración.

Agregación de detecciones

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

Detecciones en archivos comprimidos

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

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

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

Filtrado de detecciones

De forma predeterminada, se muestran todos los tipos de detección de los últimos siete días, incluidas las detecciones correctamente desinfectadas. Puede filtrar las detecciones con diversos criterios: **Ordenador silenciado y Ocurrió** están activados de forma predeterminada.

Algunos filtros están activados de forma predeterminada. Si las detecciones se indican en el botón **Detecciones** del menú principal, pero no puede verlas en la lista de detecciones, compruebe los filtros activados.

Agrupación de detecciones

Para agrupar las detecciones, seleccione en el menú desplegable:

- **Sin agrupar**: vista predeterminada
- **Agrupadas por ordenador**: detecciones agrupadas por nombre de ordenador
- **Agrupadas por categoría**: detecciones agrupadas por categoría de detección
- **Agrupadas por tipo**: detecciones agrupadas por categoría de detección y su tipo de detección
- **Agrupadas por hash**: detecciones agrupadas por hash
- **Agrupadas por causa**: detecciones agrupadas por causa
- **Agrupadas por usuario**: detecciones agrupadas por usuario

Para ver todas las detecciones agrupadas en una fila específica, haga clic en cualquier fila y en **Abrir lista de detecciones**. Se mostrará información sobre el grupo de detecciones en la parte superior de la página. Haga clic en el icono de **flecha abajo** para desplazarse por las detecciones agrupadas. Haga clic en el icono de **flecha atrás** para volver a los grupos de detecciones.

Para obtener una vista más específica, puede agregar otros filtros, como:

- **Categoría de detección**: **Antivirus**, Archivos bloqueados, ESET Inspect, **Cortafuegos**, **HIPS** y **Protección web**.
- **Tipo de detección**
- **Dirección IP** del cliente que notificó la detección.
- **Análisis**: seleccione el tipo de análisis que notificó la detección. Por ejemplo, el **análisis antirransomware** muestra las detecciones comunicadas por la protección contra ransomware.

• **Acción**: seleccione la acción realizada en la detección. Los productos de seguridad de ESET informan de las siguientes acciones a ESET PROTECT On-Prem:

o**desinfectado**: se ha desinfectado la detección.

o**eliminado/desinfectado por eliminación**: la detección se eliminó.

o**era parte de un objeto eliminado**: se ha eliminado un archivo comprimido que contenía la detección.

o**bloqueado/conexión finalizada**: se ha bloqueado el acceso al objeto detectado.

o**retenido**: no se realizó ninguna acción debido a diferentes motivos; por ejemplo:

➢ En la alerta interactiva, el usuario ha seleccionado manualmente no realizar ninguna acción.

➢ En la configuración del motor de detección del producto de seguridad de ESET, el nivel de **Protección** de la categoría de detección está establecido en un valor inferior al nivel de **Informe**.

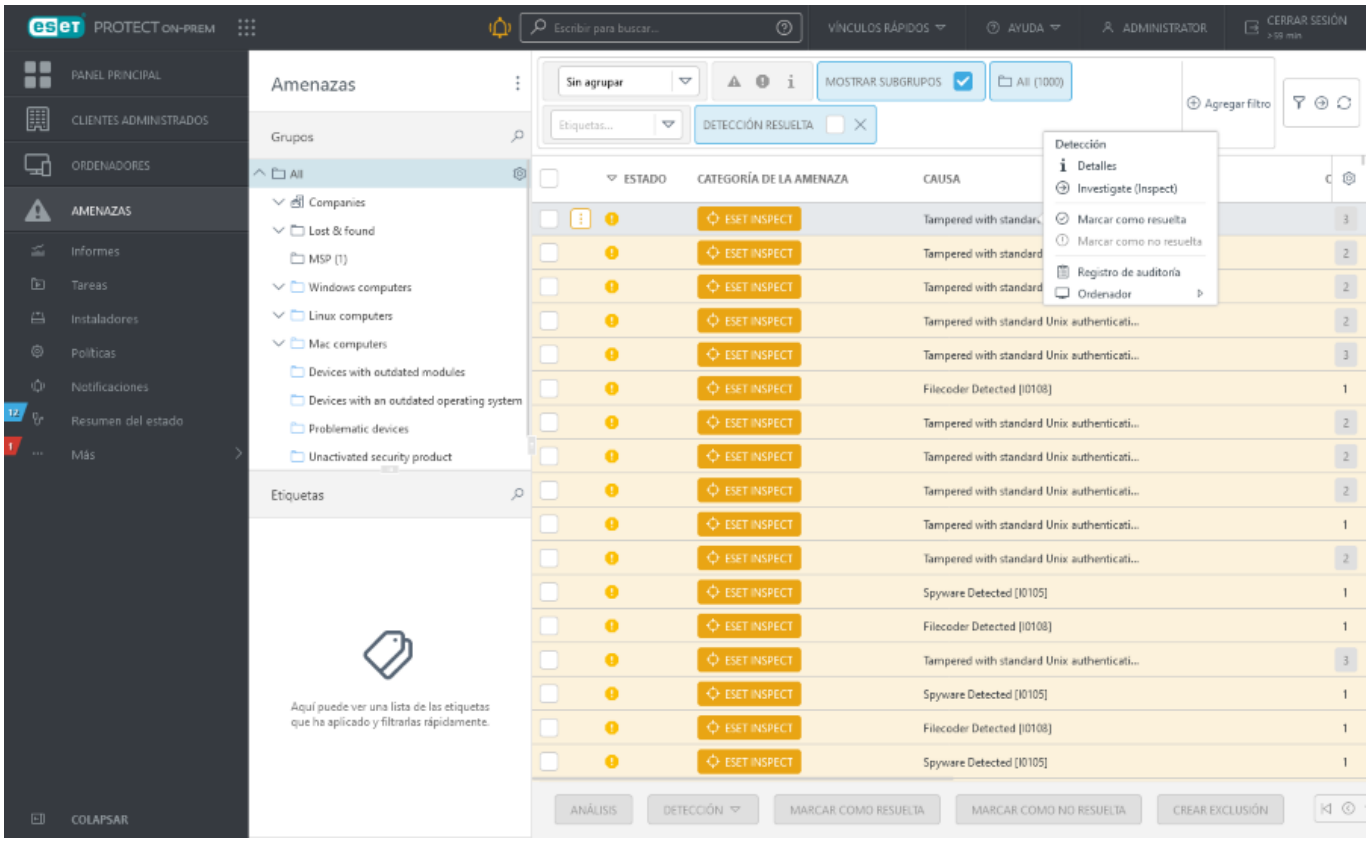
Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

• Administre el panel lateral y la tabla principal.

• Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Administrar detecciones



Haga clic en el nombre de una detección para mostrar el panel lateral Vista previa de la detección en el lateral derecho.

Para administrar las detecciones, haga clic en el elemento y seleccione una de las acciones disponibles, o bien marque la casilla de verificación situada junto a uno o más elementos y use los botones de la parte inferior de la pantalla Detecciones:

- **Análisis**: ejecuta la tarea Análisis a petición en el dispositivo desde el que se haya informado de la detección seleccionada.
- **Detalles**: vea los Detalles de la detección.
- **Ordenador**: una lista de acciones que puede realizar en el ordenador en el que se detectó la detección. Esta lista es la misma de la sección Ordenadores.
- **Registro de auditoría** - Permite 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 análisis** (disponible solo para detecciones del **Antivirus**, archivos con rutas de acceso conocidas): cree la Tarea de análisis a petición con rutas de acceso y destinos predefinidos.
- **Crear exclusión** (disponible solo para detecciones del **Antivirus** y reglas de IDS del **Cortafuegos**): crear exclusiones de detección.
- **Investigar (Inspect)** le permite abrir los detalles del elemento directamente en ESET Inspect On-Prem Web Console. El icono **Inspect** de la parte superior derecha abre la ESET Inspect On-Prem sección Detecciones de Web Console. El ESET Inspect On-Prem solo está disponible cuando tiene la licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de ESET Inspect**.
- **Enviar archivo a ESET LiveGuard** solo está disponible para **archivos bloqueados**. Puede enviar un archivo para el análisis de malware (ESET LiveGuard Advanced) desde ESET PROTECT Web Console. Puede ver los detalles del análisis del archivo en Archivos enviados. Puede enviar manualmente archivos ejecutables a ESET LiveGuard Advanced para su análisis desde el producto de ESET Endpoint (necesita tener la licencia de ESET LiveGuard Advanced).

Vista previa de la detección

En **Detecciones**, haga clic en el nombre de una detección para mostrar el panel lateral Vista previa de la detección en el lateral derecho. El panel lateral Vista previa de la detección contiene la información más importante acerca de la detección seleccionada.

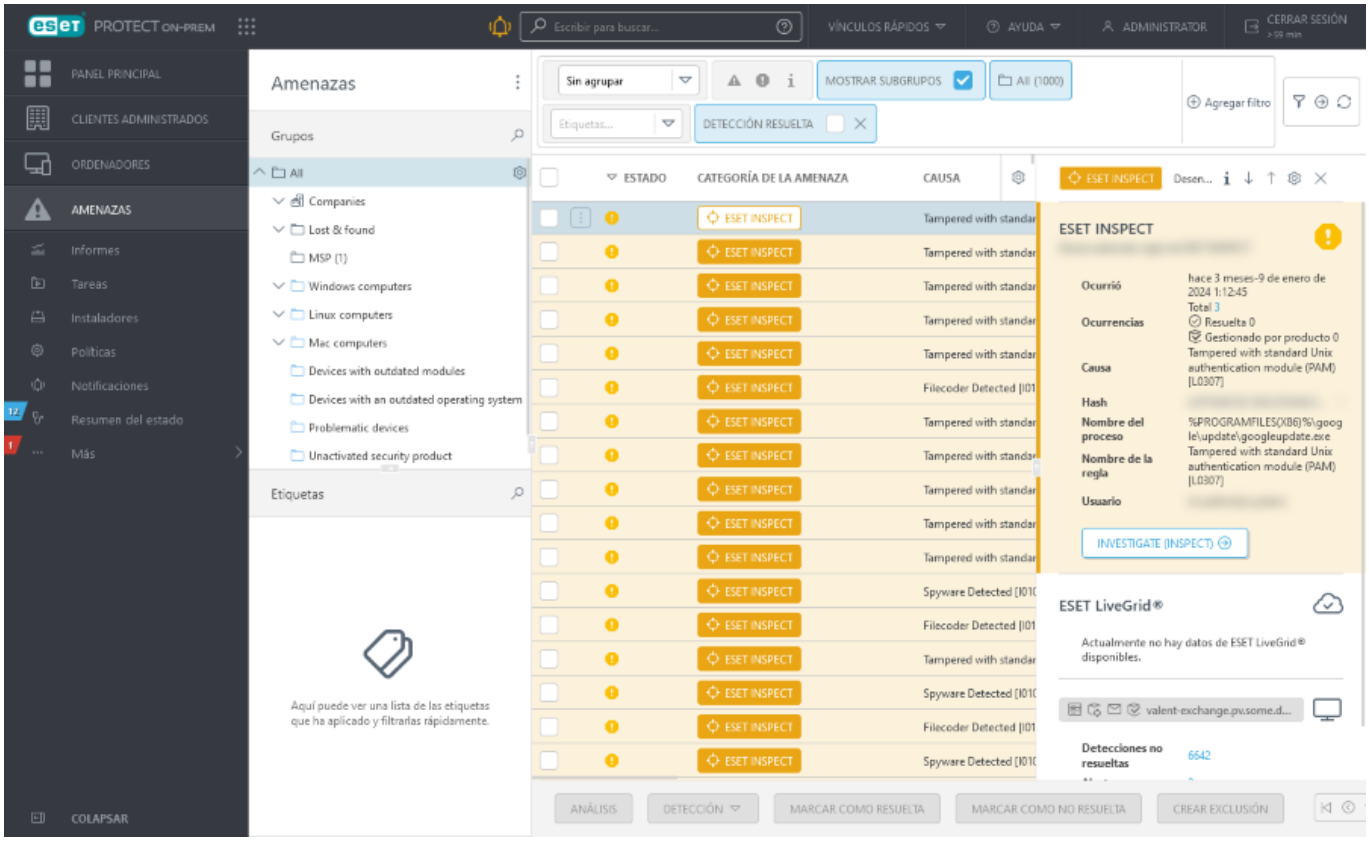
Manipulación de la vista previa del detección:

- **Mostrar detalles**: abra Detalles de la detección.
- **Siguiente**: muestra el siguiente dispositivo en el panel lateral Vista previa de la detección.

- **Anterior**: muestra el dispositivo anterior en el panel lateral Vista previa de la detección.

- **Administrar el contenido de Detalles de la detección**: puede gestionar qué secciones del panel lateral Vista previa de la detección se muestran y en qué orden.

- **Cerrar**: cierra el panel lateral Vista previa de la detección.



Detalles de la amenaza

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 mediante distintas acciones (las acciones disponibles dependen de la categoría de la detección) o dirigirse a Detalles del ordenador para ver información sobre el ordenador en el que se produjo la detección.

- **Ocurrencias**: la sección **Ocurrencias** solo está activa cuando se agrega la detección, y proporciona una lista de ocurrencias individuales de dicha detección. Puede marcar todas las ocurrencias de una misma detección como resueltas/sin resolver.

Crear exclusión

Puede excluir los elementos seleccionados para que no se **detecten** en el futuro. Haga clic en una detección y seleccione **Crear exclusión**. Solo puede excluir las detecciones del **Antivirus** y detecciones de **Cortafuegos** - Reglas de IDS. Puede crear una exclusión y aplicarla a más ordenadores o grupos. La sección **Más** > **Exclusiones** contiene todas las exclusiones creadas, aumenta su visibilidad y simplifica su administración.

⚠ Utilice las exclusiones con precaución, pues pueden provocar que su ordenador se infecte.

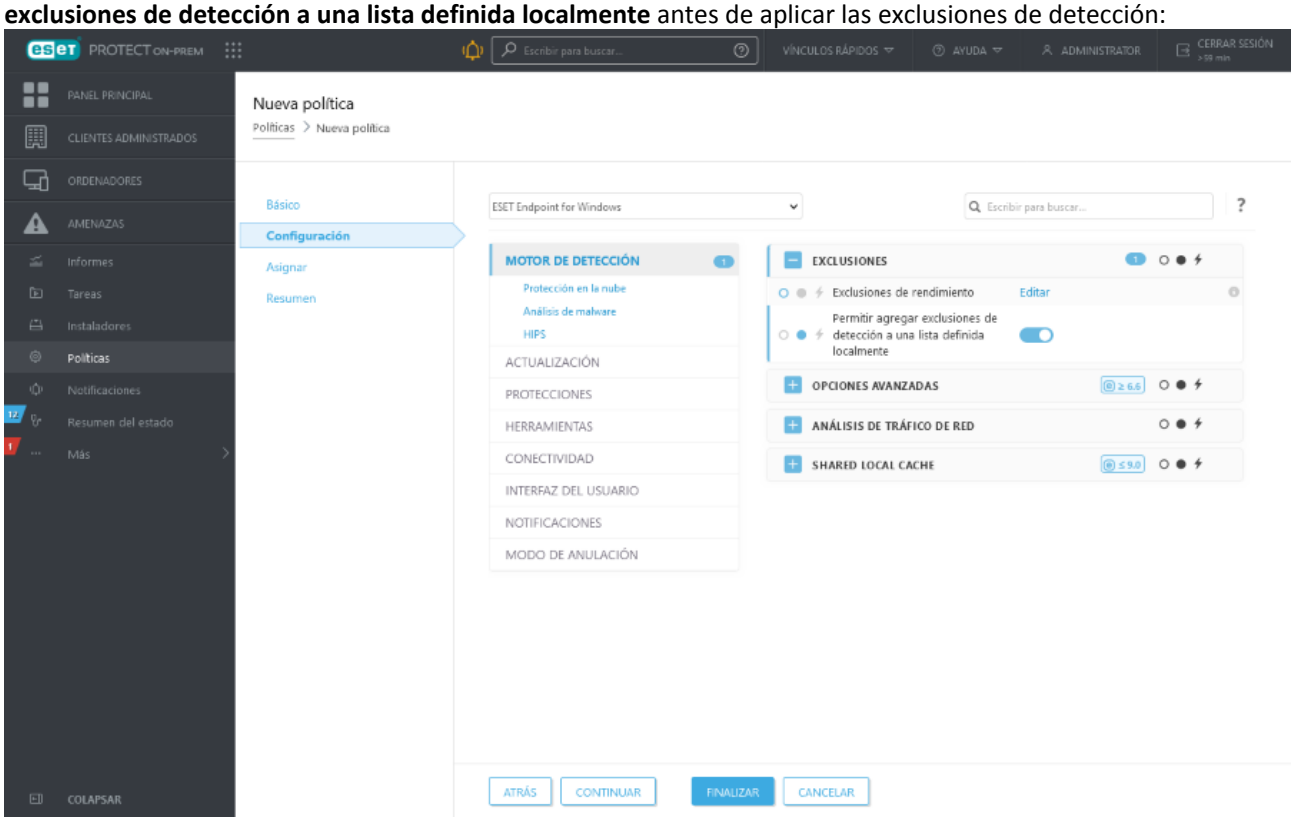
En ESET PROTECT On-Prem hay dos categorías de exclusión de **Antivirus**:

- **Exclusiones de rendimiento**: exclusiones de archivos y carpetas definidas por una ruta de acceso. Puede crearlas mediante una política. Consulte también formato y ejemplos de exclusiones de 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 la detección.

Limitaciones de las exclusiones de detección

- En ESET PROTECT On-Prem no puede crear exclusiones de detección mediante políticas.
- Si sus políticas contenían previamente exclusiones de detección, puede migrar las exclusiones de una política a la lista Exclusiones.
- De forma predeterminada, las exclusiones de detección reemplazan a la lista de exclusiones locales de los ordenadores administrados. Para conservar la lista de exclusiones locales, deberá aplicar **Permitir agregar exclusiones de detección a una lista definida localmente** antes de aplicar las exclusiones de detección:



Configuración

Puede excluir una o más detecciones en función de los siguientes **Criterios de exclusión**.

Detecciones del antivirus

- **Ruta de acceso y Detección**: excluir cada archivo por su nombre de detección y ruta de acceso, incluido el nombre del 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 su nombre de detección.

Detecciones en archivos comprimidos

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

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

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

Detecciones del cortafuegos: reglas de IDS

- **Detección y contexto** (recomendado): excluye la detección del cortafuegos mediante la combinación de los siguientes criterios: por detección, aplicación y dirección IP.
- **Dirección IP**: excluye las detecciones del cortafuegos mediante una dirección IP remota. Utilice esta opción si la comunicación de red con un ordenador determinado provoca falsos positivos.
- **Detección**: excluye la detección e ignore el falso positivo que se desencadena desde varios ordenadores remotos.
- **Aplicación**: excluye la aplicación de las detecciones de red. Permita la comunicación de red para una aplicación que provoque falsos positivos de IDS.

La opción recomendada se selecciona previamente en función del tipo de detección.

Marque la casilla de verificación **Resolver alertas con coincidencia** para resolver automáticamente las alertas que cubra la exclusión.

También puede agregar un **Comentario**.

Destino

> Puede asignar exclusiones (para las detecciones de **Antivirus** y reglas de IDS del **Cortafuegos**) únicamente a los ordenadores que tengan un producto de seguridad de ESET compatible instalado. Las exclusiones no se aplicarán a los productos de seguridad de ESET incompatibles, y se ignorarán en dichos productos.

Una exclusión se aplica de forma predeterminada al grupo de inicio del usuario.

Para cambiar las asignaciones, haga clic en **Agregar destinos** y seleccione los elementos de destino en los que se aplicará la exclusión, o bien seleccione asignaciones existentes y haga clic en **Quitar destinos**.

Vista previa

Le permite ver una descripción general de las exclusiones que se han creado. Asegúrese de que la configuración de las exclusiones sea correcta según sus preferencias.

Después de crear la exclusión, no podrá modificarla. Solo puede cambiar la asignación o eliminar la exclusión.

Haga clic en **Finalizar** para crear la exclusión.

Puede ver y gestionar todas las exclusiones creadas en **Más** > **Exclusiones**. Para verificar si un ordenador o un grupo tiene exclusiones aplicadas, diríjase a Detalles del ordenador > **Configuración** > **Exclusiones aplicadas** o Detalles del grupo > **Exclusiones**.

Productos de seguridad de ESET compatibles con las exclusiones

Las exclusiones no se aplicarán a los productos de seguridad de ESET incompatibles, y se ignorarán en dichos productos.

Exclusiones de detección antivirus

Todos los productos de seguridad de ESET que se pueden administrar son compatibles con las exclusiones de detección de **Antivirus**, excepto los siguientes:

- ESET Endpoint Security para Android
- ESET LiveGuard Advanced
- ESET Inspect On-Prem

Exclusiones de IDS de cortafuegos

Los siguientes productos de seguridad de ESET son compatibles con las exclusiones de IDS de **Cortafuegos**:

- ESET Endpoint Antivirus para Windows versión 8.0 y posteriores
- ESET Endpoint Security para Windows versión 8.0 y posteriores

Protección contra ransomware

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

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

- **Activar protección contra ransomware**: el producto empresarial de ESET bloquea automáticamente todas

las aplicaciones sospechosas que se comporten como ransomware.

• **Habilitar modo de auditoría**: cuando se habilita el modo de auditoría, las detecciones identificadas por Protección contra ransomware se informan en la ESET PROTECT Web Console, pero el producto de seguridad de ESET no las bloquea. El administrador puede decidir bloquear la detección comunicada o excluirla seleccionando **Crear exclusión**. Esta configuración de Política solo está disponible a través de la Consola web de ESET PROTECT.

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

ESET Inspect On-Prem

ESET Inspect On-Prem é un completo sistema Endpoint de detección y respuesta que incluye funciones como las siguientes: detección de incidentes, administración de incidentes y respuesta, recopilación de datos, indicadores de detección de riesgo, detección de anomalías, detección de comportamientos e incumplimientos de políticas. Si desea más información acerca de ESET Inspect On-Prem, su instalación y sus 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	Nuevo nombre	Versión en la que se ha cambiado el nombre
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 necesita que ESET PROTECT On-Prem:

• Cree un usuario de ESET Inspect On-Prem con los permisos necesarios. ESET PROTECT On-Prem contiene los conjuntos de permisos predefinidos para usuarios de ESET Inspect On-Prem. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de ESET Inspect**.

• Cree certificados utilizados durante la instalación de ESET Inspect Server.

• Active ESET Inspect On-Prem en un dispositivo conectado a ESET PROTECT On-Prem. Necesita una licencia de ESET Inspect On-Prem para activar ESET Inspect On-Prem.

Si ha actualizado ESET PROTECT Server, reinicie el servicio ESET Inspect Server para garantizar que todos los futuros cambios de ESET PROTECT On-Prem (por ejemplo, actualizaciones de permisos) se reflejen en ESET Inspect On-Prem.

Implementar ESET Inspect Connector en ordenadores administrados

Haga clic en **Ordenadores** > seleccione uno o más ordenadores y haga clic en **Ordenador** > **Soluciones** > **Activar ESET Inspect On-Prem** para implementar ESET Inspect Connector en los ordenadores Windows/Linux/macOS administrados.

Informes de detecciones de ESET Inspect On-Prem en ESET PROTECT On-Prem

Si agrega un dispositivo que ejecute ESET Inspect Connector (correctamente configurado y conectado a ESET Inspect Server) a ESET PROTECT On-Prem, ESET Inspect On-Prem comunicará las detecciones detectadas en la sección Detecciones de ESET PROTECT On-Prem. Para filtrar estas detecciones, seleccione la categoría de detección de **ESET Inspect**.

Otro tipo de detecciones notificadas por ESET Inspect On-Prem son **Archivos bloqueados**: los intentos bloqueados de iniciar ejecutables bloqueados en ESET Inspect On-Prem (hashes bloqueados).

Administración de detecciones de ESET Inspect en ESET PROTECT On-Prem

Haga clic en la detección y seleccione **Investigar (Inspect)** para ver los detalles de la detección en ESET Inspect On-Prem Web Console.

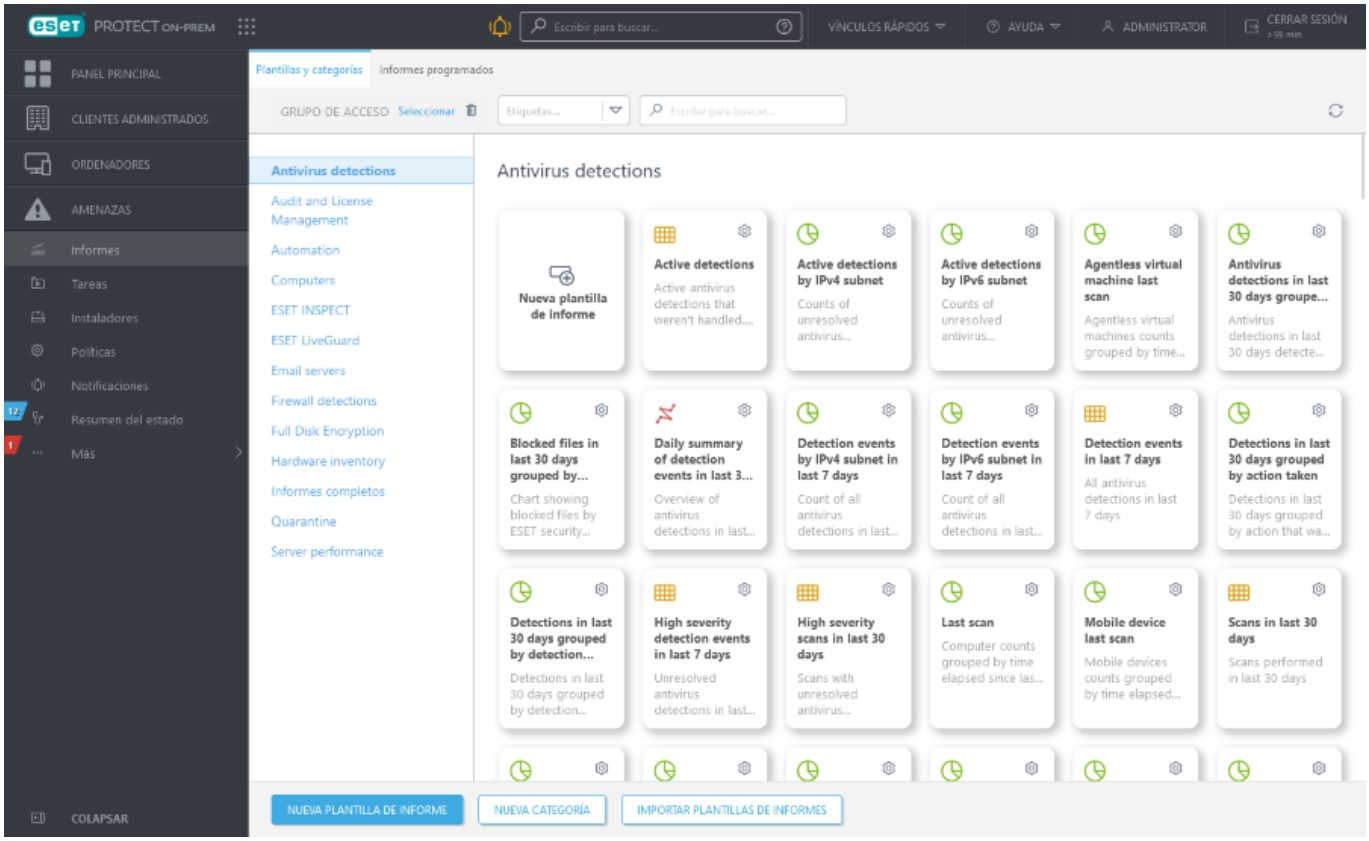
Asegúrese de usar los navegadores web y los productos de ESET compatibles para activar la administración de detecciones de ESET Inspect en ESET PROTECT Web Console.

La integración de las detecciones de ESET Inspect On-Prem en ESET PROTECT Web Console le permite administrar las detecciones de ESET Inspect directamente desde ESET PROTECT Web Console, sin necesidad de abrir ESET Inspect On-Prem Web Console. Por ejemplo, si marca la detección como resuelta en ESET PROTECT Web Console, también se marcará como resuelta en ESET Inspect On-Prem Web Console y viceversa.

Informes

Los informes le permiten acceder y filtrar los datos de la base de datos de una manera sencilla. La ventana de informes está compuesta por dos fichas:

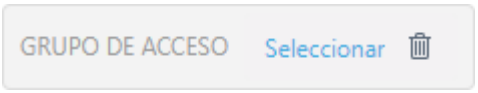
- **Categorías y plantillas**: esta es la ficha predeterminada de la sección **Informes**. Incluye información general sobre las categorías de informes y las plantillas. Aquí puede crear nuevos informes y categorías o realizar otras acciones relacionadas con los informes.
- **Informes programados**: esta ficha contiene una descripción general de los informes programados, y también puede programar un informe nuevo.



Los informes se generan a partir de plantillas clasificadas por tipo de informe. Un informe se puede generar inmediatamente o programarse para generarlo más tarde. Para generar y ver el informe inmediatamente, haga clic en **Generar ahora** junto a la plantilla de informe que desee. Puede utilizar plantillas de informes predefinidas de la lista Plantillas y categorías, o puede crear una plantilla de informe nueva con una configuración personalizada. Haga clic en Nueva plantilla de informe para abrir el asistente de plantilla de informe y especificar los ajustes personalizados del nuevo informe. También puede crear una nueva categoría de informe (**Nueva categoría**) o importar plantillas de informe anteriormente exportadas (**Importar plantillas de informe**).

En la parte superior de la página hay una barra de búsqueda. Puede buscar por categoría y nombre de plantilla, pero no por descripción.

Puede usar etiquetas para filtrar los elementos mostrados.



El botón de filtrado de **Grupo de acceso** permite a los usuarios seleccionar un grupo estático y filtrar los objetos vistos según el grupo en el que se encuentran.

Utilización de las plantillas de informe

Elija una plantilla de informe y haga clic en el icono de engranaje en la ventana dinámica de la plantilla de informe. Están disponibles las opciones siguientes:

Generar ahora	Se genera el informe y se pueden revisar los datos resultantes.

Descargar	Haga clic en **Descargar** para generar y descargar el informe. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa ; (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe PDF para ver los valores de texto.
Programar	Planificar un informe: puede modificar el desencadenador, la regulación y la entrega del informe de la planificación. Puede encontrar todos los informes planificados en la **ficha Informes programados**.
Modificar...	Edite una plantilla de informe existente. Se aplican los mismos ajustes y opciones usados al crear una plantilla nueva de informe.
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Duplicar	Cree un informe nuevo basado en el informe seleccionado (se necesita un nombre nuevo para el duplicado).
Eliminar	Elimina la plantilla de informe seleccionada por completo.
Exportar	La plantilla del informe se exportará a un archivo .dat..

Utilización de las categorías de informe

Seleccione la categoría de informe y haga clic en el icono del engranaje situado en la esquina superior derecha de la categoría. Están disponibles las opciones siguientes:

Nueva categoría	Introduzca un **Nombre** para crear una categoría de plantillas de informes nueva.
Nueva plantilla de informe	Cree una nueva plantilla de informe personalizada.
Eliminar	Elimina la categoría de plantilla de informe seleccionada por completo.
Modificar...	Cambia el nombre de una plantilla de informe existente.
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Exportar	La categoría de plantilla de informe y todas las plantillas incluidas se exportarán a un archivo *.dat*. Más tarde puede importar la categoría con todas las plantillas haciendo clic en **Importar plantillas de informe**. Esta opción resulta útil por ejemplo al migrar las plantillas de informe personalizadas a otra instancia de ESET PROTECT Server.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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 plantillas de informes/ Exportar** está diseñada solo para importar y exportar plantillas de informes, no un informe generado real con datos.

Permisos para informes

Los informes son objetos estáticos que residen en una estructura de objetos en la base de datos de ESET PROTECT. Cada nueva plantilla de informe se almacena en el grupo principal del usuario que la creó. Para acceder a un informe, necesita los permisos con la funcionalidad **Informes y consola**. También necesita permisos para acceder a los objetos que el informe inspecciona. Por ejemplo, si genera el informe **Descripción general de**

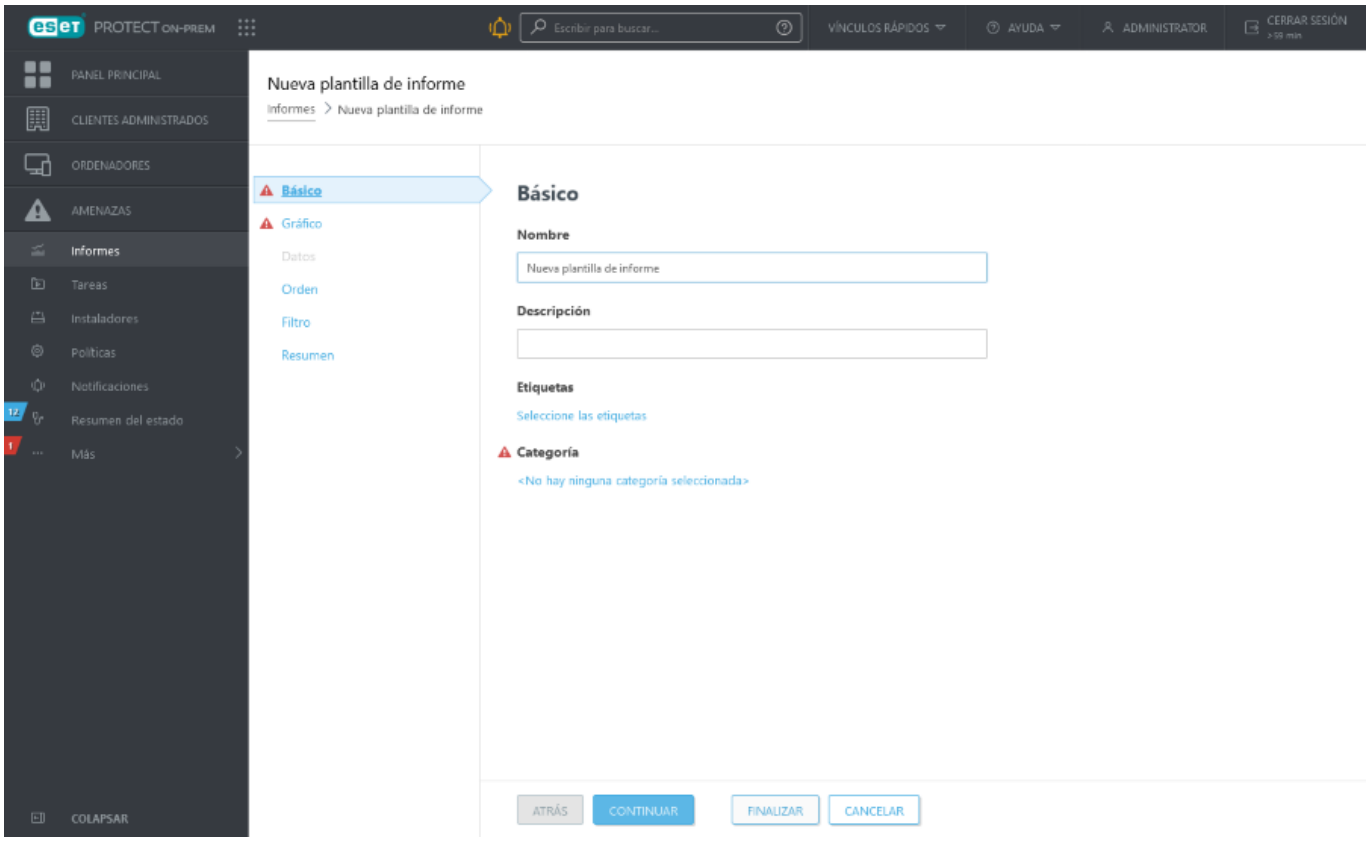
estados del ordenador, solo habrá datos de los ordenadores de los que tenga permiso de **Lectura**.

- **Leer**: el usuario puede enumerar las plantillas de informes y sus categorías, generar informes basados en plantillas de informes o leer el panel
- **Usar**: el usuario puede modificar el panel con las plantillas de informes disponibles
- **Escribir**: cree, modifique o elimine plantillas y sus categorías

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

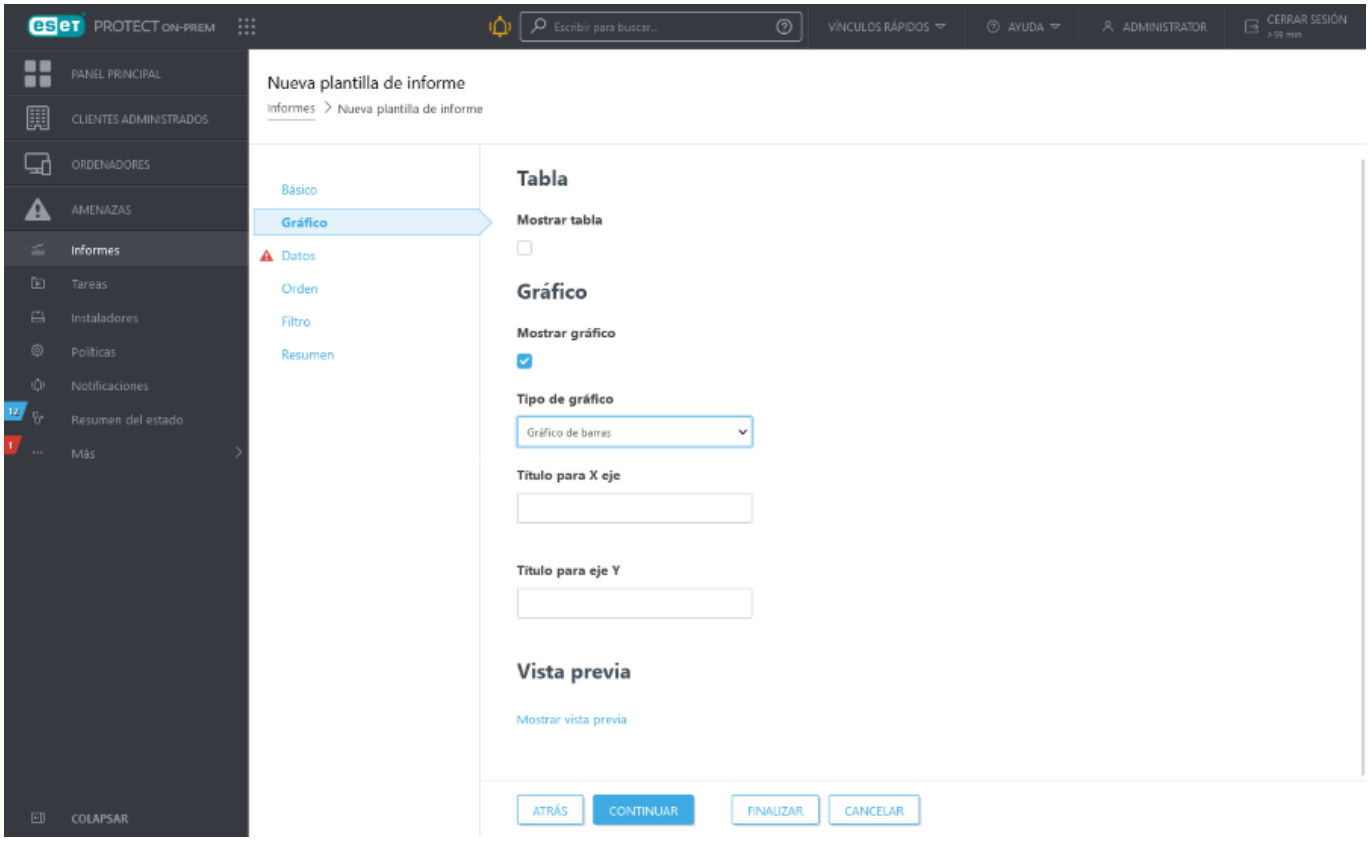
Crear una nueva plantilla de informe

Vaya a Informes y haga clic en **Nueva plantilla de informe**.



Básico

Edite la información básica acerca de la plantilla. Introduzca un **nombre**, una **descripción** y una **categoría**. Solo puede elegir categorías predefinidas. Si quiere crear una nueva categoría, utilice la opción **Nueva categoría** (descrita en el capítulo anterior). Haga clic en **Seleccione las etiquetas** para asignar etiquetas.



Gráfico

En la sección **Gráfico**, seleccione el tipo de **informe**. Ya sea una **tabla**, donde la información está ordenada en filas y columnas, o **gráfico**, que representa los datos en un eje X e Y.

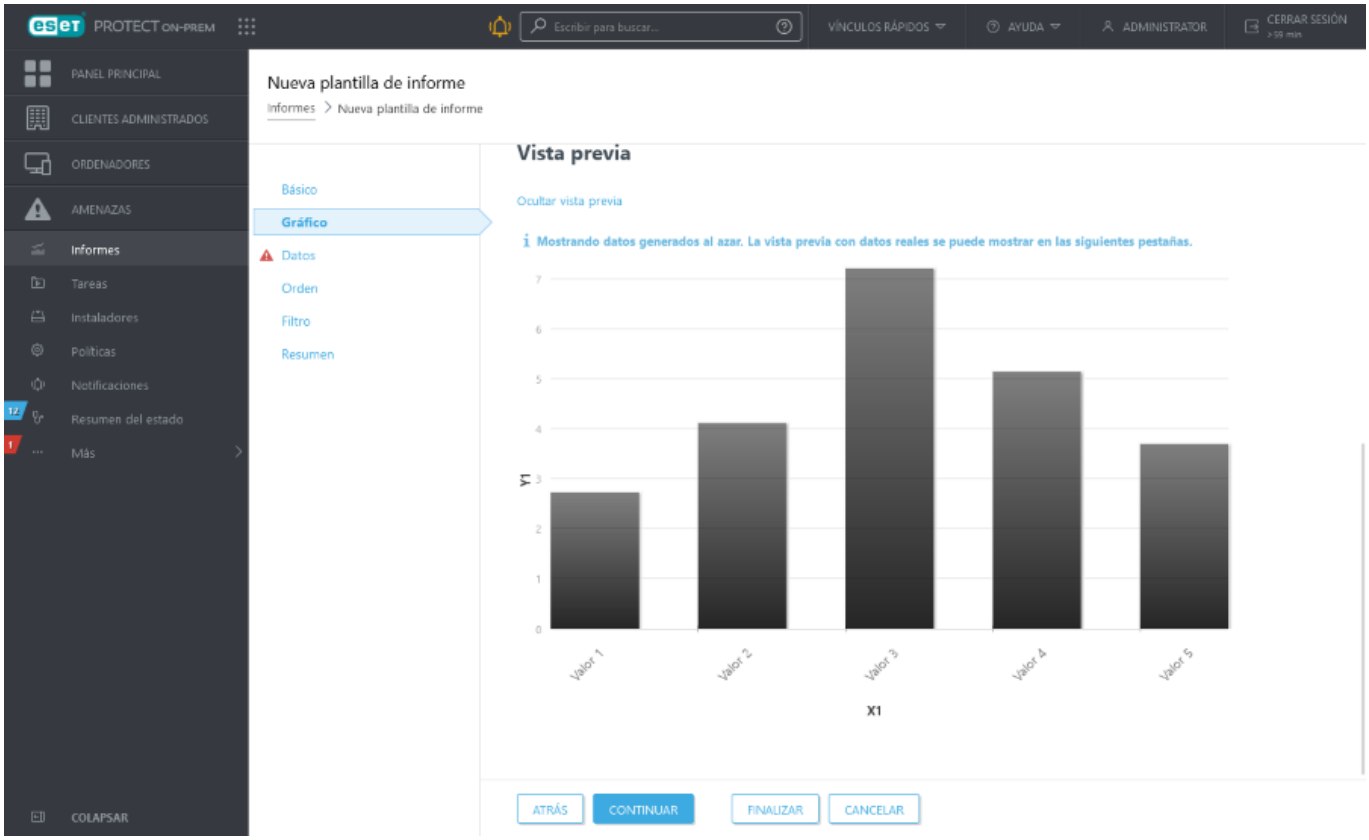
el tipo de gráfico seleccionado se mostrará en la sección **Vista previa**. De esta forma puede ver el aspecto del informe en tiempo real.

Si selecciona **Gráfico** dispone de varias opciones:

- **Gráfico de barras**: un gráfico con barras rectangulares proporcionales a los valores que representan.
- **Gráfico de puntos**: en este gráfico se utilizan puntos para mostrar valores cuantitativos (de forma similar a lo que sucede en un gráfico de barras).
- **Gráfico de tarta**: un gráfico de tarta es un gráfico circular dividido en sectores proporcionales, que representan los valores.
- **Gráfico de anillos seccionado**: similar a un gráfico de tarta, pero este puede contener diferentes 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 simple**: muestra la información como una línea basada en valores sin puntos de datos visibles.
- **Gráfico de líneas apilado**: este tipo de gráfico se utiliza cuando se desea analizar datos con diferentes unidades de medida.

• **Gráfico de barras apilado**: es similar a un gráfico de barras sencillo, pero hay varios tipos de datos con diferentes unidades de medida apilados en las barras.

Opcionalmente puede introducir un título para el eje **X** e **Y** del gráfico para que sea más fácil de leer y reconocer tendencias.



Datos

En la sección **Datos**, seleccione la información que desea mostrar:

a.**Columnas de la tabla**: la información para la tabla se agrega automáticamente en función del tipo de informe seleccionado. Puede personalizar el **nombre**, la **etiqueta** y el **formato** (ver más abajo).

b.**Ejes del gráfico**: seleccione los datos para el eje **X** e **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 que desee y haga clic en **Aceptar**.

Formato

Haga clic en el símbolo ⤢ de la sección **Datos** para ver opciones de formato ampliadas. Puede cambiar el **formato** en el que se muestran los datos. Puede ajustar el formato de las **Columnas de la tabla** y los **Ejes del gráfico**. No todas las opciones están disponibles para cada tipo de datos.

Columna de formato	Elija la columna cuyo formato desea asignar a la columna actual. Por ejemplo, al asignar formato a la columna **Nombre**, elija la columna **Gravedad** para agregar iconos de gravedad junto a los nombres.
Valor mínimo	Defina el límite mínimo para los valores mostrados.

Valor máximo	Defina el límite máximo para los valores mostrados.
Color	Elija el esquema de colores de la columna. El color se ajusta en función del valor de la columna seleccionada en **Columna de formato**.
Iconos	Agregue iconos a la columna a la que se aplica formato en función del valor de la columna de **Columna de formato**.

Haga clic en una de las flechas para cambiar el orden de las columnas.

Orden

Si los datos seleccionados en la sección **Datos** contienen un símbolo que indica la posibilidad de ordenación, la ordenación está disponible. Haga clic en **Agregar orden** para definir la relación entre los datos seleccionados. Seleccione la información de partida (valor de orden) y el método de orden, entre **Ascendente** o **Descendente**. Esto definirá el resultado mostrado en el gráfico. Haga clic en **Subir** o **Bajar** para cambiar el orden de los elementos de ordenación. Haga clic en el icono de la papelera para quitar el elemento de la selección.

Filtro

Defina el método de filtrado. Haga clic en **Agregar filtro** y seleccione el elemento de filtrado en la lista junto con su valor. Esto define qué información se mostrará en el gráfico. Haga clic en el icono de la papelera para quitar el elemento de la selección.

Resumen

En el **Resumen** revise la información y las opciones seleccionadas. Haga clic en **Finalizar** para crear una nueva **plantilla de informe**.

Generar informes

Existen varias formas de generar un informe al instante a partir de una plantilla de informe:

- Desplácese hasta **Vínculos 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 a partir de la cual desea generar un informe. Haga clic en el icono del engranaje y, si desea realizar cambios en la plantilla, haga clic en **Modificar**.

  - Puede hacer clic en la ventana dinámica del informe para generar y ver el informe en ESET PROTECT Web Console. Cuando se genera el informe, puede hacer clic en **Generar y descargar** para guardar el informe en el formato que desee. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa ; (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe PDF para ver los valores de texto.

- Vaya a **Tareas** > **Nuevo** > **Tarea del servidor** para crear una nueva tarea de Generar informe.

  - Se crea la tarea y se muestra 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 inmediatamente.

oConfigure las opciones (como se describe en la tarea Generar informe) y haga clic en **Finalizar**.

Si hace clic en un elemento mostrado en un informe que aparece en la Consola web de ESET PROTECT, aparecerá un menú de profundización con opciones adicionales.

Plantilla de informe MDR

El informe de MDR es un informe de seguridad para proveedores de detección y respuesta administradas.

Un usuario necesita un conjunto de permisos con la funcionalidad **Informes completos** (conjunto de permisos de administrador/revisor/personalizados) para generar la plantilla de informe de MDR:

1. Haga clic en **Informes** y selecciona la pestaña **Categorías y plantillas**.
2. Haga clic en **Informes completos** y, a continuación, en **Plantilla de informe de MDR**.
3. Haga clic en **Generar y descargar**. Solo puede generar la plantilla de informe de MDR como un archivo .odt.

Necesita una licencia de ESET Inspect On-Prem para ver los incidentes de ESET Inspect en la plantilla de informe de MDR.

Planificar un informe

Existen varias formas de programar la generación de un informe:

- Vaya a **Tareas** > **Nuevo** > **Tarea del servidor** para crear una nueva tarea de Generar informe.
- Diríjase a **Informes**, seleccione una plantilla de informe de la que desea generar un informe, haga clic en el icono del engranaje en la ventana dinámica de la plantilla y seleccione **Programar**. Puede utilizar y editar una plantilla de informe predefinida o crear una nueva plantilla de informe.
- Haga clic en **Programar** en el menú contextual de una plantilla de informe de una consola.
- Diríjase a **Informes** > ficha **Informes programados** > haga clic en **Programar informe**.

Al programar un informe tiene varias opciones, como se describe en la tarea Generar informe:
- Puede elegir varias plantillas de informe para un informe.
- Los usuarios de MSP pueden filtrar el informe mediante la selección del cliente.
- Defina la entrega del informe en un correo electrónico o guárdelo en un archivo.
- Si lo desea, defina los parámetros de desencadenadores y límites.

Una vez programado el informe, haga clic en **Finalizar**. Se crea la tarea y se ejecutará en el intervalo definido en el desencadenador (una vez o repetidamente) y en función de la configuración de regulación (opcional).

Ficha Informes programados.

Puede ver los informes que ha programado en **Informes > Informes programados**. A continuación se muestran otras acciones disponibles en esta ficha:

Programar	Crea una programación nueva para un informe existente.
Mostrar detalles	Muestra información detallada sobre la programación seleccionada.
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Ejecutar ahora	Ejecuta el informe planificado.
Modificar...	Permite modificar la programación del informe. Puede agregar o cancelar la selección de plantillas de informe, modificar la configuración de programación o editar los ajustes de limitación y distribución del informe.
Duplicar	Crea una programación duplicada en el grupo principal.
Eliminar	Elimina la programación. La plantilla de informe se conservará.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Aplicaciones obsoletas

Utilice el informe **Aplicaciones obsoletas** (disponible en la categoría **Informes** > **Ordenadores** para ver qué componentes de ESET PROTECT no están actualizados.

Hay dos formas de ejecutar este informe:

- Agregue una Nueva consola o modifique uno de los paneles de consola existente.
- Diríjase a **Informes** > categoría **Ordenadores** > ventana dinámica **Aplicaciones obsoletas** > haga clic en **Generar ahora**.

Si ha encontrado alguna aplicación obsoleta, puede realizar las siguientes operaciones:

- Utilizar la tarea del cliente ESET PROTECT Actualización de componentes para actualizar ESET Management Agent, Server y MDM.
- Utilizar la tarea del cliente Instalación de software para actualizar su producto de seguridad.

Visor de registros de SysInspector

Con el visor de registros de SysInspector puede consultar los registros de SysInspector después de ejecutarlo en un ordenador cliente. También puede abrir los registros de SysInspector directamente desde una tarea de

Solicitud de registro de SysInspector después de ejecutarla correctamente. Los archivos de registro se pueden descargar y visualizar en SysInspector en su ordenador local.

ESET SysInspector solo se ejecuta en ordenadores Windows.

Cómo ver el registro de SysInspector

Desde una consola

1.Agregue una Nueva consola o modifique un informe de consola existente.

2.Seleccione la plantilla de informe **Automatización** > **Historial de instantáneas de SysInspector en los últimos 30 días**.

3.Abra el informe, seleccione un ordenador y, a continuación, seleccione **Abrir vista del registro de SysInspector** en el menú desplegable.

Desde un informe

1.Diríjase a Informes > Categoría **Automatización**.

2.Seleccione la plantilla **Historial de instantáneas de SysInspector en los últimos 30 días** en la lista y haga clic en **Generar ahora**.

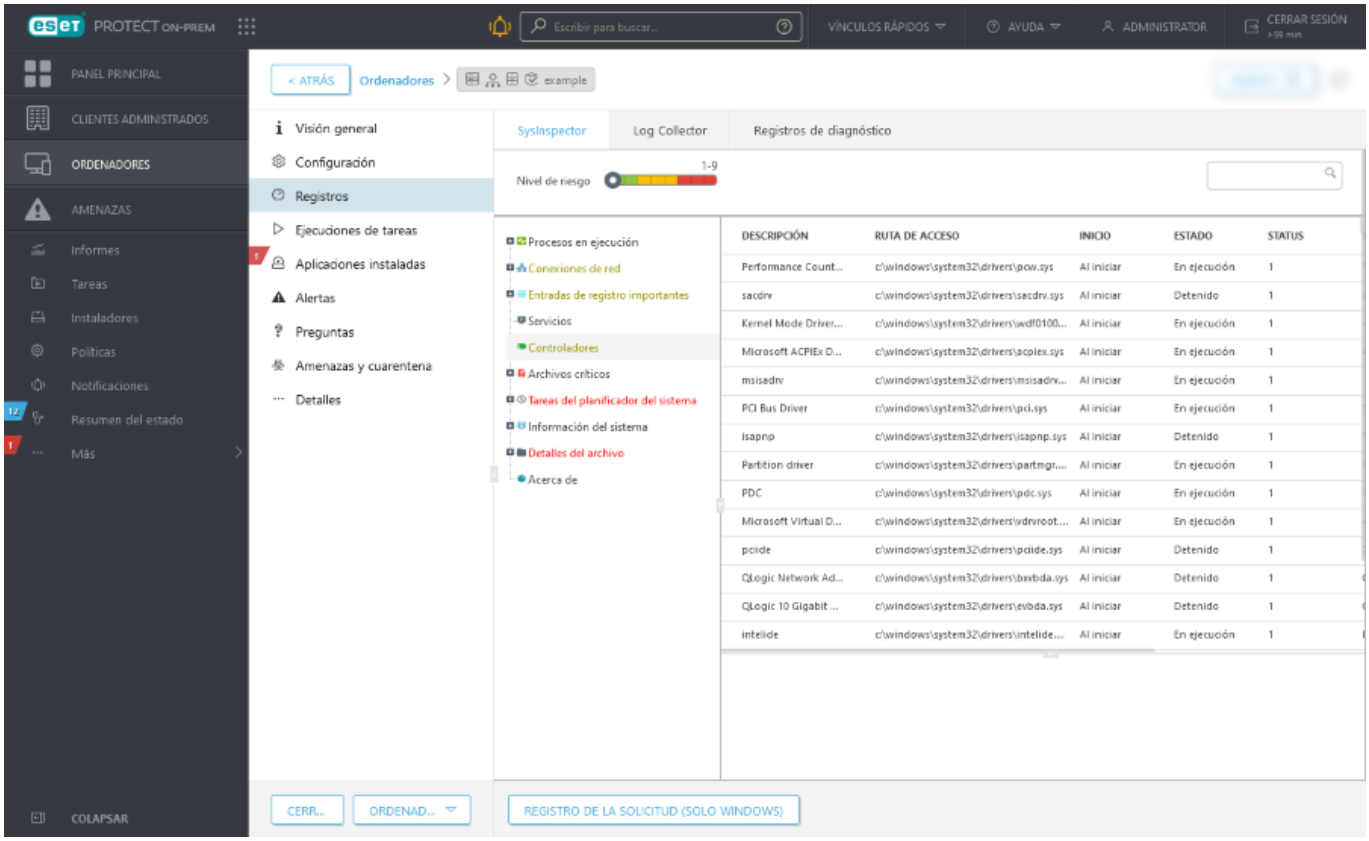
3.Abra el informe, seleccione un ordenador y, a continuación, seleccione **Abrir vista del registro de SysInspector** en el menú desplegable.

Desde el menú Ordenadores

1.Desplácese hasta Ordenadores.

2.Seleccione un ordenador en un grupo estático o dinámico, y haga clic en **Mostrar detalles**.

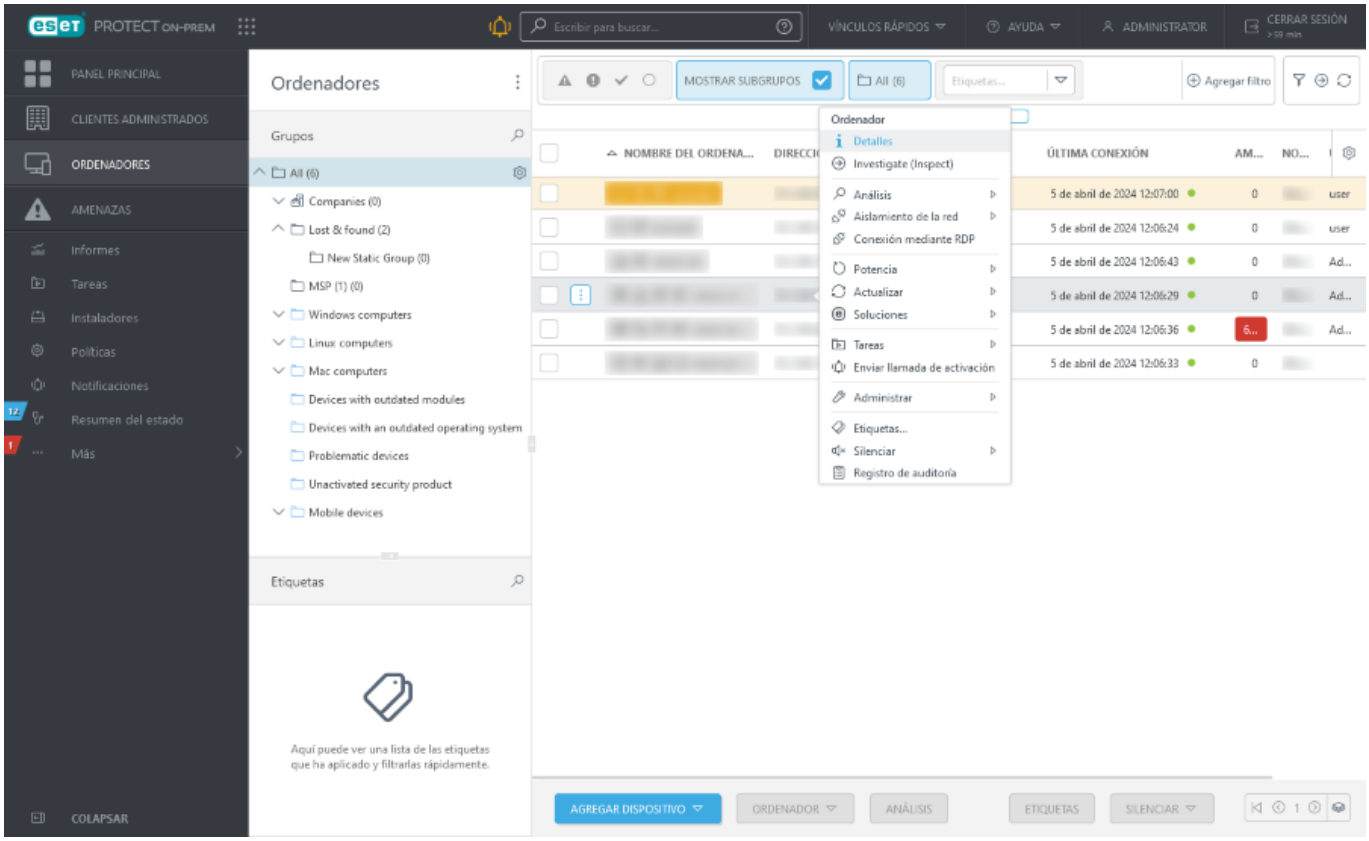
3.Diríjase hasta la sección **Registros** > ficha **SysInspector**, haga clic en una entrada de la lista y seleccione **Abrir visor de registros de SysInspector**.



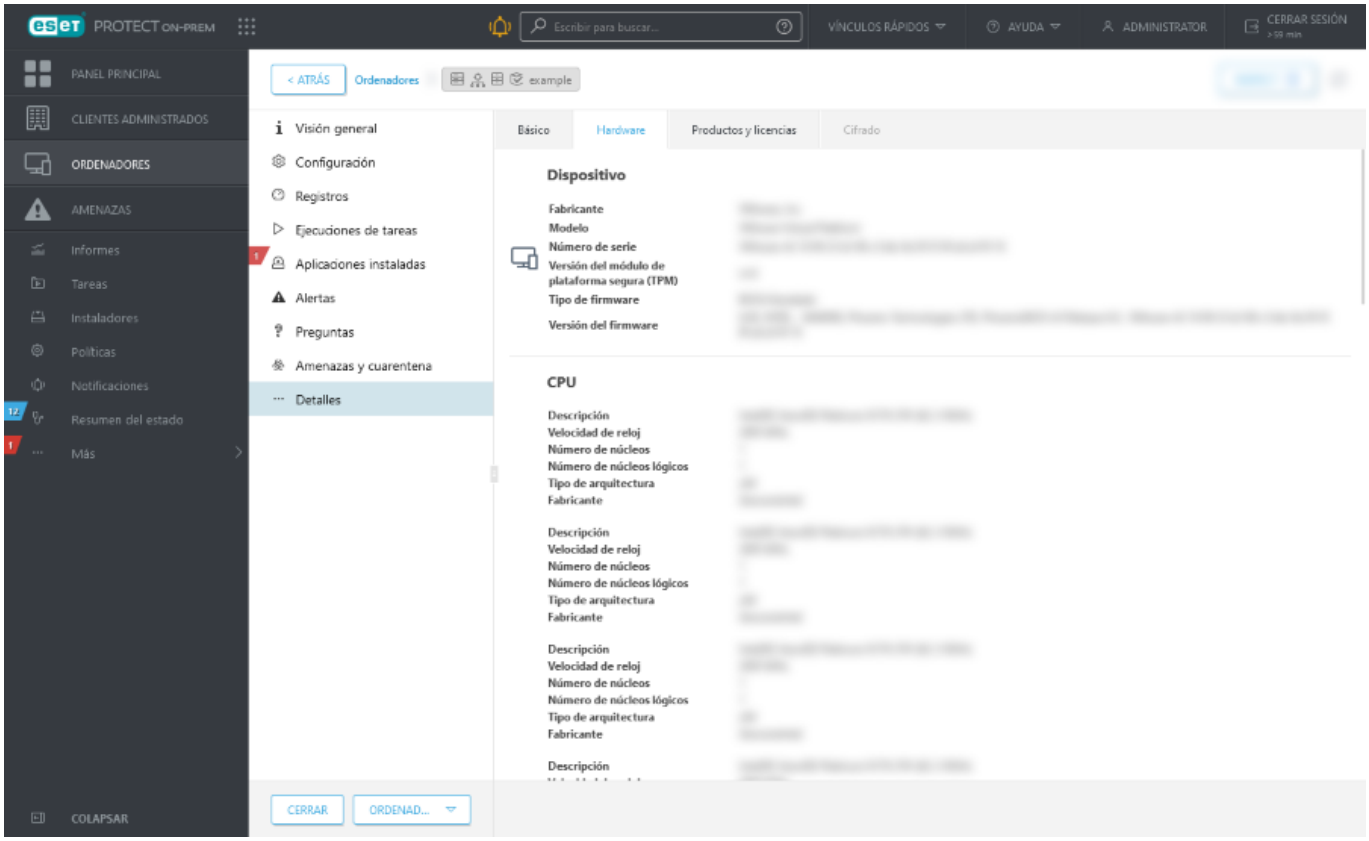
Inventario de hardware

ESET PROTECT On-Prem ofrece la posibilidad de recuperar detalles del inventario de hardware de dispositivos conectados, como, por ejemplo, detalles de la RAM, el almacenamiento y el procesador de un dispositivo.

Haga clic en **Ordenadores** > haga clic en un dispositivo conectado y seleccione **Detalles**.



Haga clic en **Detalles** y seleccione la ficha **Hardware**.



Informes del inventario de hardware

Puede encontrar informes del inventario de hardware predefinidos en **Informes** > **Inventario de hardware**. Puede crear informes del inventario de hardware personalizados. Al crear una Nueva plantilla de informe, seleccione en

Datos una subcategoría de uno de los filtros de **Inventario de hardware**. Cuando añada la primera columna de la tabla o el eje X, solo podrán seleccionarse los datos compatibles.

Grupos dinámicos basados en inventario de hardware

Puede crear grupos dinámicos personalizados basados en los detalles de inventario de hardware de los dispositivos conectados. Cuando cree una Nueva plantilla de grupo dinámico, seleccione reglas en las categorías de **Inventario de hardware** para filtrar los dispositivos conectados en función de sus parámetros de hardware.

Puede seleccionar entre las siguientes categorías de inventario de hardware: Chasis, Información del dispositivo, Pantalla, Adaptador de pantalla, Dispositivo de entrada, Almacenamiento masivo, Adaptador de red, Impresora, Procesador, RAM y Dispositivo de sonido. Por ejemplo, puede crear un grupo dinámico con dispositivos filtrados por su capacidad de RAM para obtener información general de los dispositivos que cuentan con una cantidad de RAM determinada.

Sistemas operativos compatibles con el inventario de hardware

La función de inventario de hardware está disponible en todos los ordenadores Windows, Linux* y macOS compatibles.

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

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

Informe de registros de auditoría

El informe de **registro de auditoría** contiene todas las acciones y todos los cambios realizados por los usuarios en ESET PROTECT Server.

Para ejecutar este informe, haga clic en **Informes** > categoría **Administración de licencias y auditorías** > **Registro de auditoría**.

Puede ver y filtrar un registro de auditoría directamente en Web Console en **Más** > **Registro de auditoría**.

Para ver el registro de auditoría, el usuario de Web Console debe tener un conjunto de permisos con la funcionalidad **Registro de auditoría**.

Tareas

Las **Tareas** se pueden utilizar para administrar ESET PROTECT Server, los ordenadores cliente y sus productos de ESET. Las tareas pueden automatizar trabajos rutinarios. Hay una serie de tareas predefinidas que engloban los casos más comunes, y también puede crear tareas personalizadas con ajustes concretos. Utilice las tareas para solicitar una acción a los ordenadores cliente. Para ejecutar una tarea correctamente, es necesario tener suficientes derechos de acceso para la tarea y para los objetos (dispositivos) que utiliza la tarea. Consulte la lista

de permisos para obtener más información sobre los derechos de acceso.

Hay dos categorías de tareas principales: Tareas del cliente y Tareas del servidor.

- Puede asignar tareas del cliente a grupos o a ordenadores individuales. Una vez creada, la tarea se ejecuta por medio de un desencadenador. Una tarea del cliente puede tener más desencadenadores configurados. Las tareas del cliente se distribuyen a los clientes cuando el ESET Management Agent de un cliente se conecta al ESET PROTECT Server. Por esta razón, los resultados de la ejecución de la tarea pueden tardar tiempo en trasladarse al ESET PROTECT Server. Puede gestionar el intervalo de conexión de ESET Management Agent para reducir los tiempos de ejecución de la tarea.

- Las tareas del servidor las ejecuta ESET PROTECT Server de forma independiente o en otros dispositivos. las tareas del servidor no se pueden asignar a cualquier cliente o grupo de clientes. Cada tarea del servidor puede tener un desencadenador configurado. Si la tarea debe ejecutarse con distintos eventos, tiene que haber una tarea del servidor por cada desencadenador.

Puede crear una nueva tarea de dos formas:

- Haga clic en **Nuevo** > **Tarea del cliente** o **Tarea del servidor**.

- Seleccione el tipo de tarea que desee a la izquierda y haga clic en **Nuevo** > Tarea del cliente o Tarea del servidor.

Le ofrecemos las siguientes tareas predefinidas para facilitar su labor (cada Categoría de la tarea contiene Tipos de tareas):

Todas las tareas

Tareas del cliente

Producto de seguridad ESET

Buscar actualizaciones del producto
Diagnóstico
Finalizar aislamiento del ordenador de la red
Exportar configuración de productos administrados
Aislar ordenador de la red
Actualización de módulos
Reversión de la actualización de módulos
Exploración a petición
Activación del producto
Administración de cuarentena
Ejecutar script de SysInspector
Enviar archivo a ESET LiveGuard
Análisis del servidor
Instalación de software
Solicitud de registro de SysInspector (solo Windows)
Cargar archivo en cuarentena

ESET PROTECT

Diagnóstico
Reiniciar agente clonado
Restablecimiento de la base de datos de Rogue Detection Sensor
Actualización de componentes de ESET PROTECT
Detener administración (desinstalar ESET Management Agent)

Sistema operativo

Mostrar mensaje
Cerrar sesión
Actualización del sistema operativo
Ejecutar comando
Apagar el ordenador
Instalación de software
Desinstalación del software
Detener administración (desinstalar ESET Management Agent)

Móvil

Acciones Anti-Theft
Mostrar mensaje
Exportar configuración de productos administrados
Actualización de módulos
Exploración a petición
Activación del producto
Instalación de software
Detener administración (desinstalar ESET Management Agent)

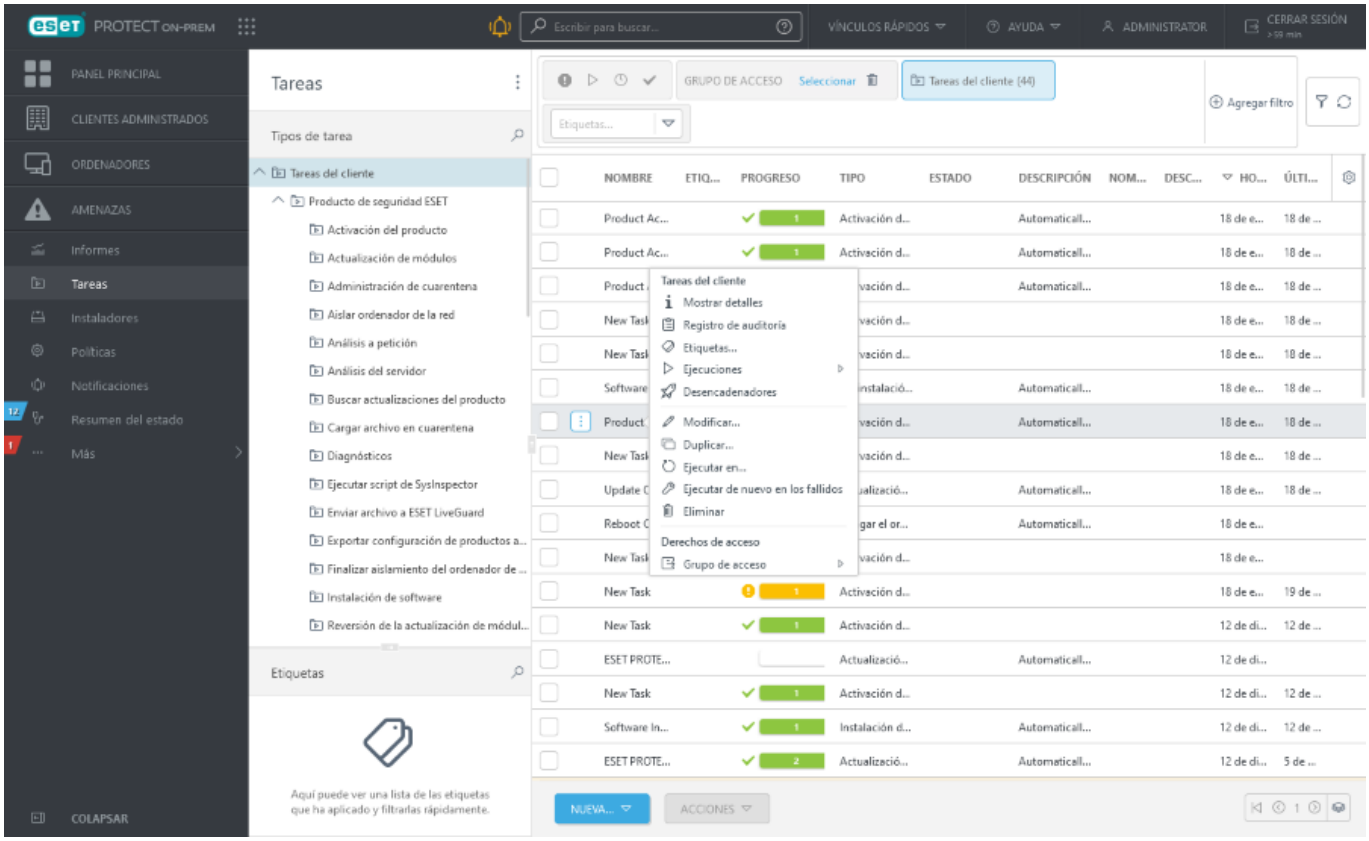
Tareas del servidor

Implementación del agente: distribuye el agente a los ordenadores cliente.
Eliminar ordenadores que no se conecten: elimina clientes que ya no se conectan a ESET PROTECT On-Prem desde Web Console.
Generar informe: se utiliza para generar informes cuando sean necesarios.
Cambiar nombre de los ordenadores: esta tarea cambiará regularmente el nombre de los ordenadores mediante el uso del formato FQDN.
Sincronización de grupos estáticos: actualiza la información del grupo para mostrar los datos actuales.
Sincronización de usuarios: actualiza el usuario o el grupo de usuarios.

Información general de las tareas

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Debe crear un Desencadenador para ejecutar una tarea del cliente.



Haga clic en una tarea para realizar más acciones:

Mostrar detalles	Permite ver detalles de la tarea: resumen, ejecuciones, desencadenadores (los detalles de estos últimos solo están disponibles para tareas del cliente).
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Ejecuciones	Solo tareas del cliente: Puede seleccionar resultados de ejecución de tareas y realizar más acciones en caso de que sea necesario; consulte Detalles de la tarea para obtener más información.
Desencadenadores	Solo tareas del cliente: Consulte la lista de Desencadenadores de la tarea del cliente seleccionada.
Modificar...	Permite realizar modificaciones en la tarea seleccionada. La edición de las tareas existentes resulta útil cuando solo necesita realizar pequeños ajustes, En el caso de tareas más específicas se recomienda crear una nueva tarea.
Duplicar	Permite crear una nueva tarea basada en la tarea seleccionada; se necesita un nombre nuevo para el duplicado.
Ejecutar ahora	Solo tareas del servidor: ejecuta la tarea del servidor seleccionada.
Ejecutar en	Solo tareas del cliente: Permite añadir un desencadenador nuevo y seleccionar ordenadores o grupos de destino para la tarea del cliente.

Error al ejecutar de nuevo	Solo tareas del cliente: Crea un nuevo desencadenador con todos los ordenadores que fallaron durante la ejecución de la tarea anterior establecidos como destinos. Si lo prefiere, puede modificar la configuración de la tarea o hacer clic en Finalizar para ejecutar de nuevo la tarea sin realizar modificaciones.
Eliminar	Quita por completo las tareas seleccionadas. • Si la tarea se elimina después de crearse, pero antes de su inicio programado, se eliminará y no se ejecutará y nunca se iniciará. • Si la tarea se elimina después de su inicio programado, se completará, pero la información no se mostrará 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 suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Indicador de progreso

El indicador de progreso es una barra de color en la que se muestra el estado de ejecución de una tarea. Cada tarea tiene su propio indicador (mostrado en la fila **Progreso**). El estado de ejecución de una tarea se muestra en colores distintos, e incluye el número de ordenadores asignados a una tarea concreta que se encuentran en ese estado:

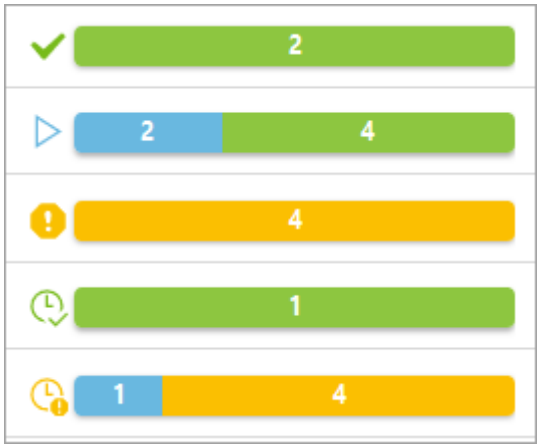
En ejecución (azul)

Finalizada correctamente (verde)

Con error (naranja)

Tarea recientemente creada (blanco): el indicador puede tardar tiempo en cambiar de color, ESET PROTECT Server necesita recibir una respuesta de ESET Management Agent para mostrar el estado de ejecución. El indicador de progreso se mostrará de color blanco si no hay ningún desencadenador asignado.

Una combinación de los elementos anteriores:



Consulte el icono de estado si desea obtener información detallada sobre los diferentes tipos y estados de iconos.

En el indicador de progreso se muestra el estado de una tarea cuando se ejecutó por última vez. Esta información procede de ESET Management Agent. En el indicador de progreso se muestra exactamente lo que el ESET Management Agent indica desde los ordenadores cliente.

Icono de estado

El icono que aparece junto al indicador de progreso proporciona información adicional. Indica si hay ejecuciones planificadas de una tarea determinada, así como el resultado de las ejecuciones que se han completado. Esta información la expone el ESET PROTECT Server. Pueden aparecer los siguientes estados:

En ejecución	La tarea se está ejecutando al menos en un destino, y no hay ejecuciones planificadas ni con error. Se aplica incluso si la tarea ya ha concluido en algunos destinos.
Éxito	La tarea se ha completado correctamente en todos los destinos, y no hay ejecuciones planificadas ni en marcha.
Error	La tarea se ha ejecutado en todos los destinos, pero ha fallado al menos en uno de ellos. No hay planificada ninguna ejecución posterior (programada).
Planificado	La ejecución de la tarea está planificada, pero no hay ejecuciones en marcha.
Planificado/en ejecución	La tarea tiene ejecuciones planificadas (del pasado o en el futuro). No hay ejecuciones que hayan fallado, y se está ejecutando al menos una ejecución.
Planificado/con éxito	La tarea aún tiene ejecuciones planificadas (del pasado o en el futuro), no hay ejecuciones erróneas o en ejecución y al menos una ejecución se ha completado correctamente.
Planificado/error	La tarea aún tiene ejecuciones planificadas (del pasado o en el futuro), no hay ejecuciones en ejecución y al menos una ejecución ha fallado. Esto se aplica incluso si algunas ejecuciones han finalizado correctamente.

Detalles de la tarea

Haga clic en una tarea y seleccione **Mostrar detalles** para ver los detalles de la tarea en las siguientes pestañas:

Resumen

Esta pestaña contiene información general de la configuración de la tarea.

Ejecuciones

La ficha **Ejecuciones** muestra una lista de ordenadores con resultados de ejecución de las tareas del cliente. La ficha **Ejecuciones** no está disponible para las tareas del servidor.

Si hay demasiadas ejecuciones, puede filtrar la vista para limitar los resultados.

Haga clic en **Agregar filtro** para filtrar las ejecuciones seleccionadas según su estado:

- **Planificada**: **Sí** (la tarea del cliente está planificada para su ejecución), **No** (se ha completado la ejecución de la tarea del cliente).
- **Último estado** – **Sin estado**, **En ejecución**, **Finalizado**, **Error**.

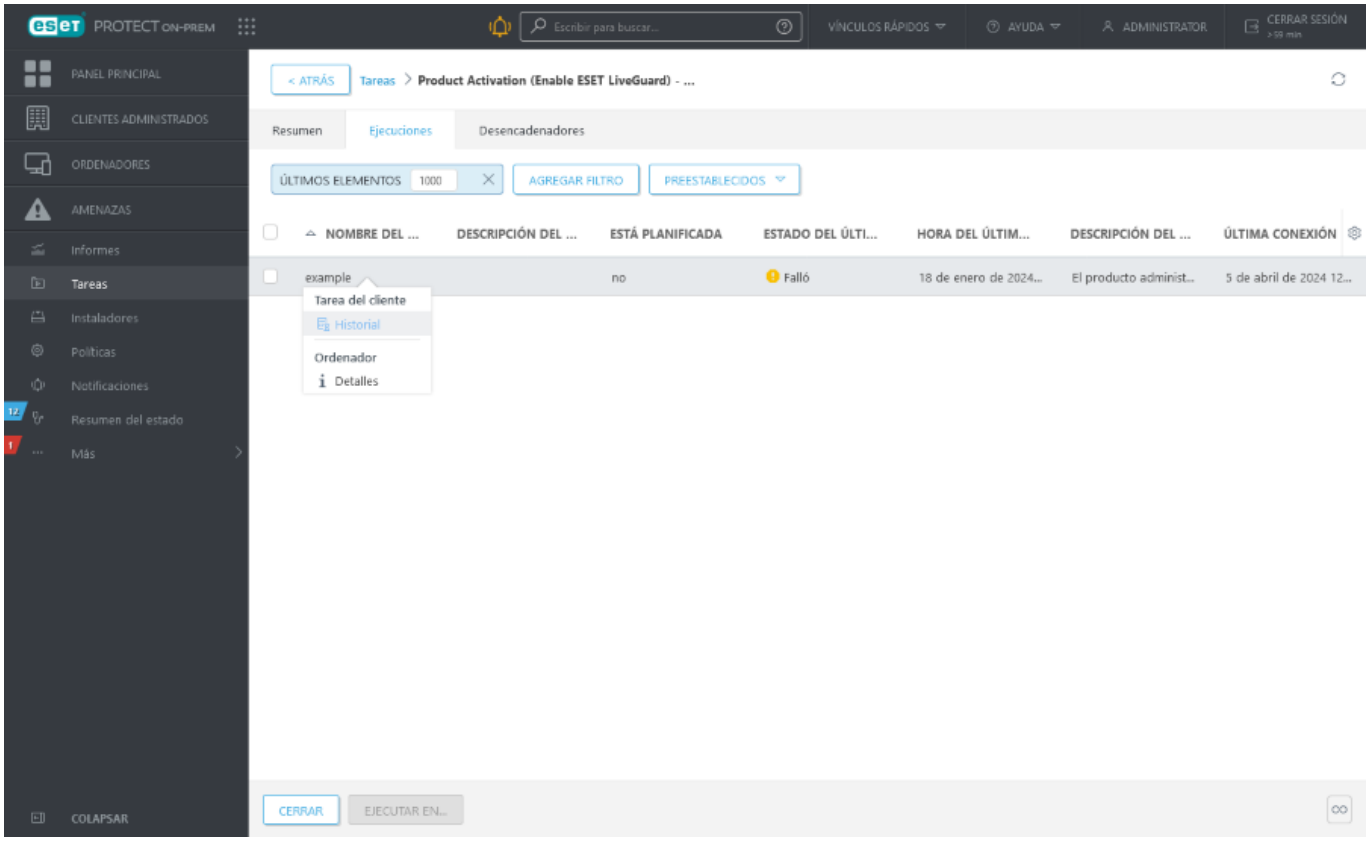
Puede modificar el filtro o desactivarlo para ver todos los ordenadores, sea cual sea su estado.

Haga clic en una línea de **Nombre del ordenador** o **Descripción del ordenador** para realizar más acciones:

- **Historial**: vea los detalles de ejecución de las tareas del cliente, incluidos los valores de **Ocurrió**, **Producto Estado del progreso**, **Descripción del progreso** y **Mensaje de seguimiento** de la ejecución (si están disponibles). 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 del **historial**, ajuste el filtro **Ocurrió** a una duración más amplia.
> - Al instalar productos de ESET anteriores, el mensaje de seguimiento mostrará lo siguiente: **Tarea entregada al producto administrado**.

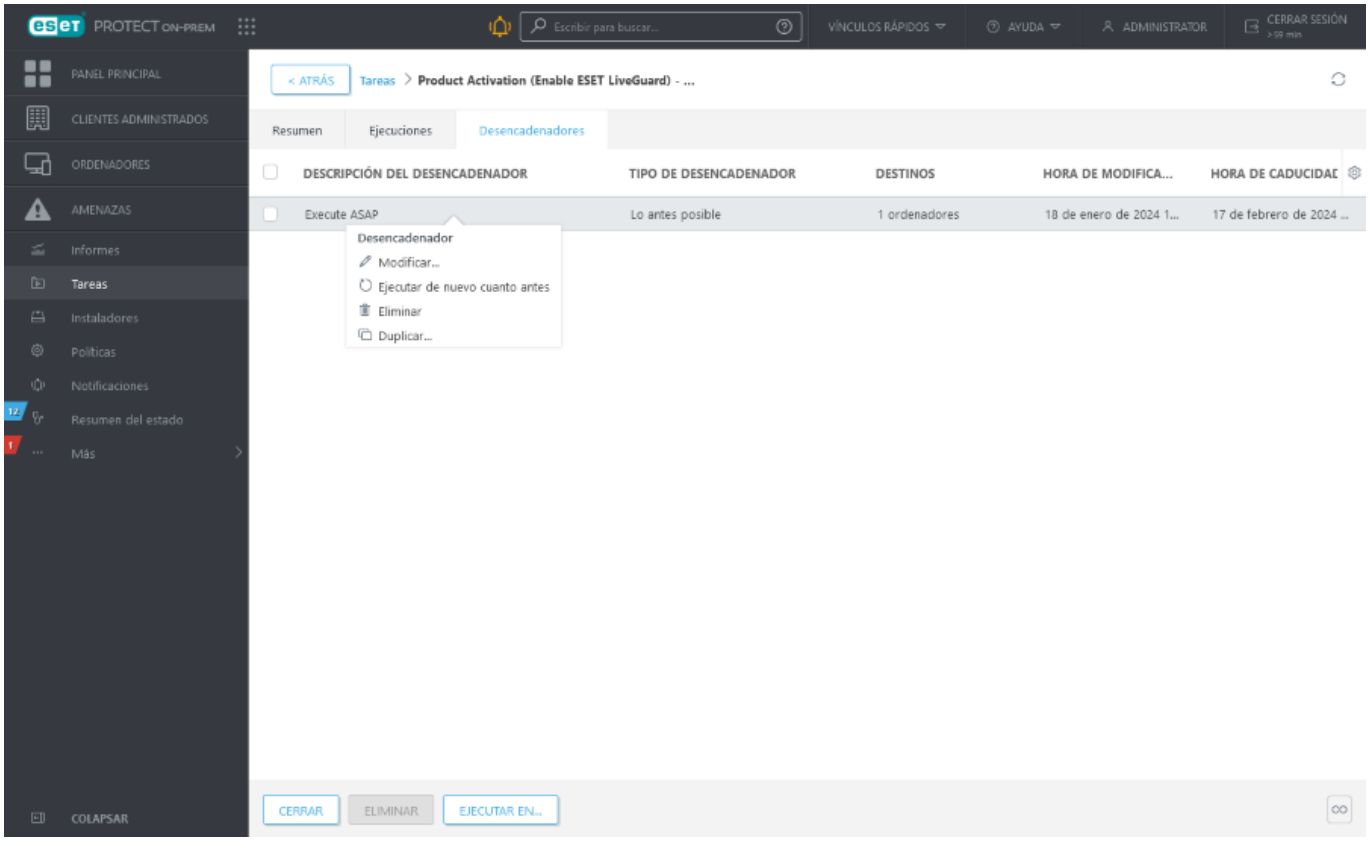
- **Detalles**: consulte los detalles del ordenador seleccionado.



Desencadenadores

La pestaña **Desencadenadores** solo está disponible para tareas del cliente, y muestra la lista de desencadenadores para la tarea del cliente seleccionada. Para administrar el desencadenador, haga clic en él y seleccione uno de los siguientes elementos:

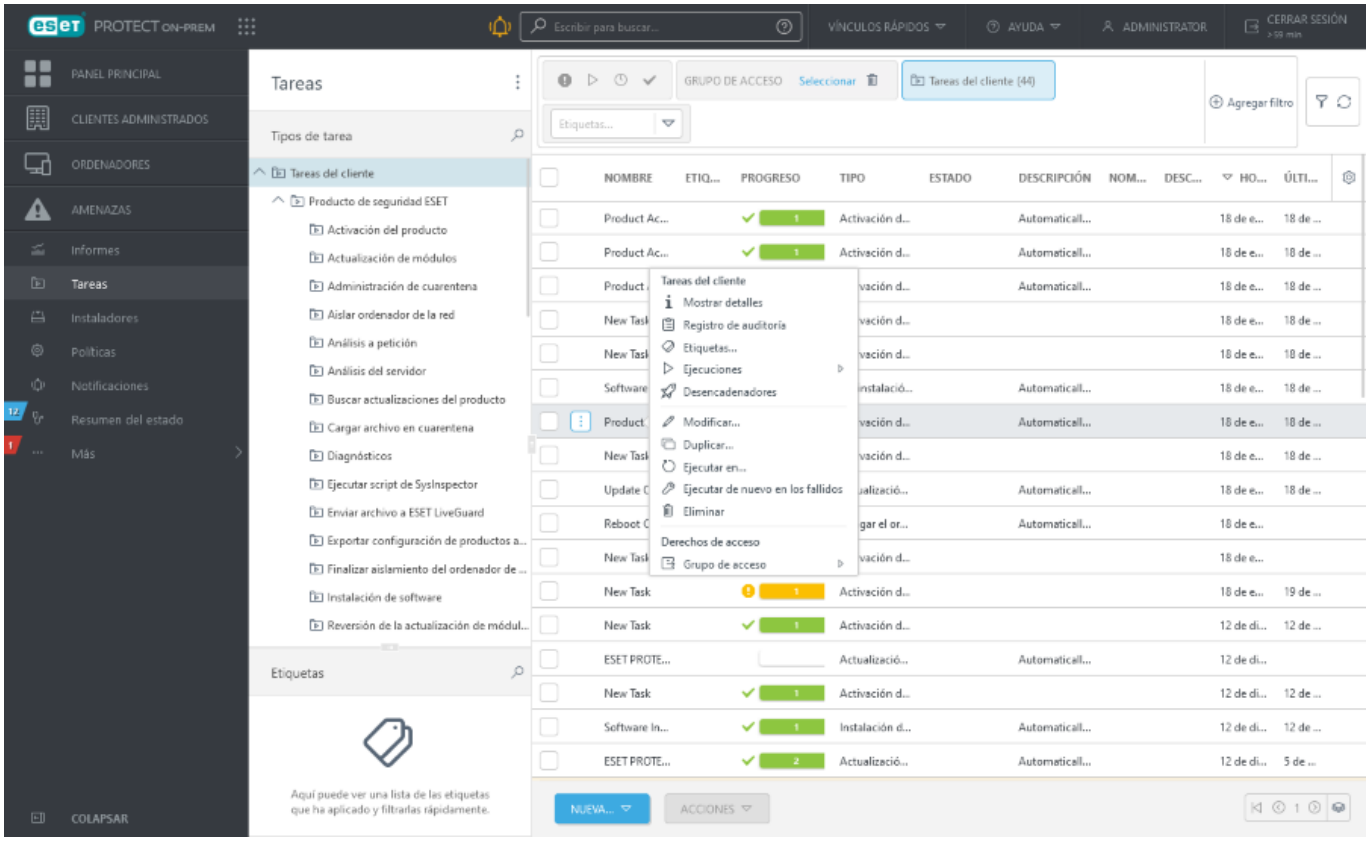
Modificar...	Permite realizar modificaciones en el desencadenador seleccionado.
Ejecutar de nuevo cuanto antes	Ejecute la tarea del cliente de nuevo (lo antes posible) con un desencadenador existente sin modificación.
Eliminar	Elimina el desencadenador seleccionado por completo. Para eliminar varios desencadenadores, marque las casillas de verificación de la izquierda y haga clic en el botón **Eliminar**.
Duplicar	Permite crear un nuevo desencadenador basado en el seleccionado; se necesita un nombre nuevo para el duplicado.



Tareas del cliente

Puede asignar tareas del cliente a grupos o a ordenadores individuales. Una vez creada, la tarea se ejecuta por medio de un desencadenador. Una tarea del cliente puede tener más desencadenadores configurados. Las tareas del cliente se distribuyen a los clientes cuando el ESET Management Agent de un cliente se conecta al ESET PROTECT Server. Por esta razón, los resultados de la ejecución de la tarea pueden tardar tiempo en trasladarse al ESET PROTECT Server. Puede gestionar el intervalo de conexión de ESET Management Agent para reducir los tiempos de ejecución de la tarea.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.



Crea una nueva tarea del cliente

1. Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

   - Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
   - Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
   - Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

2. En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

3. Configure los ajustes de 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 del cliente o haga clic en **cerrar** y cree el desencadenador más tarde.

Desencadenadores de la tarea del cliente

Para que una tarea del cliente se ejecute se debe asignar un desencadenador. Para crear un desencadenador, haga clic en **Tareas** > haga clic en la instancia Tarea del cliente en la tabla principal y seleccione > **Ejecutar en** en el

menú desplegable. También puede asignar una tarea del cliente a grupos u ordenadores.

Para definir un desencadenador, seleccione los ordenadores o grupos de **destino** en los que se debe ejecutar la tarea del cliente. Con los destinos seleccionados, defina las condiciones de **desencadenador** para ejecutar la tarea a una hora determinada o cuando se produzca un suceso concreto. También puede usar **Configuración avanzada - Aceleración** para especificar con precisión los ajustes del desencadenador, en caso de ser necesario.

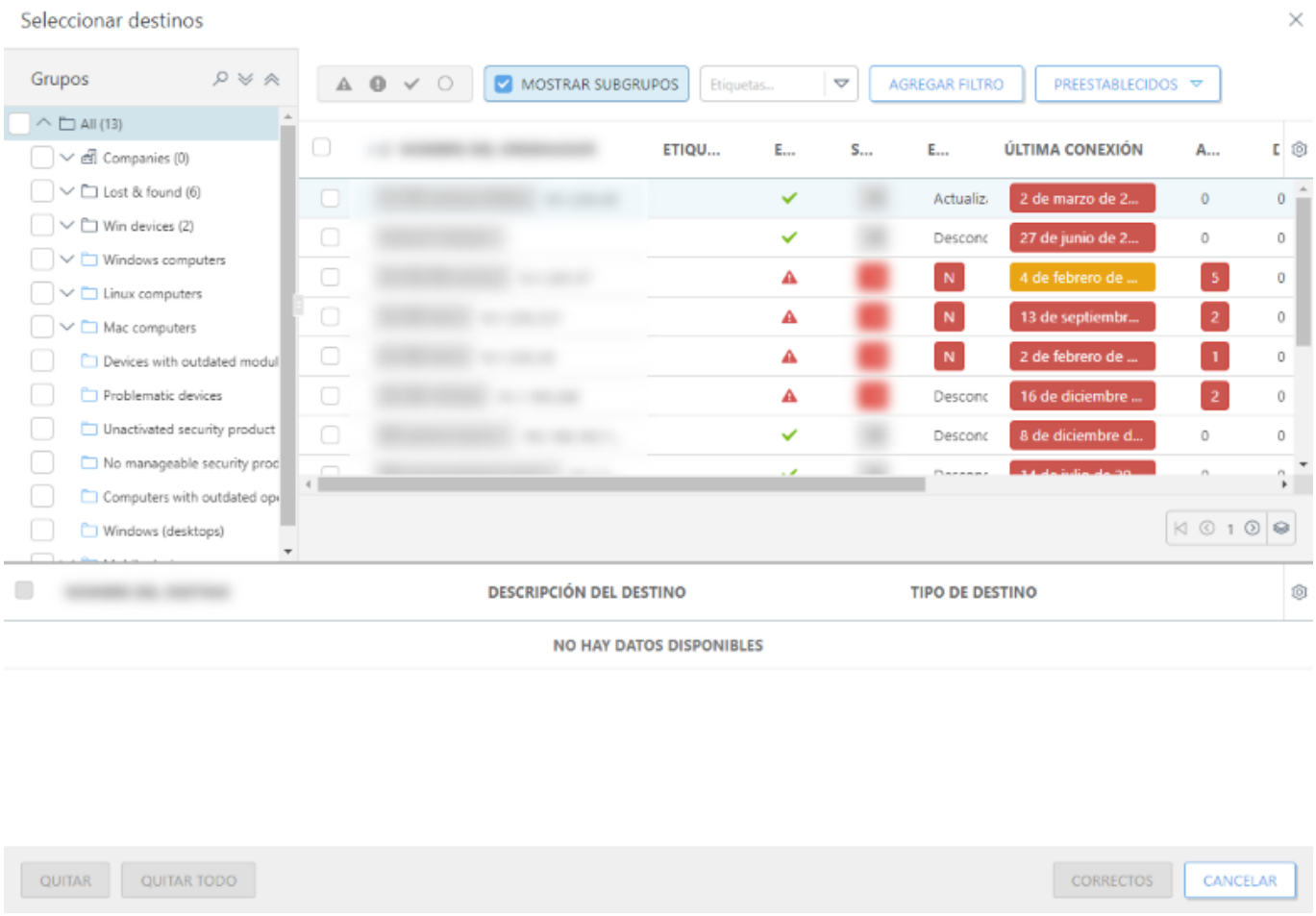
Básico

Introduzca información básica sobre el **Desencadenador en el campo Descripción** y, a continuación, haga clic en **Destino**.

Destino

La ventana **Destino** le permite especificar los clientes (grupos u ordenadores individuales) que son destinatarios de esta tarea. Haga clic en **Agregar destinos** para mostrar todos los grupos estáticos y dinámicos así como sus miembros.

> Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
> Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Tras la selección, haga clic en **Aceptar** y vaya a la sección **Desencadenador**.

Desencadenador

El desencadenador determina qué evento activa 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 efectuar hasta la **Fecha de caducidad**, se borra de la cola; no se elimina, pero no se ejecuta.
- **Programado**: ejecuta la tarea en el momento elegido.
- **Desencadenador de registro de eventos**: ejecuta la tarea en función de los sucesos especificados aquí. Este desencadenador se invoca cuando en los registros se produce un suceso determinado. 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 de destino. Si se selecciona un grupo estático o cliente individual, esta opción no está disponible.
- Expresión CRON: también puede establecer el intervalo de su desencadenador mediante una expresión CRON.

> Para obtener más información acerca de los desencadenadores, consulte el capítulo Tipos de desencadenadores de tarea.

Configuración avanzada: límites

Los límites se utilizan para evitar que una tarea se ejecute si esta se desencadena por un evento que ocurre con frecuencia, por ejemplo, el **Desencadenador de registro de eventos** o el **Desencadenador de grupo dinámico unido** (ver más arriba). Para obtener más información, consulte el capítulo Configuración avanzada: límites.

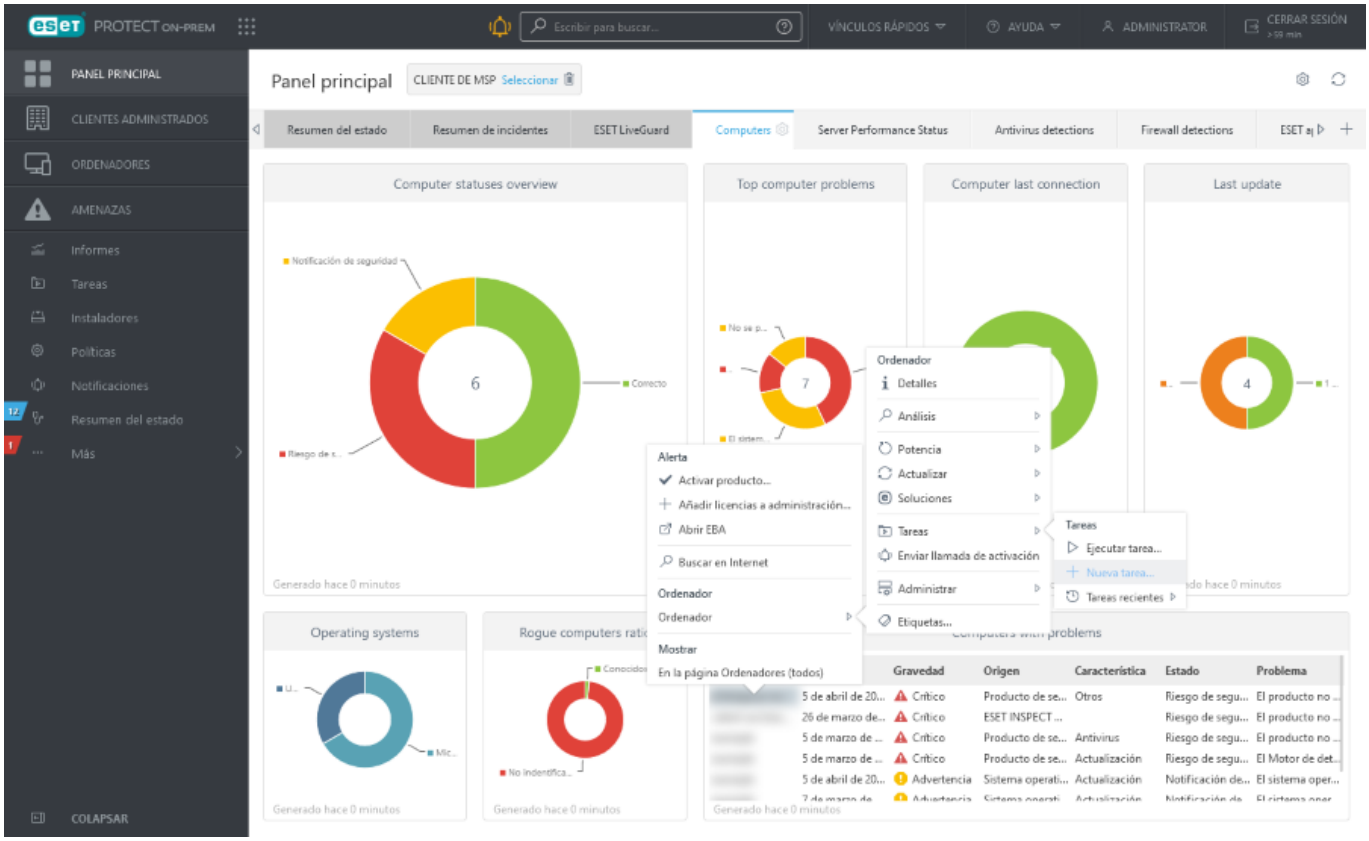
Haga clic en **Finalizar** cuando haya definido los destinatarios de esta tarea y los desencadenadores que la ejecutan.

Asignar una tarea del cliente a grupos u ordenadores

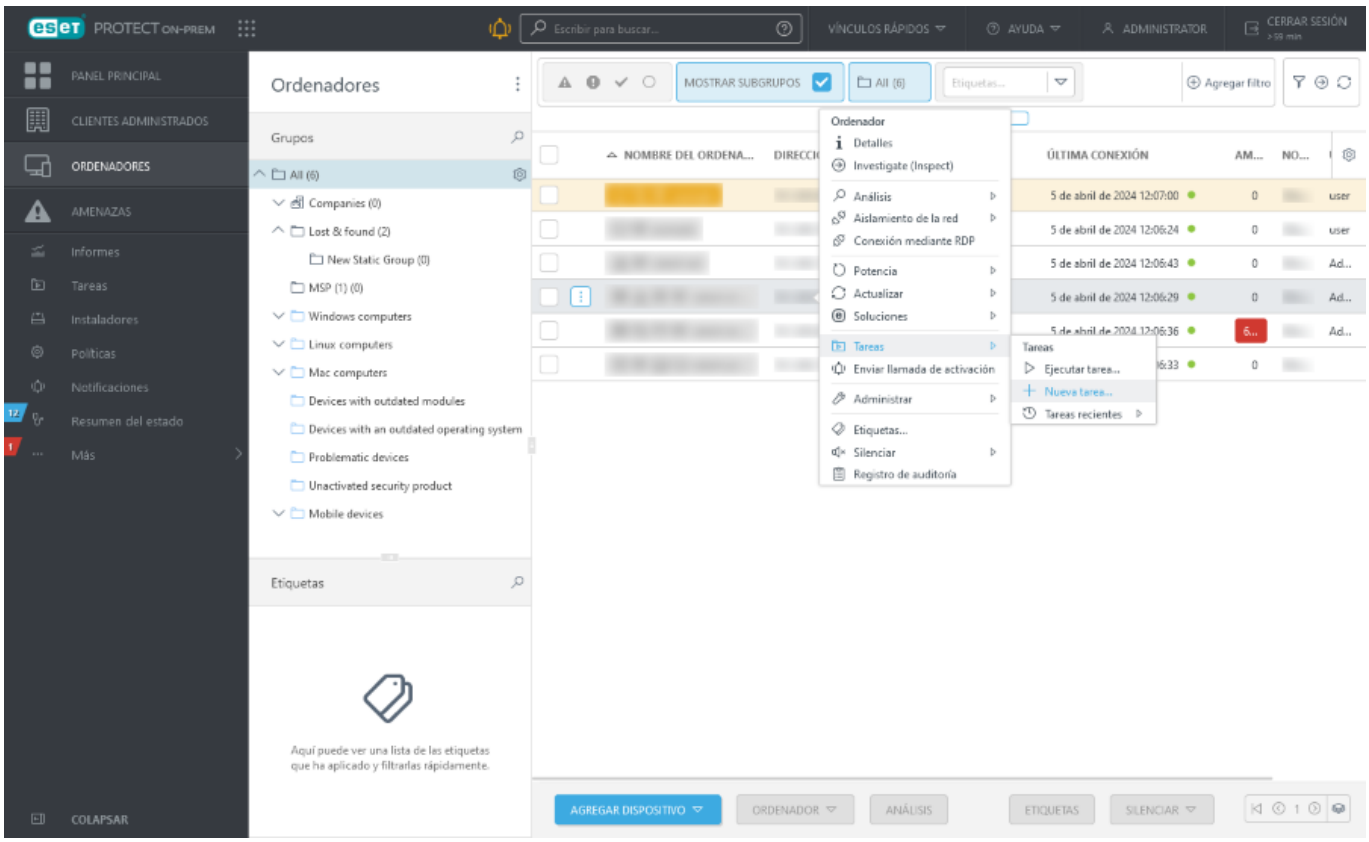
Lea cómo asignar una tarea del cliente a un grupo aquí.

Existen dos formas de asignar una tarea a ordenadores.

1. **Panel de control** > **Ordenadores** > **Ordenadores con problemas** > seleccione un ordenador y haga clic en **Ordenador** > **Tareas** > **Nueva tarea**



2.Ordenador > seleccione ordenadores con las casillas de verificación > **Tareas** > **Nueva tarea**.



Se abrirá la ventana del Asistente para nueva tarea del cliente.

Acciones Anti-Theft

La función **Anti-Theft** protege los dispositivos móviles del acceso no autorizado.

Si el dispositivo móvil del usuario (inscrito y administrado por ESET PROTECT On-Prem) se pierde o se lo roban, hay algunas acciones que se desencadenan automáticamente y otras que se pueden efectuar con una tarea del cliente.

Si una persona sin autorización cambia la tarjeta SIM por otra que no sea de confianza, ESET Endpoint Security para Android **bloqueará** automáticamente el dispositivo y enviará un SMS de alerta a los números de teléfono definidos por el usuario. Este mensaje incluirá la siguiente información:

- el número del dispositivo móvil de la tarjeta SIM que se está utilizando en ese momento
- el número **IMSI** (identidad internacional del abonado a un móvil)
- el número **IMEI** (identidad internacional de equipo móvil) del dispositivo móvil

El usuario no autorizado no tendrá conocimiento de que se ha enviado este mensaje porque se eliminará automáticamente de los hilos de mensaje del dispositivo. También puede solicitar las coordenadas **GPS** del dispositivo móvil perdido o borrar de forma remota todos los datos almacenados en el dispositivo por medio de una tarea del cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

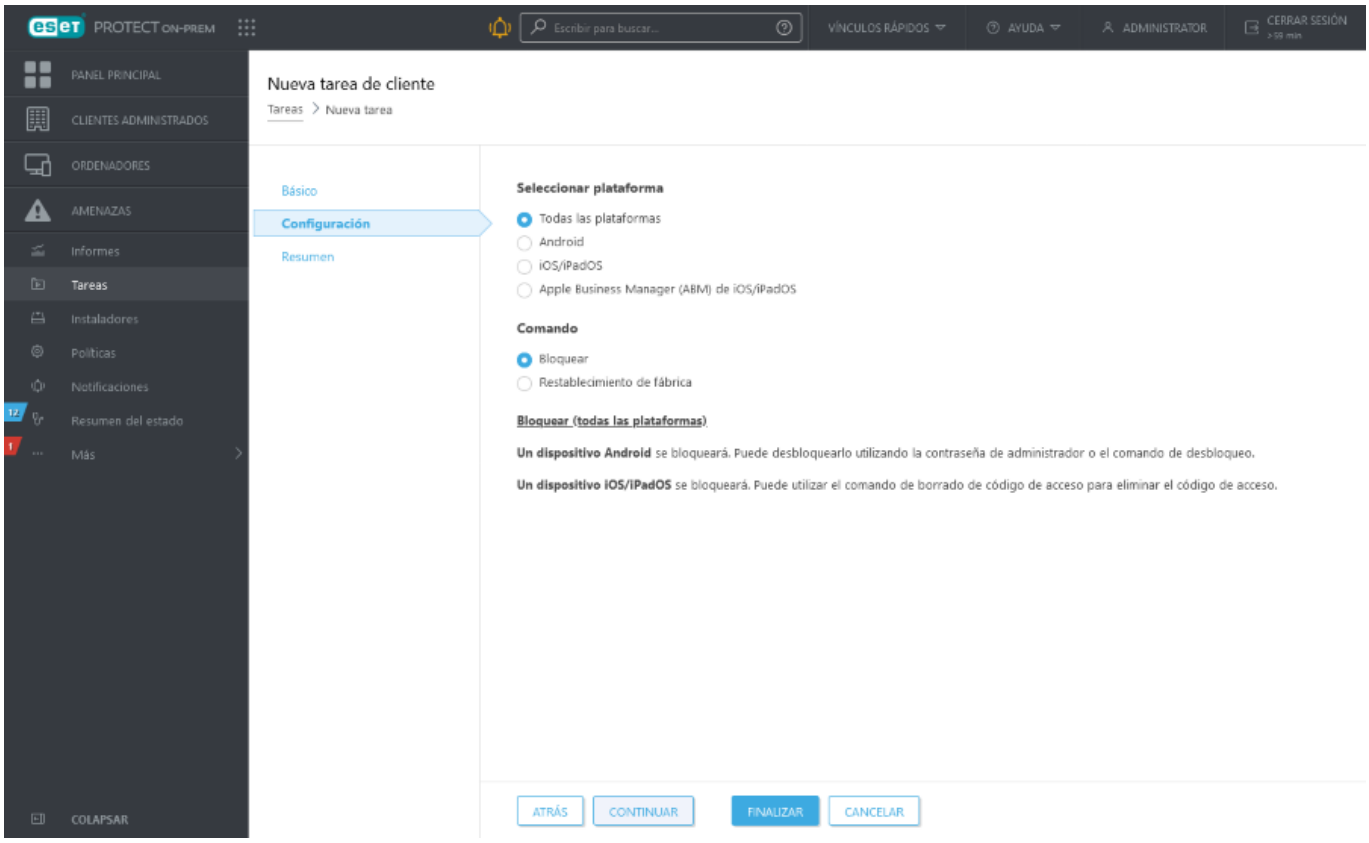
Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Acción	Comportamiento en SO para móvil	Descripción
Utilice la opción Buscar		: el dispositivo responderá con un mensaje de texto que contiene las coordenadas GPS. Si hay una ubicación más exacta transcurridos 10 minutos, el dispositivo enviará el mensaje de nuevo. La información recibida se muestra en los detalles del dispositivo. **Buscar** solo funciona si el GPS está activado en el dispositivo.
		No compatible.
Bloquear		Se bloqueará el dispositivo. El dispositivo se puede desbloquear con la contraseña de administrador o el comando de **desbloqueo**.
		Se bloqueará el dispositivo. Puede quitar el código de acceso con el comando **Borrar el código de acceso**.
Desbloquear		El dispositivo se desbloqueará para que pueda volver a utilizarse. La tarjeta SIM que actualmente se encuentra en el dispositivo se guardará como SIM de confianza.
		No compatible.
Sonido de Sirena/Modo perdido		El dispositivo se bloqueará y emitirá un sonido muy alto durante 5 minutos (o hasta que se desbloquee).
		No compatible.
Borrar el código de acceso		No compatible.
		Se quita el código de acceso del dispositivo. Se le pedirá al usuario que configure un nuevo código de acceso cuando encienda el dispositivo.

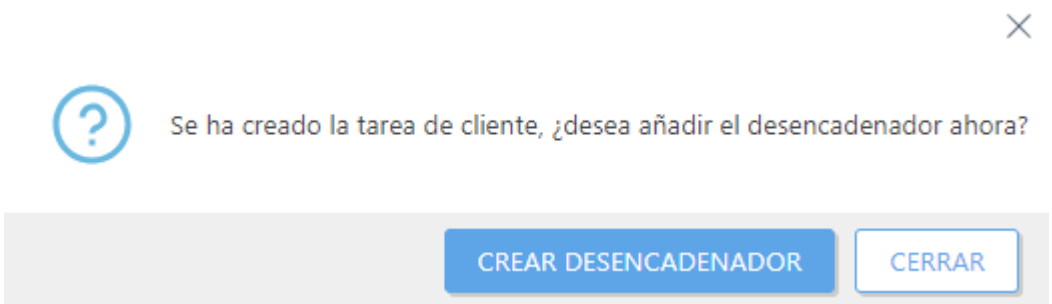
Acción	Comportamiento en SO para móvil	Descripción
Restablecimiento a valores de fábrica		Todos los datos accesibles en el dispositivo se borrarán (se destruirán los encabezados de los archivos) y el dispositivo volverá a los ajustes predeterminados de fábrica. Esto puede llevar varios minutos.
		Se eliminará toda la configuración y toda la información y el dispositivo volverá a los ajustes predeterminados de fábrica. Esto puede llevar varios minutos.
Activar Modo perdido y buscar		Compatible solo con iOS ABM. El dispositivo cambiará al "modo perdido", se bloqueará y solo podrá desbloquearse ejecutando la tarea **Desactivar el modo perdido** desde ESET PROTECT On-Prem. Puede personalizar el número de teléfono, el mensaje y la nota a pie de página que se mostrará en la pantalla del dispositivo perdido. El estado de protección del dispositivo cambiará a **Perdido**.
Desactivar el modo perdido		Compatible solo con iOS ABM. El estado de protección del dispositivo cambiará y el dispositivo volverá a funcionar con normalidad.



Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Buscar actualizaciones del producto

La tarea **Buscar actualizaciones del producto** activa la búsqueda de actualizaciones de productos de seguridad de ESET (actualizaciones automáticas) en los ordenadores administrados:

> Los productos de seguridad ESET compatibles:
> • 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.
- Para actualizar el producto de seguridad de ESET hay que reiniciar el ordenador, pero no inmediatamente (el reinicio no se fuerza). El administrador de ESET PROTECT On-Prem puede forzar la actualización y el reinicio del ordenador de forma remota desde la consola web mediante la tarea del cliente Apagar el ordenador con la casilla de verificación **Reiniciar ordenadores** seleccionada.
- El producto de seguridad de ESET anterior permanece totalmente operativo hasta el reinicio. La actualización se realiza después del siguiente reinicio del ordenador.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

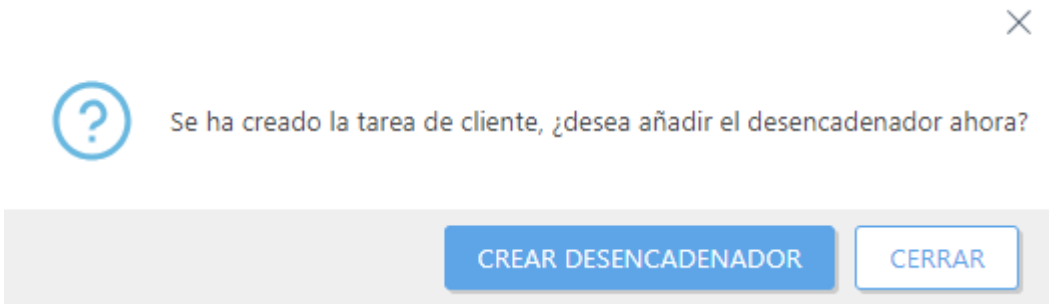
Configuración

> no hay **configuración** disponible para esta tarea.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Diagnóstico

Use la tarea **Diagnóstico** para solicitar una acción de diagnóstico de un producto de seguridad de ESET en un ordenador cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Acción de diagnóstico

- **Ejecutar Log Collector**: recopila datos concretos (como de configuración y registros) de un equipo seleccionado para facilitar la recopilación de información del equipo del cliente durante la resolución de un caso de asistencia técnica.

  o**Parámetros de Log Collector**: puede especificar los parámetros de Log Collector en Windows, macOS o Linux. Para recopilar todos los datos disponibles, deje en blanco el campo **Parámetros de Log Collector**. Si especifica los parámetros de Log Collector, seleccione solo ordenadores que ejecuten el sistema operativo correspondiente como destinos para la tarea.

El límite de tamaño de archivo para la entrega de registro por dispositivo es de 200 MB. Puede acceder a los registros desde Web Console en **Detalles** > sección **Registros**. Si los registros que ha recopilado la tarea superan los 200 MB, se producirá un error en la tarea. Si se produce un error en la tarea, puede:

- Recopilar los registros localmente en el dispositivo.
- Cambiar el nivel de detalle de los registros y repetir la tarea:
  - En el caso de destinos Windows, utilice el parámetro `/Targets:EraAgLogs` para recopilar solo los registros de ESET Management Agent.
  - En el caso de destinos Linux/macOS, utilice el parámetro `--no-productlogs` para excluir los registros del producto de seguridad de ESET instalado.

- **Configurar modo de diagnóstico** - El Modo de diagnóstico consta de las siguientes categorías: **Registro de correo no deseado**, **Registro de cortafuegos**, **Registro de HIPS**, **Registro de control de dispositivos** y **Registro de control web**. La finalidad principal del Modo de diagnóstico es recopilar registros con todos los niveles de seguridad en aquellas situaciones en las que es necesario realizar labores de solución de problemas.

  - **Activar**: activa el registro de todas las aplicaciones de ESET.

  - **Desactivar**: puede desactivar el registro manualmente, o el registro se desactivará automáticamente tras el reinicio del ordenador.

Los siguientes requisitos previos son necesarios para crear correctamente registros de diagnóstico:

- Los registros del Modo de diagnóstico pueden recopilarse de ordenadores cliente con sistemas operativos Windows y macOS.

- El ordenador cliente debe tener el producto de seguridad de ESET instalado y activado.

ESET Management Agent solo envía registros recopilados por un producto de ESET instalado en un ordenador cliente. La categoría y el nivel de detalle del registro dependen del tipo y de la configuración del producto. Configure cada producto (mediante Políticas) para recopilar registros específicos.

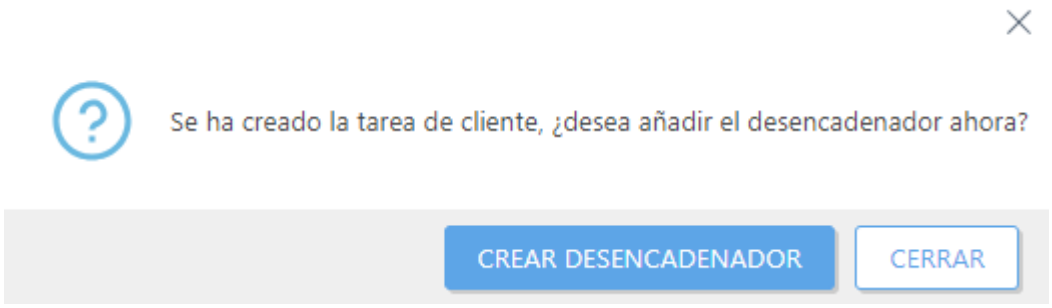
Los registros de diagnóstico con una antigüedad superior a las 24 horas se eliminan todos los días, durante la limpieza que se efectúa a medianoche. Esto evita que la base de datos de ESET PROTECT se sobrecargue.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Puede ver los registros creados en Detalles del ordenador: **Registros** > **Registro de diagnóstico**.

Mensaje de visualización

La tarea **Mensaje de visualización** le permite enviar un mensaje a cualquier dispositivo administrado (ordenador cliente, tableta, dispositivo móvil, etc.). El mensaje se mostrará en la pantalla para informar al usuario.

- Windows: el mensaje se muestra como notificación.

> En Windows, la tarea del cliente Mensaje de visualización utiliza el comando msg.exe, presente solo en las ediciones Windows Professional/Enterprise. Por ello, no puede utilizar esta tarea para mostrar un mensaje en un ordenador cliente con la edición Windows Home.

- macOS y Linux: el mensaje se muestra solo en un terminal.

> Para ver el mensaje en macOS o Linux, tiene que abrir el terminal.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

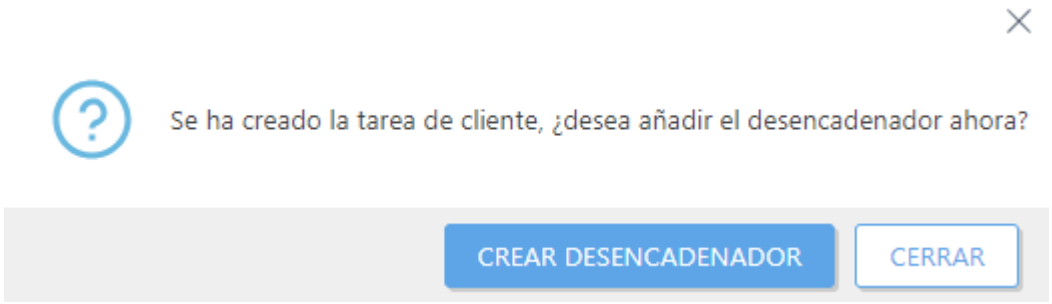
Configuración

Puede introducir un **Título** y escribir su **Mensaje**.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Finalizar aislamiento del ordenador de la red

La tarea **Finalizar aislamiento del ordenador de la red** finaliza el aislamiento del ordenador de la red y vuelve a permitir las conexiones de dicho ordenador. 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** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

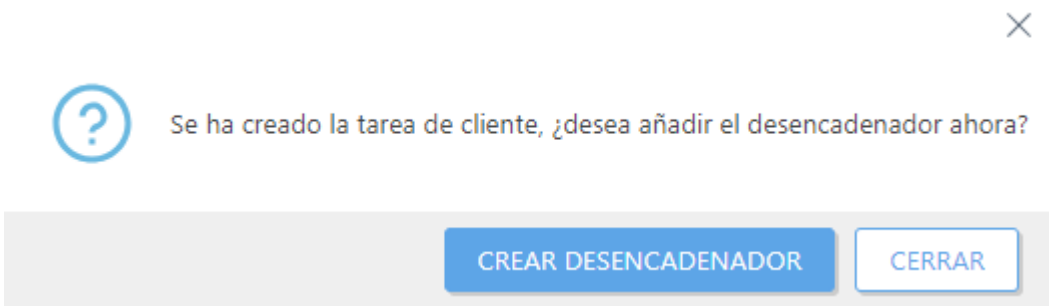
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

no hay **configuración** disponible para esta tarea.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Exportar configuración de productos administrados

La tarea **Exportar configuración de productos administrados** se utiliza para exportar la configuración de los componentes individuales de ESET PROTECT o los productos de seguridad de ESET instalados en los clientes.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

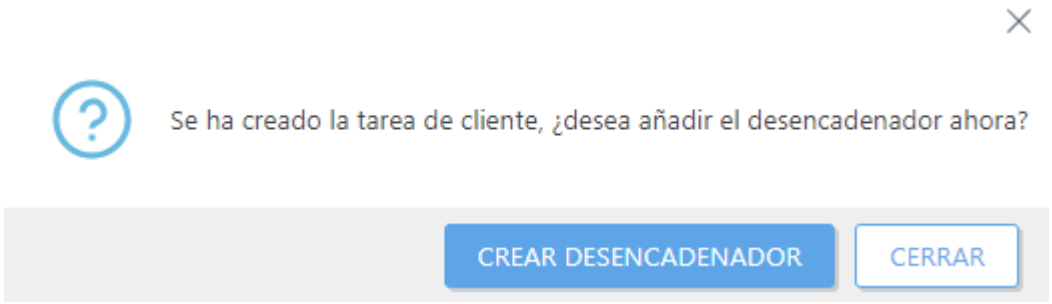
Exportar opciones de configuración de productos administrados.

- **Producto**: seleccione un componente de ESET PROTECT o un producto de seguridad de ESET cliente para los que desee exportar la configuración.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Cuando finalice la tarea, podrá encontrar la configuración exportada en la ficha **Configuración**, en los detalles del ordenador de los ordenadores de destino.

Aislar ordenador de la red

La tarea **Aislar ordenador de la red** aísla los ordenadores seleccionados de la red, y todas las conexiones, excepto aquellas que son necesarias para el correcto funcionamiento de los productos de ESET, se bloquearán. Entre las conexiones permitidas se incluyen:

- La obtención de una dirección IP por parte del ordenador.
- comunicación de *ekrn.exe*, ESET Management Agent, ESET Inspect Connector
- El inicio de sesión en un dominio.

El aislamiento de la red solo es compatible con los productos de seguridad de ESET (Endpoint Antivirus/Security y productos de seguridad para servidores).
Es probable que el aislamiento de red interrumpa el funcionamiento normal de los ordenadores, por lo que debe usarse únicamente en casos de emergencia (por ejemplo, si se identifica un problema de seguridad grave en un ordenador administrado). Puede finalizar el aislamiento con una tarea del cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

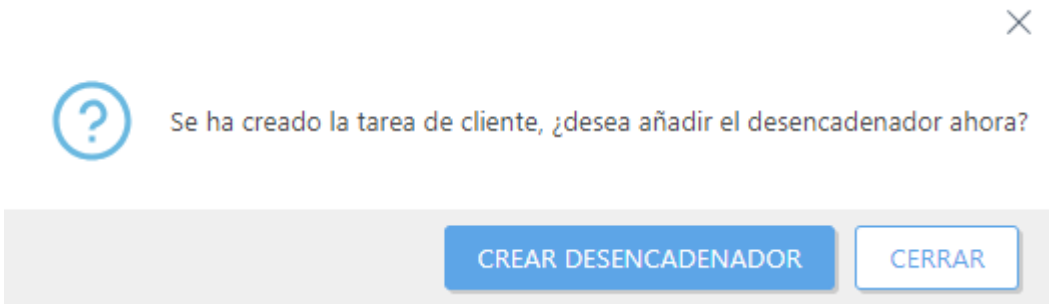
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

no hay **configuración** disponible para esta tarea.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Cerrar sesión

La tarea **Cerrar sesión** registra todos los usuarios del ordenador de destino. También puede hacer clic en un ordenador y seleccionar **Inicio/Apagado** > **Cerrar sesión**.

El ordenador debe ejecutar ESET Management Agent 10.0 o una versión posterior. La tarea del cliente **Cerrar sesión** fallará en un ordenador que ejecute una versión anterior del agente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

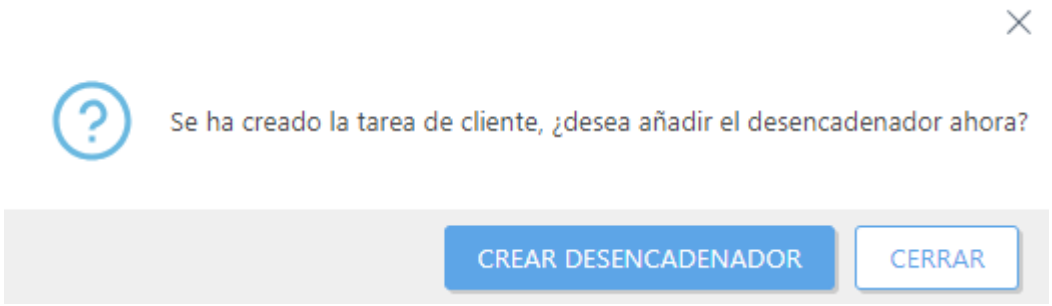
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

no hay **configuración** disponible para esta tarea.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Actualización de módulos

La tarea **Actualización de módulos** fuerza la actualización de todos los módulos del producto de seguridad instalado en un dispositivo de destino. Esta es una tarea general para todos los productos de seguridad de todos los sistemas. Puede encontrar la lista de todos los módulos del producto de seguridad de destino 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** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

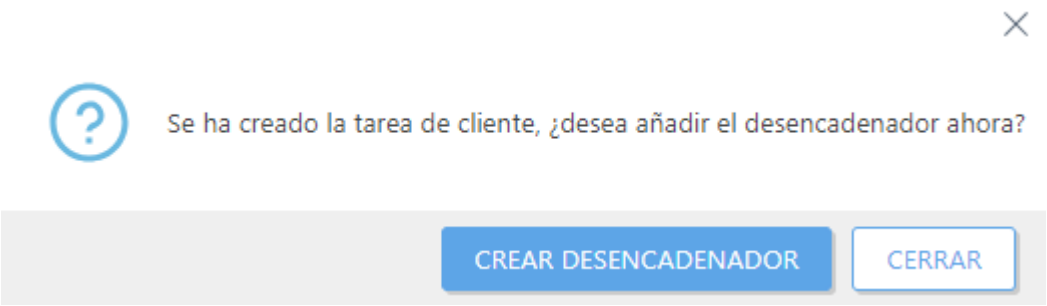
- **Borrar caché de actualización**: esta opción elimina los archivos de actualización temporales de la memoria caché del cliente y, con frecuencia, se puede utilizar para reparar los errores de actualizaciones de módulos.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Configurar un servidor personalizado para las actualizaciones de módulos

Si la actualización de los módulos del producto de seguridad de ESET falla debido al bloqueo geográfico, utilice una política para establecer un servidor personalizado para las actualizaciones de módulos:
1. En la configuración de la política de productos de seguridad de ESET, seleccione **Actualización** > **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 en los detalles de licencias anteriores.

Reversión de la actualización de módulos

Cuando la actualización de un módulo cause problemas, o cuando no quiera aplicar la actualización a todos los clientes (por ejemplo, para realizar pruebas, o cuando utilice actualizaciones de prueba), puede utilizar la tarea **Reversión de la actualización de módulos**. Cuando aplica esta tarea, los módulos se restablecen a la versión anterior.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Despliegue esta sección para personalizar la configuración de la reversión de la actualización de módulos.

Acción

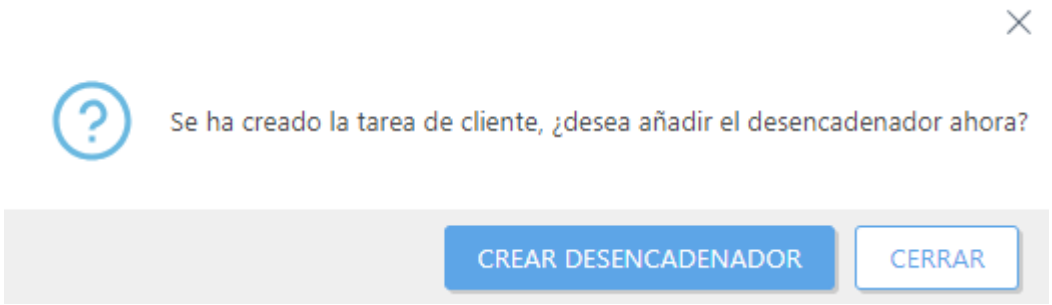
- **Activar actualizaciones:** las actualizaciones están activadas y el cliente recibirá la próxima actualización del módulo.
- **Revertir y desactivar actualizaciones hasta el siguiente**: las actualizaciones están desactivadas durante el periodo de tiempo específico del menú desplegable **Desactivar intervalo** (12, 24, 36 horas o hasta que se revoque).

Tenga cuidado al utilizar la opción **Hasta que se revoque**, ya que presenta un riesgo de seguridad.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Análisis a petición

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** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Apagar el ordenador tras el análisis: si marca esta casilla, el ordenador se apagará tras el análisis.

Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste.

Perfil de análisis

Puede seleccione el perfil que desee en el menú desplegable:

- **Análisis exhaustivo**: se trata de un perfil predefinido en el cliente, está configurado para ser el perfil de análisis más completo y realiza una comprobación de todo el sistema, pero también requiere más tiempo y recursos.
- **Análisis inteligente**: el análisis inteligente le permite iniciar rápidamente un análisis del ordenador y

desinfectar los archivos infectados sin la intervención del usuario. La ventaja del análisis inteligente es que es fácil de utilizar y no requiere una configuración detallada del análisis. El análisis estándar comprueba todos los archivos de los discos locales y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece automáticamente en el valor predeterminado.

• **Analizar desde menú contextual**: analiza un cliente utilizando un perfil de análisis predefinido; es posible personalizar los objetivos del análisis.

• **Perfil personalizado**: el análisis personalizado le permite especificar parámetros de análisis como objetivos y métodos de análisis. La ventaja del análisis personalizado es que permite configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis definidos por el usuario, para repetir el análisis con los mismos parámetros. Se debe crear un perfil antes de ejecutar la tarea con la opción de perfil personalizado. Cuando seleccione un perfil personalizado en el menú desplegable, escriba el nombre exacto del perfil en el campo de texto **Perfil personalizado**.

Desinfección

De forma predeterminada, se selecciona **Analizar y limpiar**. Esta configuración activa la limpieza automática de los objetos infectados encontrados. Si no es posible se ponen en cuarentena.

Analizar destinos

La opción **Analizar todos los destinos** también está seleccionada de forma predeterminada. Con esta opción se analizan todos los objetivos especificados en el perfil de análisis. Si anula la selección de esta opción, deberá especificar manualmente los objetivos del análisis en el campo **Agregar destino**. Escriba el objetivo del análisis en el campo de texto y haga clic en **Agregar**. El objetivo se muestra en el campo **Destinos del análisis** a continuación. Un objeto de análisis puede ser un archivo o una ubicación. Además, puede ejecutar un análisis predefinido con cualquiera de las siguientes cadenas como **Objeto de análisis**:

Objeto de análisis	Ubicaciones analizadas
`${DriveRemovable}`	Todos los dispositivos y unidades extraíbles.
`${DriveRemovableBoot}`	Sectores de arranque de todas las unidades extraíbles.
`${DriveFixed}`	Discos duros (HDD, SSD).
`${DriveFixedBoot}`	Sectores de arranque de los discos duros.
`${DriveRemote}`	Unidades de red.
`${DriveAll}`	Todas las unidades disponibles.
`${DriveAllBoot}`	Sectores de arranque y UEFI de todas las unidades. Puede obtener más información sobre el análisis UEFI en el glosario.
`${DriveSystem}`	Unidades del sistema.
`${Share}`	Unidades compartidas (solo para productos de servidor).
`${Boot}`	Sector de arranque principal.
`${Memory}`	Memoria operativa.
`${Registry}`	Registro del sistema (solo para ESET Endpoint 8 y versiones posteriores).
`${Wmi}`	Base de datos WMI (solo para ESET Endpoint 8 y versiones posteriores).

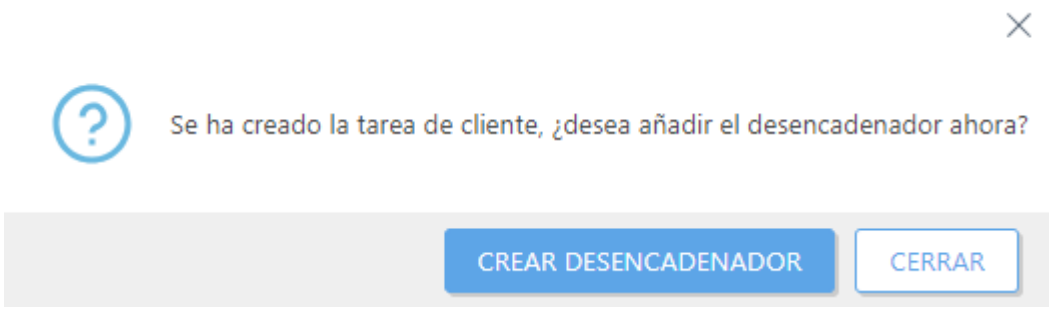
A continuación se exponen algunos ejemplos de uso de los parámetros de objeto del **Análisis a petición**:
■Archivo: *C:\Users\Data.dat*
■Carpeta: *C:\MyFolder*
■Ruta o archivo Unix */usr/data*
■Ubicación UNC de Windows *\\server1\scan_folder*
■Cadena predefinida `${Memory}`

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

• Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Actualización del sistema operativo

La tarea Actualización del sistema operativo se utiliza para actualizar el sistema operativo del ordenador cliente. Esta tarea puede desencadenar la actualización del sistema operativo en los sistemas operativos 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). Comprueba distintos administradores de paquetes, por lo 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 invocando una API interna de Windows. No instala actualizaciones de la función, que actualiza Windows a una versión más reciente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

- **Aceptar CLUF automáticamente** (solo Windows): active esta casilla de verificación si quiere aceptar el CLUF automáticamente. No se mostrará texto al usuario. Si no acepta el CLUF, la tarea omite las actualizaciones que requieran la aceptación del CLUF.
- **Instalar actualizaciones opcionales** (solo Windows): las actualizaciones marcadas como opcionales que no requieren intervención del usuario también se instalarán.
- **Permitir reinicio** (Windows y macOS): fuerza al ordenador cliente para que se reinicie tras la instalación de las actualizaciones que requieren un reinicio.

Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste. Si el ordenador administrado no admite la configuración del comportamiento de reinicio:

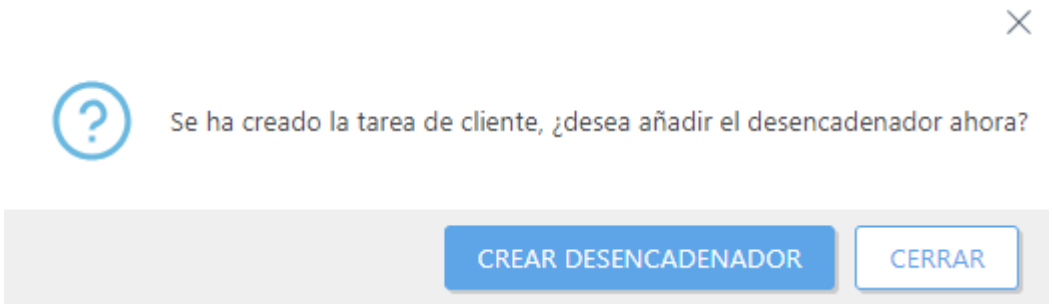
- Windows informará al usuario del ordenador sobre el reinicio forzado planificado 4 horas antes del reinicio y 10 minutos antes del mismo.
- macOS se reiniciará inmediatamente después de la actualización.

- Se instalarán actualizaciones que requieran reiniciarse, aunque no active la casilla de verificación **Permitir reinicio**.
- **Configuración** no influye en la tarea si en el dispositivo de destino se está ejecutando un tipo de SO no compatible.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Administración de cuarentena

La tarea **Administración de cuarentena** se utiliza para administrar los objetos en cuarentena en ESET PROTECT On-Prem: objetos infectados o sospechosos encontrados durante el análisis.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Configuración de la administración de cuarentena

Acción: seleccione la acción que desea realizar con el objeto que está en cuarentena.

- **Restaurar objetos** restaura el objeto a su ubicación original, pero se analiza y, si persisten las razones de la cuarentena, el objeto se pone de nuevo en cuarentena.
- **Restaurar objetos y excluirlos en el futuro** restaura el objeto a su ubicación original y no lo volverá a poner en cuarentena de nuevo.
- **Eliminar objetos**: elimina el objeto de forma permanente.

Tipo de filtro: filtra los objetos en cuarentena en función de los criterios definidos a continuación.

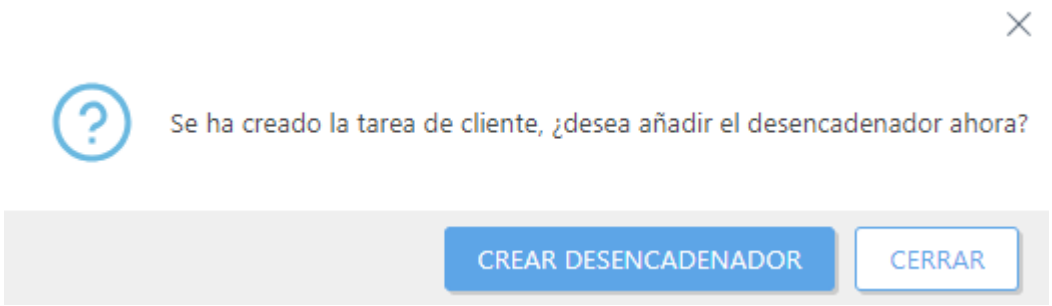
Configuración del filtro:

- **Elementos de hash**: agregue elementos de hash al campo. Solo se pueden introducir los objetos conocidos; por ejemplo, un objeto que ya se haya puesto en cuarentena.
- **Ocurrió** > **Ocurrido desde**, **Ocurrido hasta**: defina el intervalo de tiempo durante el que se ha puesto en cuarentena el objeto.
- **Tamaño** > **Tamaño mínimo/máximo (bytes)**: permite definir el intervalo de tamaño del objeto que se ha puesto 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 las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Activación del producto

Use la tarea **Activación del producto** para activar un producto de seguridad de ESET en un ordenador cliente o un dispositivo móvil.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Configuración de activación del producto – Seleccione la licencia del producto adecuada en la lista de licencias disponibles. Esta licencia se aplicará a los productos ya instalados en el cliente. La lista de licencias disponibles no muestra las licencias caducadas o sobreutilizadas (las que tienen estado **Error** u **Obsoleto**). Puede agregar una licencia con uno de los métodos descritos en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de inicio sea **Todo** y que tenga el permiso de **Escritura** en las licencias.

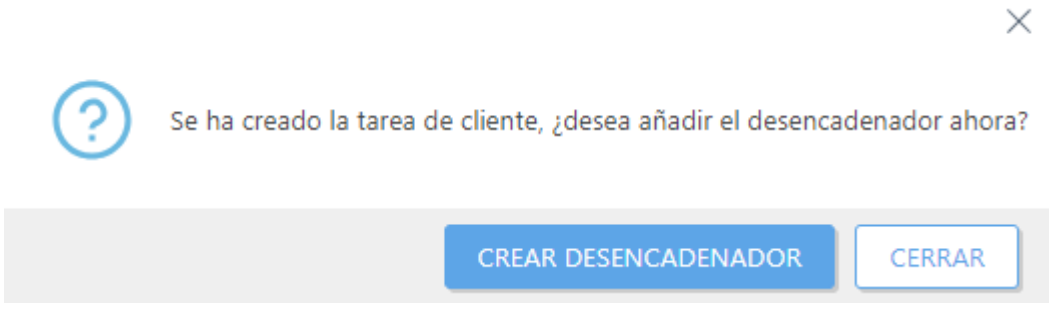
La tarea **Activación del producto** puede activar un producto móvil, ESET Endpoint para Android, también con una licencia sin conexión.
La tarea de activación no puede activar los productos de ESET de las versiones 4 y 5 con la licencia sin conexión. Debe activar el producto manualmente o utilizar una versión del producto compatible (se recomienda usar la versión más reciente).

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Reiniciar agente clonado

Puede distribuir ESET Management Agent en su red mediante una imagen predefinida, como se describe en este artículo de la base de conocimiento. Los agentes clonados tienen el mismo SID, lo que puede causar problemas (múltiples agentes con el mismo SID). Para resolver esta situación, utilice la tarea **Reiniciar agente clonado** para restablecer el SID y asignar a los agentes una identidad única.

ESET Management Agent identifica las máquinas cliente clonadas que se ejecutan en Windows automáticamente, sin la tarea Reiniciar agente clonado. Solo las máquinas cliente con Linux y macOS (y clientes Windows con la detección de hardware desactivada) necesitan la tarea para dividir las máquinas clonadas.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

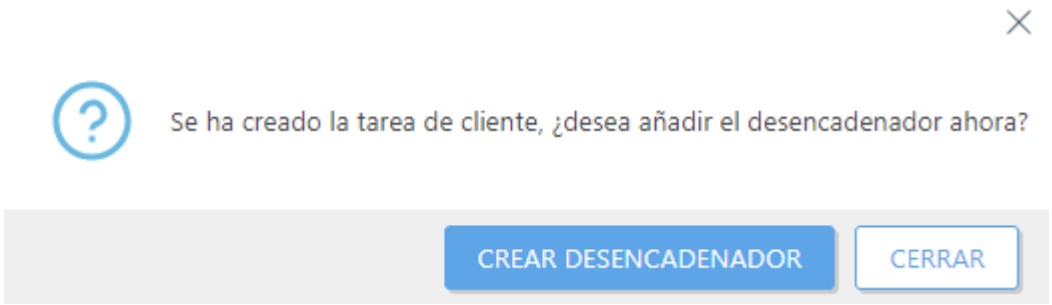
Ejecute esta tarea con cuidado. Tras el restablecimiento de la instancia actual de ESET Management Agent, se abandonarán todas las tareas que se estén ejecutando en ella. Es posible que los estados de ejecución **En ejecución**, **Finalizado** o **Con error** de esta tarea no se tengan en cuenta, en función de la replicación de datos.

no hay **configuración** disponible para esta tarea.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Restablecimiento de la base de datos de Rogue Detection Sensor

La tarea **Restablecimiento de la base de datos de Rogue Detection Sensor** se utiliza para restablecer la caché de búsqueda del Sensor RD. La tarea elimina la memoria caché y almacena de nuevo los resultados de la búsqueda, pero no elimina los ordenadores detectados. Esta tarea es útil cuando los ordenadores detectados se encuentran todavía en la memoria caché y no se ha informado al servidor.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

no hay **configuración** disponible para esta tarea.

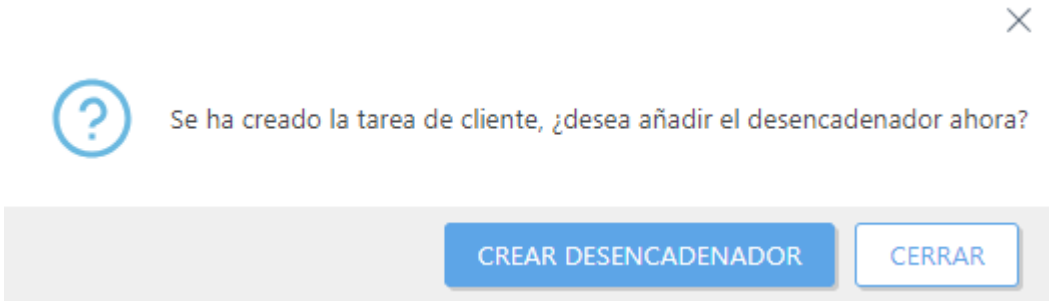
Cuando cree un desencadenador para esta tarea, elija un ordenador que tenga instalado RD Sensor.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Ejecutar comando

La tarea **Ejecutar comando** se puede utilizar para ejecutar las instrucciones específicas de la línea de comandos en el cliente. El administrador puede especificar la entrada de la línea de comandos que ejecutar.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del 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. Debido a esto, la ejecución de comandos con requisitos sobre la interfaz gráfica de usuario de la aplicación puede fallar.

Puede usar los comandos de `ecmd` con la tarea Ejecutar comando. Para obtener más información, visite este artículo de la Base de conocimiento.

Sistema operativo	El comando se ejecutará como usuario	Directorio de trabajo predeterminado	Ubicaciones de red accesibles	El comando se ejecutará en
Windows	*Local System*	*C:\Windows\Temp*	Solo ubicaciones del dominio actual y disponibles para el usuario Sistema local	Símbolo del sistema (`cmd.exe`)
Linux o macOS	*root*	*/tmp*	Solo si la ubicación está montada y disponible para el usuario raíz	Consola

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

- **Línea de comando que ejecutar**: introduzca una línea de comandos que desee ejecutar en los clientes.

• **Directorio de trabajo**: introduzca el directorio donde se ejecutará la línea de comandos indicada anteriormente.

Puede escribir un comando de varias líneas. Restricciones de longitud máxima de los comandos:
• Web Console puede procesar hasta 32.768 caracteres. Si copia y pega un comando más largo, se recortaría el final automáticamente.
• Linux y macOS pueden procesar la longitud completa del comando. Windows tiene una restricción de 8.191 caracteres como máximo.

• Para ejecutar un script local que está en un cliente en *C:\Users\user\script.bat*, siga estos pasos:
1.Cree una nueva tarea de cliente y seleccione **Ejecutar comando**.
2.En la sección **Configuración**, introduzca:
Línea de comando que ejecutar: `call script.bat`
Directorio de trabajo: *C:\Users\user*
3.Haga clic en **Finalizar**, cree un desencadenador y seleccione los clientes de destino.
• Para ejecutar un comando de varias líneas para reiniciar un servicio de Windows de forma remota (sustituya `service_name` por el nombre de servicio, por ejemplo, `wuauserv` para el servicio Windows Update):

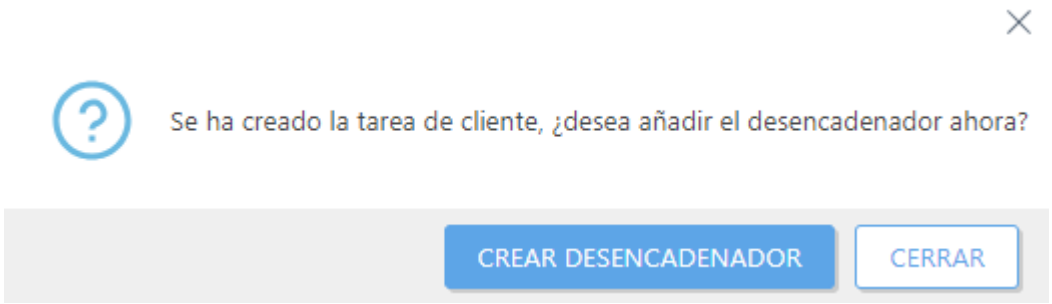
```
net stop service_name
net start service_name
```

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

• Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Análisis de la salida de la tarea Ejecutar comando

1. Haga clic en **Tareas** > seleccione la tarea > **Mostrar detalles** > ficha **Ejecuciones** > haga clic en una línea de la tabla > **Historial**.

2. La columna **Mensaje de seguimiento** contiene los primeros 255 caracteres de la salida de la tarea Ejecutar comando. Puede crear informes y procesar estos datos desde varios ordenadores. Puede descargar una salida más grande como registro del Log Collector en **Detalles del ordenador** > **Registros** > Log Collector.

Ejecutar script de SysInspector

La tarea **Ejecutar script de SysInspector** se utiliza para eliminar objetos no deseados del sistema. Para utilizar esta tarea primero es necesario exportar un script de SysInspector desde ESET SysInspector. Después de exportar el script puede marcar los objetos que desea eliminar, ejecutar el script con los datos modificados y se eliminarán los objetos marcados.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

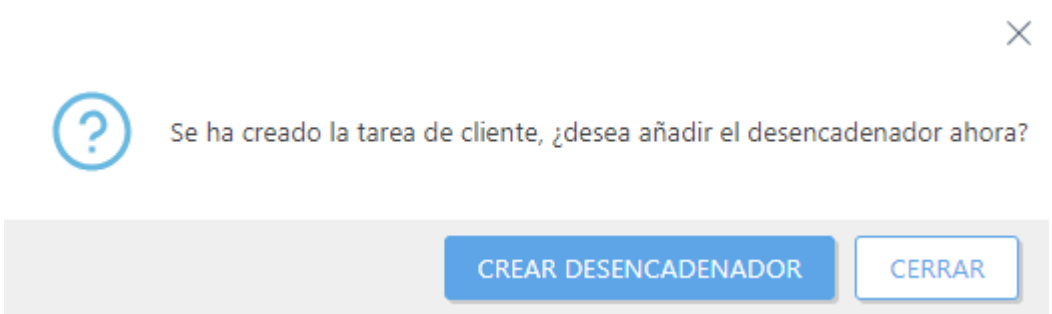
Configuración

- **Script de SysInspector**: haga clic en **Examinar** para desplazarse hasta el script del servicio. El script del servicio debe crearse antes de ejecutar esta tarea.
- **Acción**: puede **Cargar** o **Descargar** un script de ESET PROTECT Web Console.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Cuando finalice la tarea puede comprobar los resultados en un informe.

Actualización de componentes de ESET PROTECT

La tarea **ESET PROTECT Actualización de componentes** se utiliza para actualizar los componentes de ESET PROTECT (ESET Management Agent, ESET PROTECT Server, Web Console, ESET Bridge y MDM, pero no Apache Tomcat ni Proxy HTTP Apache). La tarea de actualización solo se puede ejecutar en un equipo que tenga ESET Management Agent instalado. El agente también se necesita en un ESET PROTECT Server.

ESET PROTECT On-Prem le envía automáticamente una notificación cuando hay una nueva versión de ESET PROTECT Server disponible.
Puede actualizar a ESET PROTECT On-Prem 11.0 a partir de 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 la vida útil y no se admite. Consulte la Guía de instalación para obtener instrucciones detalladas.
Consulte también otras formas de actualizar ESET PROTECT On-Prem a la versión más reciente.

Con el fin de evitar fallos de instalación, agente de ESET Management realiza las siguientes comprobaciones antes de instalar o actualizar los productos de ESET:

- Si se puede acceder al repositorio.
- Si hay suficiente espacio libre (1 GB) en el equipo cliente (no disponible para Linux)

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

- **Instancia de ESET PROTECT Server de referencia**: seleccione la versión ESET PROTECT Server en la lista.

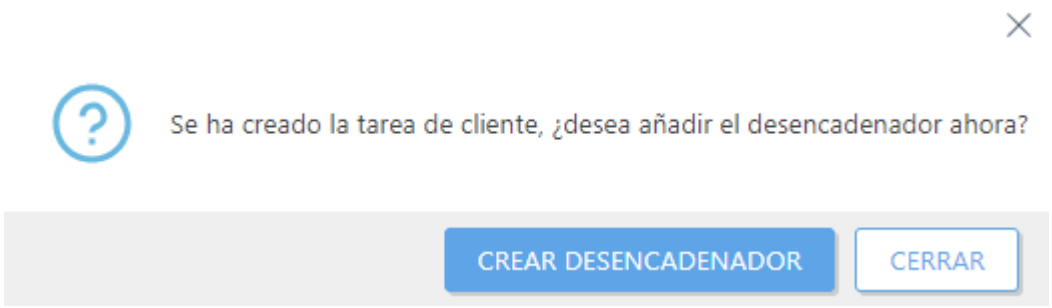
Todos los componentes de ESET PROTECT se actualizarán a versiones compatibles con el servidor seleccionado.

Marque la casilla de verificación situada junto a **Reiniciar automáticamente cuando sea necesario** para forzar un reinicio automático del ordenador cliente tras la instalación. También puede dejar esta opción sin seleccionar y reiniciar manualmente el ordenador cliente. Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

> La actualización puede llevar más tiempo, en función del sistema y la configuración de red. No puede acceder a Web Console durante la actualización de ESET PROTECT Server o Web Console. Tras la actualización, inicie sesión en Web Console y compruebe que tiene la versión de ESET PROTECT On-Prem más reciente en **Ayuda** > Acerca de.

Enviar archivo a ESET LiveGuard

Para ejecutar esta tarea, vaya a **Detecciones**.

Enviar archivo a ESET LiveGuard solo está disponible para **archivos bloqueados**. Puede enviar un archivo para el análisis de malware (ESET LiveGuard Advanced) desde ESET PROTECT Web Console. Puede ver los detalles del análisis del archivo en Archivos enviados. Puede enviar manualmente archivos ejecutables a ESET LiveGuard Advanced para su análisis desde el producto de ESET Endpoint (necesita tener la licencia de ESET LiveGuard Advanced).

Análisis del servidor

Puede usar la tarea **Análisis del servidor** para analizar clientes con la versión de ESET Server instalada. El tipo de análisis ejecutado depende de la solución de ESET instalada:

Producto	Análisis	Descripción
ESET Server Security para Windows (anteriormente ESET File Security para Microsoft Windows Server)	**Análisis Hyper-V**	Este tipo de análisis le permite analizar los discos de una instancia de Microsoft Hyper-V Server, que es una máquina virtual (VM), sin instalar ESET Management Agent en la máquina virtual.
ESET Security para Microsoft SharePoint Server	**Análisis de la base de datos SharePoint, análisis Hyper-V**	Esta funcionalidad permite que ESET PROTECT On-Prem utilice el destino de análisis adecuado al ejecutar la tarea del cliente **Análisis del servidor** en un servidor con ESET Security para Microsoft SharePoint.
ESET Mail Security para Microsoft Exchange Server	**Análisis de la base de datos de buzones a petición, análisis Hyper-V**	Esta funcionalidad permite que ESET PROTECT On-Prem utilice el destino de análisis adecuado. Cuando ESET PROTECT On-Prem ejecuta una tarea del cliente **Análisis del servidor**, recopila la lista de destinos y se le pedirá que seleccione los destinos de análisis para el análisis de la base de datos de buzones a petición en ese servidor concreto.
ESET Mail Security para IBM Domino	**Análisis de la base de datos a petición , análisis Hyper-V**	Esta funcionalidad permite que ESET PROTECT On-Prem utilice el destino de análisis adecuado al ejecutar la tarea del cliente **Análisis 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** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

- Haga clic en **Seleccionar** en **Servidor analizado** y seleccione un ordenador que tenga instalado un producto ESET Server Security. Se le pedirá que seleccione unidades, carpetas o archivos concretos de ese ordenador para analizarlos.
- Seleccione un **Desencadenador** para esta tarea, o defina los límites. De forma predeterminada, la tarea se ejecuta en cuanto resulta posible.

Analizar destinos

ESET PROTECT On-Prem le ofrece una lista de los destinos disponibles en el servidor seleccionado. Para usar esta lista se debe activar **Generar lista de objetos** en la política para su producto de servidor en **Herramientas** > **Objetos de análisis de ESET Management**:

- **Generar lista de objetos**: active este ajuste para permitir que ESET PROTECT On-Prem genere listas de objetos.
- **Periodo de actualización [minutos]**: la primera vez que se genere la lista de destinos, se tardará aproximadamente la mitad del tiempo aquí indicado.

Seleccione en la lista los destinos de análisis. Para obtener más información, consulte Objetos del análisis de ESET PROTECT On-Prem.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Apagar el ordenador

Puede utilizar la tarea **Apagar el ordenador** para apagar o reiniciar ordenadores clientes.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

- **Reiniciar ordenadores**: marque esta casilla si desea reiniciar el ordenador cliente después de finalizar la tarea. Anule la selección de esta opción si desea apagar los ordenadores.

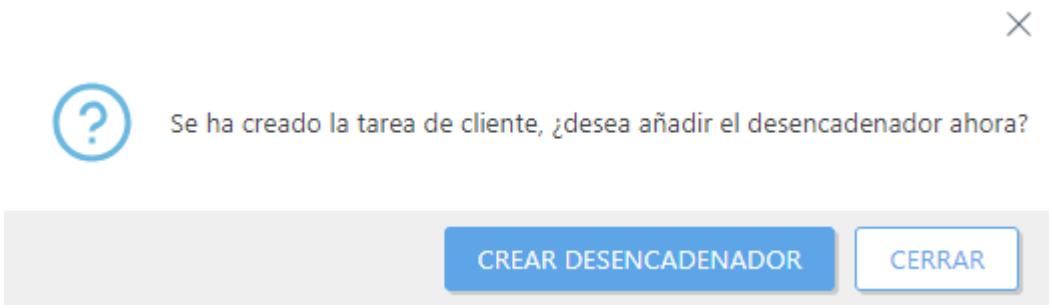
Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible

con este ajuste.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Instalación del software

Utilice la tarea **Instalación del software** para instalar software en los ordenadores cliente:

- Instale productos de seguridad de ESET. También puede usar el menú contextual de **Ordenadores**. Haga clic en un ordenador y seleccione **Soluciones** > **Implementar producto de seguridad** para implementar un producto de seguridad ESET en el ordenador.
- Actualizar productos de seguridad de ESET Ejecute la tarea con el paquete instalador más reciente para realizar la instalación de la versión más reciente sobre la solución existente. Puede ejecutar una actualización del producto de seguridad de ESET inmediata desde **Panel** con acciones con un solo clic. Consulte las instrucciones de actualización de ESET Security para Microsoft SharePoint para completar esta actualización.
- Instale software de terceros.

Tanto ESET PROTECT Server como ESET Management Agent deben disponer de acceso a Internet para poder acceder al repositorio y efectuar instalaciones. Si no tiene acceso a Internet, debe instalar el software cliente localmente, ya que la instalación remota fallará, o crear un repositorio sin conexión. Con el fin de evitar fallos de instalación, agente de ESET Management realiza las siguientes comprobaciones antes de instalar o actualizar los productos de ESET:

- Si se puede acceder al repositorio.
- Si hay suficiente espacio libre (1 GB) en el equipo cliente (no disponible para Linux)

Al realizar una tarea Instalación de software en ordenadores situados en un dominio con ESET Management Agent en ejecución, el usuario debe tener permiso de *Lectura* de la carpeta en la que se encuentran los instaladores. Si es necesario, siga los pasos indicados a continuación para conceder estos permisos:

1.Agregue una cuenta del ordenador de Active Directory al ordenador en el que se ejecuta la tarea (por ejemplo, *NewComputer$*).

2.Otorgue permisos de **Lectura** a *NewComputer$*; para ello haga clic con el botón derecho en la carpeta en la que están situados los instaladores y seleccione **Propiedades** > **Uso compartido** > **Compartir en el menú contextual**. Tenga en cuenta que el símbolo "$" debe estar al final de la cadena del nombre del ordenador. La instalación desde una ubicación compartida solo puede realizarse si el ordenador cliente forma parte de un dominio.

No utilice una tarea de Instalación del software para actualizar componentes de ESET PROTECT (Agent, Server, MDM). En su lugar, utilice la tarea Actualización de componentes. Puede utilizar una tarea Instalación del 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** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Paquete que instalar: hay dos opciones:

- **Instalar paquete desde el repositorio**

  oElija un sistema operativo: seleccione el sistema operativo para la instalación del producto.

  oSeleccionar paquete desde el 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 (recomendado). Puede seleccionar una versión anterior. Para

actualizar un producto de ESET, seleccione la versión más reciente disponible. También puede hacer clic en **Personalizar más configuraciones** y seleccionar 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 **Aceptar**.

o**Instalar la versión más reciente**: marque la casilla de verificación para instalar la versión más reciente del producto de ESET si el EULA del producto ya está aceptado.

• **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 está realizando la instalación desde un servidor web público o desde su servidor HTTP.

o*file://\\pc22\install\ees_nt64_ENU.msi*: si está realizando la instalación desde una ruta de acceso de la red.

o*file://C:\installs\ees_nt64_ENU.msi*: si está realizando la instalación desde la ruta de acceso local.

Licencia de ESET –Seleccione la licencia del producto adecuada en 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 caducadas o sobreutilizadas (las que tienen 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 con uno de los métodos descritos en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de inicio sea **Todo** y que tenga el permiso de **Escritura** en las licencias.

• Seleccione una licencia solo cuando instale o actualice productos no activos o si quiere cambiar la licencia que se utiliza en ese momento por otra.

• No seleccione una licencia cuando actualice un producto ya activado.

Activar ESET LiveGuard: la casilla de verificación está disponible cuando tiene una licencia de ESET LiveGuard Advanced y ha seleccionado un producto de seguridad de ESET compatible con ESET LiveGuard Advanced y la licencia del producto. Marque la casilla de verificación para activar ESET LiveGuard Advanced en los ordenadores de destino de la tarea Instalación del software. Tras la activación, podrá administrar la configuración de ESET LiveGuard Advanced mediante una política.

Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

Si ha seleccionado un producto de seguridad de ESET para Windows:Marque la casilla de verificación situada junto al ajuste para activarlo para el instalador:

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

o**Activar la detección de aplicaciones potencialmente indeseables**: obtenga más información en este artículo de la base de conocimiento.

Los parámetros de instalación (opcional):

• Utilice los parámetros de instalación de la línea de comandos solo con los ajustes de interfaz de usuario

reducido, **básico** y **ninguno**.

• Consulte la documentación de la versión de **msiexec** utilizada para los modificadores de la línea de comandos correspondientes.

• Lea la ayuda en línea correspondiente de la instalación de la línea de comandos de los productos ESET Endpoint y los productos ESET Server.

Marque la casilla de verificación situada junto a **Reiniciar automáticamente cuando sea necesario** para forzar un reinicio automático del ordenador cliente tras la instalación. También puede dejar esta opción sin seleccionar y reiniciar manualmente el ordenador cliente. Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste.

Instalación de software de terceros

Puede utilizar la tarea **Instalación de software** para instalar software que no sea de ESET (de terceros).

Sistema operativo	Tipos de archivos de instalación compatibles	Compatibilidad con parámetros de instalación
Windows	*.msi*	La tarea Instalación del software siempre ejecuta la instalación en segundo plano de los paquetes *.msi*. No puede especificar parámetros msiexec. Solo puede especificar parámetros utilizados por el paquete de instalación (únicos para cada paquete de instalación de software).
Linux	*.deb*, *.rpm*, *.sh*	Solo puede utilizar parámetros con archivos *.sh* (*.deb* y *.rpm* no son compatibles con parámetros).
macOS	*.pkg*, *.dmg* (con 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.

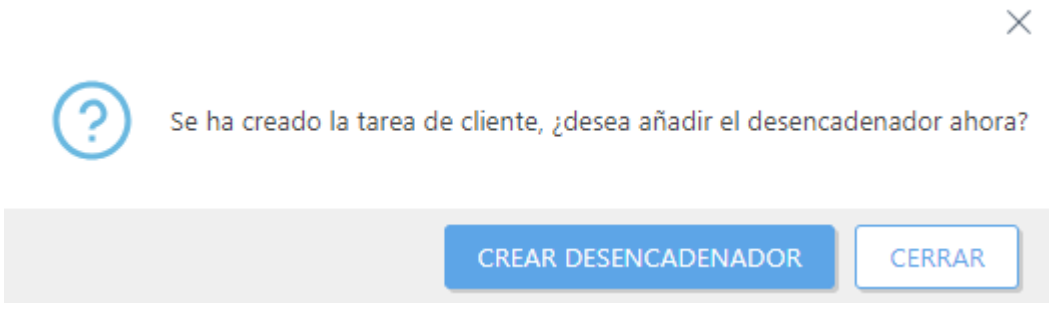
Quiere instalar software en Linux con el archivo *install_script.sh* que tiene dos parámetros: `-a` es el primer parámetro y `-b` el segundo.
Instalación en terminal (como usuario raíz en la carpeta en la que está *install_script.sh*):
`./install_script.sh -a parameter_1 -b parameter_2`
Instalación con la tarea Instalación del software:
• Introduzca la ruta de acceso del archivo en **Instalar por URL de paquete directo**, por ejemplo: *file:///home/user/Desktop/install_script.sh*
• Escriba los **parámetros de instalación**: `-a parameter_1 -b parameter_2`.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

• Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Lista de problemas cuando la instalación falla

• Paquete de instalación no encontrado.

• Se necesita la versión más reciente del servicio Windows Installer.

- Ya hay instalada otra versión o un producto en conflicto.
- Ya hay otra instalación en curso. Finalice esa instalación antes de proceder con esta.
- La instalación o la desinstalación ha finalizado correctamente, pero es necesario reiniciar el ordenador.
- Error en la tarea: se produjo un error. Se ha producido un error, debe consultar el registro de seguimiento del agente y anotar el código de devolución del instalador.

Software de Safetica

Qué es Safetica

Safetica es una empresa externa de software y miembro de ESET Technology Alliance. Safetica ofrece una solución de seguridad de TI para prevenir la pérdida de datos y es complementaria de las soluciones de seguridad de ESET. Entre las principales características del software de Safetica se incluyen las siguientes:

- Prevención de la pérdida de datos: supervisión de todos los discos duros, unidades USB, transferencias de archivos en red, mensajes de correo electrónico e impresoras, así como del acceso a archivos de las aplicaciones
- Bloqueo de actividad e informes: para operaciones de archivos, sitios web, mensajes de correo electrónico, mensajería instantánea, uso de aplicaciones y palabras clave buscadas

Cómo funciona Safetica

Safetica implementa un agente (cliente de punto de acceso de Safetica) en los puntos de acceso que usted desee y mantiene una conexión regula con ellos a través del servidor (servicio de administración de Safetica). Este servidor crea una base de datos de la actividad de la estación 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

ESET Management Agent detecta y comunica el software de Safetica como software de ESET en **Detalles del ordenador** > Aplicaciones instaladas. ESET PROTECT Web Console actualizará el agente de Safetica si hay una nueva versión disponible.

Implementación de Safetica Agent

Puede implementar el agente de Safetica directamente a través de ESET PROTECT Web Console desde el repositorio de software de ESET con la tarea Instalación de software, para lo cual deberá escribir `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 **Safetica Management Service**).

También puede instalar el agente de Safetica con la Tarea del cliente - Ejecutar comando.

Uso de 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 y en modo "silencioso": `msiexec /i safetica_agent.msi STSERVER=Server_name /silent`
Para realizar la instalación mencionada anteriormente el paquete .msi debe estar presente en el dispositivo.
Para ejecutar la instalación si el paquete *.msi* se encuentra en una ubicación compartida, especifique la ubicación en el comando de la siguiente forma: `msiexec /i Z:\sharedLocation\safetica_agent.msi STSERVER=Server_name`

Actualizar agente Safetica

Para actualizar el agente de Safetica en un ordenador administrado, vaya a **Detalles del ordenador** > Aplicaciones instaladas, seleccione el **agente de Safetica** y haga clic en **Actualizar productos de ESET**.

Desinstalar Safetica Agent

Para desinstalar el agente de Safetica de un ordenador administrado, vaya a **Detalles del ordenador** > Aplicaciones instaladas, seleccione el **agente de Safetica** y haga clic en **Desinstalar**.

Desinstalación del software

La tarea **Desinstalación del software** se utiliza para desinstalar un producto de ESET de los ordenadores cliente cuando ya no se desea o no es necesario.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**.
Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

Configuración de desinstalación del 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 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 de Agent. En esta lista aparecerán todos los paquetes que se pueden desinstalar de los clientes seleccionados.

Cuando desinstale el agente de ESET Management del ordenador cliente, ESET PROTECT On-Prem dejará de administrar el dispositivo:
• El producto de seguridad de ESET puede conservar algunos ajustes después de la desinstalación del agente de ESET Management.
• Si ESET Management Agent está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar el producto (con cambios). Se recomienda restablecer algunos ajustes que no se deseen mantener (por ejemplo, la protección con contraseña) a los valores predeterminados mediante una política antes de quitar el dispositivo de la administración.
• Asimismo se abandonarán todas las tareas que se estén ejecutando en el agente. Es posible que los estados de ejecución **En ejecución**, **Finalizado** o **Con error** de esta tarea no se muestren con precisión en ESET PROTECT Web Console en función de la replicación de los datos.
• Tras la desinstalación del agente puede gestionar el producto de seguridad mediante eShell o la EGUI integrada.

• **Versión del paquete**: puede quitar una versión concreta (a veces una versión concreta puede causar problemas) del paquete, o **desinstalar todas las versiones de un paquete**.

• **Parámetros de desinstalación**: puede especificar parámetros de desinstalación.

• Marque la casilla de verificación situada junto a **Reiniciar automáticamente cuando sea necesario** para forzar un reinicio automático del ordenador cliente tras la instalación. También puede dejar esta opción sin seleccionar y reiniciar manualmente el ordenador cliente. Puede configurar el comportamiento de reinicio o apagado de los ordenadores administrados. El ordenador debe ejecutar ESET Management Agent 9.1 o versiones más recientes y un producto de seguridad de ESET compatible con este ajuste.

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 de Agent.

Si desea acceder a una lista del software antivirus compatible, consulte el artículo de nuestra base de conocimiento. Este proceso de eliminación es distinto de la desinstalación desde **Agregar o quitar programas**. Emplea métodos alternativos para quitar software antivirus de terceros de manera exhaustiva, incluidas las entradas del registro residuales y otros restos.

Siga las instrucciones detalladas del artículo Quitar software antivirus de terceros de ordenadores cliente con ESET PROTECT On-Prem para enviar una tarea de eliminación de software antivirus de terceros de ordenadores cliente.

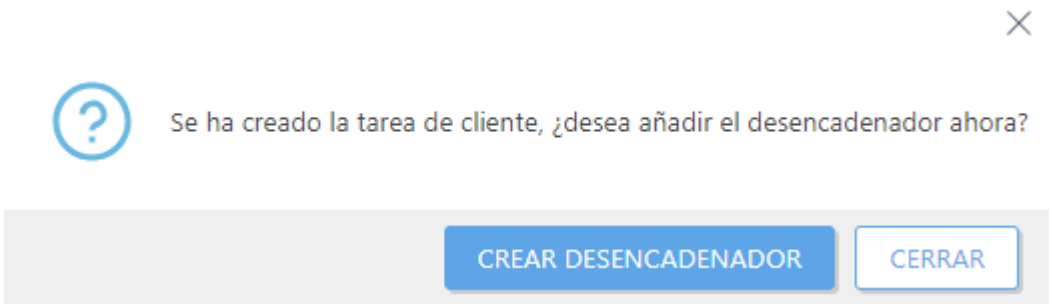
Si desea permitir la desinstalación de aplicaciones protegidas mediante contraseña, consulte el artículo de nuestra base de conocimiento.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

La tarea de desinstalación de productos de seguridad de ESET puede dar un error relacionado con la contraseña, por ejemplo: **Producto: ESET Endpoint Security -- Error 5004. Introduzca una contraseña válida para continuar con la desinstalación**. Esto se debe a que está activada la configuración de protección por contraseña en el producto de seguridad de ESET. Aplique una política a los ordenadores cliente para quitar la protección por contraseña. A continuación, puede desinstalar el producto de seguridad de ESET con la tarea Desinstalación del software.

Detener administración (desinstalar ESET Management Agent)

Esta tarea desinstalará ESET Management Agent de los dispositivos de destino seleccionados. Si se selecciona un ordenador de sobremesa, la tarea eliminará ESET Management Agent. Si se selecciona un dispositivo móvil, la tarea cancelará la inscripción de MDM del dispositivo.

Cuando desinstale el agente de ESET Management del ordenador cliente, ESET PROTECT On-Prem dejará de administrar el dispositivo:
- El producto de seguridad de ESET puede conservar algunos ajustes después de la desinstalación del agente de ESET Management.
- Si ESET Management Agent está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar el producto (con cambios). Se recomienda restablecer algunos ajustes que no se deseen mantener (por ejemplo, la protección con contraseña) a los valores predeterminados mediante una política antes de quitar el dispositivo de la administración.
- Asimismo se abandonarán todas las tareas que se estén ejecutando en el agente. Es posible que los estados de ejecución **En ejecución**, **Finalizado** o **Con error** de esta tarea no se muestren con precisión en ESET PROTECT Web Console en función de la replicación de los datos.
- Tras la desinstalación del agente puede gestionar el producto de seguridad mediante eShell o la EGUI integrada.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

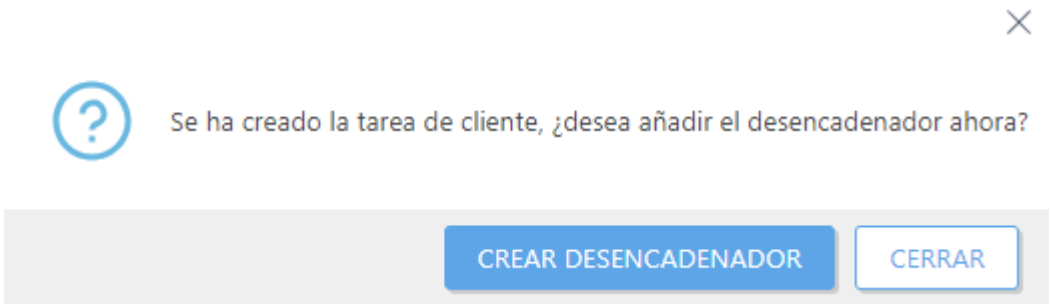
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

no hay **configuración** disponible para esta tarea.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Solicitud de registro de SysInspector (solo Windows)

La tarea **Solicitud de registro de SysInspector** se utiliza para solicitar el registro de SysInspector a un producto de seguridad del cliente.

ESET SysInspector solo se ejecuta en ordenadores Windows.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**. También puede ejecutar esta tarea desde **Ordenadores** > haga clic en un ordenador > **Detalles** > **Registros** > **Registro de la solicitud (solo Windows)**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

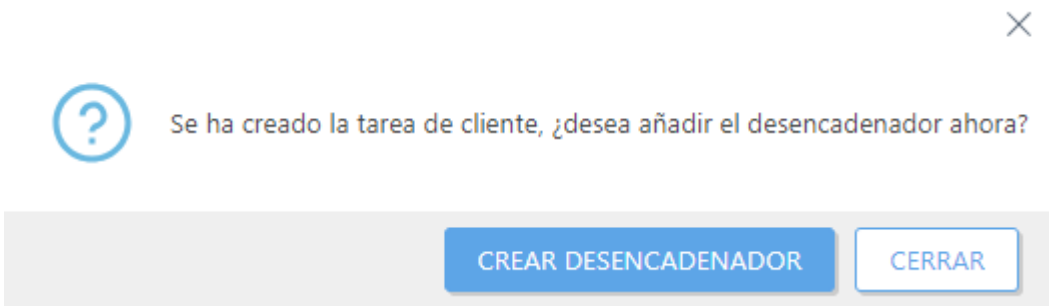
Configuración

- **Almacenar registro en el cliente:** seleccione esta opción si desea almacenar el registro de SysInspector tanto en el cliente como en ESET PROTECT Server. Por ejemplo, cuando un cliente tiene instalado ESET Endpoint Security, el registro generalmente se almacena en *C:\Program Data\ESET\ESET Security\SysInspector*.

Resumen

Revise el resumen de las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Una vez completada la tarea, se muestra una nueva entrada en la lista de registros de ESET SysInspector. Haga clic en uno de los registros de la lista para explorarlo.

Cargar archivo en cuarentena

La tarea **Cargar archivo en cuarentena** se utiliza para administrar los archivos en cuarentena en los clientes. Puede cargar el archivo en cuarentena desde la cuarentena a una ubicación específica para realizar una investigación avanzada.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nuevo** > **Tareas del cliente**.

- Haga clic en **Tareas** > seleccione el tipo de tarea deseado y haga clic en **Nueva tarea** > **Tarea del cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

Configuración

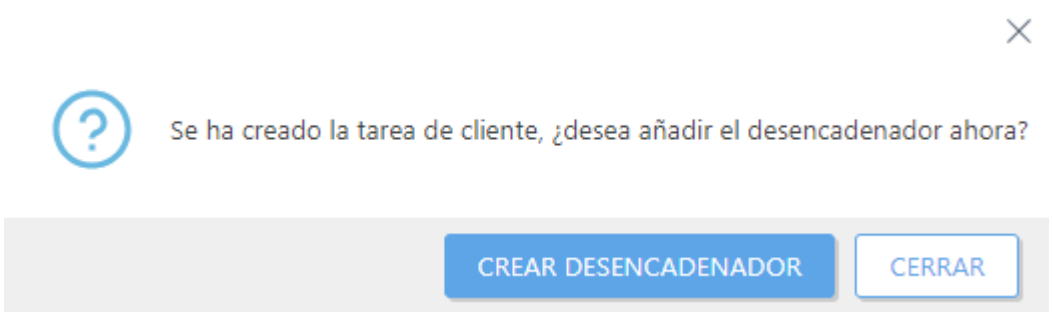
- **Objeto en cuarentena**: seleccione un objeto específico en la cuarentena.
- **Contraseña del objeto**: escriba una contraseña para cifrar el objeto por motivos de seguridad. Tenga en cuenta que la contraseña se mostrará en el informe correspondiente.
- **Cargar ruta**: escriba una ruta a la ubicación en la que desea cargar el objeto. Utilice la siguiente sintaxis: *smb://server/share*
- **Cargar nombre de usuario/contraseña**: en caso de que la ubicación requiera autenticación (recurso compartido de red, etc.), introduzca 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 las opciones configuradas y haga clic en **Finalizar**. La tarea del cliente se crea y se abre una ventana:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (ordenadores o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia de la tarea del cliente y seleccione **Ejecutar en** en el menú desplegable.



Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Una vez cargado el archivo en cuarentena en la ubicación de **Ruta de carga** seleccionada:

- El archivo se almacena en un archivo *.zip* comprimido protegido por contraseña. La contraseña es el nombre del archivo *.zip* (hash del archivo en cuarentena).
- El archivo en cuarentena no tiene extensión de archivo. Para restaurar el archivo, agréguele la extensión del archivo original.

Tareas del servidor

Las tareas del servidor las ejecuta ESET PROTECT Server de forma independiente o en otros dispositivos. las tareas del servidor no se pueden asignar a cualquier cliente o grupo de clientes. Cada tarea del servidor puede tener un desencadenador configurado. Si la tarea debe ejecutarse con distintos eventos, tiene que haber una tarea del servidor por cada desencadenador.

Tareas del servidor

- Implementación de agente
- Eliminar ordenadores que no se conecten
- Generar informe
- Cambiar nombre de los ordenadores
- Sincronización de grupos estáticos
- Sincronización de usuarios

Tareas del servidor y permisos

Tanto la tarea como el desencadenador necesitan un usuario ejecutante. Este es el usuario que modifica la tarea (y el desencadenador). Este usuario debe tener permisos suficientes para la acción seleccionada. Durante la ejecución, la tarea siempre obtiene el usuario ejecutante del desencadenador. Si la tarea se ejecuta utilizando el ajuste **Ejecutar tarea inmediatamente después de finalizar**, el usuario ejecutante será el usuario que ha iniciado sesión en ESET PROTECT Web Console. Un usuario tiene permisos (**Lectura**, **Uso**, **Escritura**) para la instancia de **tarea del servidor** seleccionada si tiene esos permisos seleccionados en su conjunto de permisos (**Más** > **Conjuntos de permisos**) y tiene configurados estos permisos para el grupo estático en el que se encuentra la tarea del servidor. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

John, cuyo grupo principal es *Grupo de John*, quiere quitar la *Tarea del servidor 1:* **Generar informe**. La tarea la creó *Larry*, por lo que la tarea está en el grupo principal de Larry, *Grupo de Larry*. Deben cumplirse las siguientes condiciones para que *John* pueda quitar la tarea:

- *John* debe tener asignado un conjunto de permisos en el que se incluyan permisos de **escritura** sobre **Tareas y desencadenadores de servidor**: **Generar informes**.
- El conjunto de permisos debe contener *Grupo de Larry* en **Grupos estáticos**.

Permisos necesarios para determinadas acciones relacionadas con tareas del servidor

- Para crear una nueva tarea del servidor, el usuario necesita permiso de **escritura** en el tipo de tarea seleccionado y los correspondientes derechos de acceso a los objetos a los que se haga referencia (ordenadores, licencias, grupos).

- Para modificar una tarea del servidor, el usuario necesita permiso de **escritura** en la instancia de tarea del servidor seleccionada y los correspondientes derechos de acceso a los objetos a los que se haga referencia (ordenadores, licencias, grupos).

- Para quitar una tarea del servidor, el usuario necesita permiso de **escritura** en la instancia de tarea del servidor seleccionada.

- Para ejecutar una tarea del servidor, el usuario necesita permiso de **uso** en 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** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

2. En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.

- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

3. Configure los ajustes de la tarea en la sección **Configuración**.

4. Configure el desencadenador en la sección **Desencadenador** si está disponible.

5. Compruebe todos los ajustes de esta tarea en la sección **Resumen** y, a continuación, haga clic en **Finalizar**.

> Se recomienda a los usuarios que utilicen con regularidad tareas del servidor que creen sus propias tareas en vez de compartirlas con otros usuarios. Cada vez que se ejecuta la tarea, utiliza los permisos del usuario ejecutante. Esto puede confundir a algunos usuarios.

Implementación de agente

La tarea del servidor Implementación de agente lleva a cabo una implementación remota de ESET Management Agent.

> La tarea de implementación de agente ejecuta la instalación de ESET Management Agent en los ordenadores de destino uno por uno (de forma secuencial). Por tanto, cuando ejecuta la tarea Implementación de agente en muchos ordenadores cliente, el proceso podría tardar mucho tiempo en finalizar. Le recomendamos usar ESET Remote Deployment Tool. Ejecuta la instalación de ESET Management Agent en todos los ordenadores de destino a la vez (en paralelo) y ahorra ancho de banda de la red al usar archivos del instalador almacenados de forma local, sin tener que acceder al repositorio en línea.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.
- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración de implementación del agente

Destinos: haga clic en esta opción 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 usan como direcciones del cliente durante la implementación; si no son correctos, la implementación falla. Use el atributo `dNSHostName` como **Atributo Nombre de host del ordenador** durante la sincronización a efectos de implementación del agente.

Nombre de host del servidor (opcional): puede introducir un nombre de host del servidor, si es diferente en el lado del cliente y en el del servidor.

Credenciales del ordenador de destino

Nombre de usuario/contraseña: nombre de usuario y contraseña del usuario con derechos suficientes para realizar una instalación remota del agente.

Configuración ce certificados

Certificado de igual:

- **certificado de ESET PROTECT**: el certificado de igual para la instalación del agente y la autoridad certificadora de ESET PROTECT se seleccionan automáticamente. 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 **Personalizar certificado** > **cargue** el certificado .pfx y selecciónelo al instalar el agente. Si desea obtener más información, consulte Certificados.

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

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

ESET PROTECT Server puede seleccionar el paquete de instalación del agente apropiado para cada sistema operativo de forma automática:

- Linux: seleccione un usuario con permiso para utilizar el comando `sudo` o el usuario `root`. Si se utiliza el usuario `root`, el servicio `ssh` le debe permitir 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. Utilice el siguiente comando (cambie la dirección IP por la dirección IP de su ESET PROTECT Server) para añadir una excepción al cortafuegos 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 Resolución de problemas de implementación de agente.

Otros ajustes

Marque la casilla de verificación **Participar en el programa para la mejora del producto** para enviar informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto).

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea**

del servidor puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Resolución de problemas

Si la tarea de implementación de agente falla, consulte Resolución de problemas de implementación de agente.

> ⚠ Para volver a implementar el agente ESET Management, no quite nunca el agente instalado. Ejecute la tarea de implementación de agente sobre el agente instalado. Si quita el agente, el nuevo agente puede empezar a ejecutar tareas anteriores después de la nueva implementación.

Eliminar ordenadores que no se conecten

La tarea **Eliminar ordenadores que no se conecten** le permite eliminar ordenadores de acuerdo con criterios especificados. Por ejemplo, si el ESET Management Agent de un ordenador cliente no se ha conectado durante 30 días, puede eliminarse de ESET PROTECT Web Console.

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

- Amarillo (error): hace entre 2 y 14 días que el ordenador no se conecta.
- Rojo (advertencia): el ordenador no se conecta desde hace más de 14 días.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.

- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Nombre del grupo: seleccione un grupo estático o cree un nuevo grupo estático para los ordenadores con nombres cambiados.

Número de días que el ordenador lleva sin conectarse: escriba el número de días después de los cuales se eliminarán ordenadores.

Desactivar licencia: marque esta casilla de verificación para desactivar las licencias de los ordenadores que ha quitado.

Quitar ordenadores no gestionados: marque esta casilla de verificación para quitar también los ordenadores no administrados.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Generar informe

La tarea **Generar informe** se utiliza para generar informes a partir de plantillas de informes anteriormente creadas o predefinidas.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo

de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.
- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Plantillas de informe: haga clic en Agregar plantilla de informe para elegir una plantilla de informe en la lista. El usuario que cree la tarea solo podrá ver y elegir plantillas de informe disponibles en su grupo. Puede elegir varias plantillas de informe para un informe.

Los usuarios de MSP pueden filtrar el informe mediante la selección del cliente.

Seleccione Enviar correo electrónico o Guardar en archivo para obtener el informe generado.

Entrega del informe

Enviar correo electrónico

Para enviar y recibir mensajes de correo debe configurar los ajustes de SMTP en **Más** > Configuración > **Configuración avanzada**.

- **Enviar a**: introduzca las direcciones de correo de los destinatarios de los correos electrónicos de informe. Separe las direcciones con una coma (,). También es posible agregar los campos CC y CCO, que funcionan exactamente igual que en los clientes de correo.
- ESET PROTECT On-Prem rellena el asunto y el cuerpo del mensaje de correo electrónico en función de la plantilla de informe seleccionada. Puede marcar la casilla de verificación situada debajo de **Personalizar mensaje** para personalizar el **Asunto** y el **Mensaje**:
  - **Asunto**: asunto del mensaje del informe. Escriba un asunto distintivo, para que los mensajes entrantes puedan clasificarse. Este ajuste es opcional, pero le recomendamos que no lo deje en blanco.
  - **Mensaje**: defina el cuerpo del mensaje del informe.

• **Enviar correo si el informe está en blanco**: utilice esta opción si desea que se envíe el informe aunque no contenga datos.

Haga clic en **Mostrar opciones de impresión** para mostrar las opciones siguientes:

• **Formato de salida**: seleccione el formato de archivo adecuado. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa ; (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe PDF para ver los valores de texto.

Si selecciona resultados en CSV en los valores de hora y fecha en el informe, se guardarán en formato UTC. Si selecciona PDF, el informe utilizará la hora local del servidor.

• **Lenguaje de salida**: seleccione el idioma para el mensaje. El idioma predeterminado se basa en el idioma seleccionado para ESET PROTECT Web Console.

• **Tamaño de página/Resolución/Orientación del papel/Formato de color/Unidades del margen/Márgenes**: seleccione las opciones adecuadas en función de sus preferencias de impresión. Estas opciones son relevantes si quiere imprimir el informe y solo se aplican al formato PDF, no al formato CSV.

Guardar en archivo

• **Ruta del archivo relativa**: el informe se generará en un directorio específico, por ejemplo:

*o*En Windows, los informes suelen colocarse en*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports*

*o*En Linux, los informes suelen colocarse en/var/opt/eset/RemoteAdministrator/Server/GeneratedReports/

En Windows, algunos caracteres especiales (: ? \) no se interpretarán correctamente en el nombre de archivo almacenado.

• **Guardar archivo si el informe está en blanco**: utilice esta opción si desea que se guarde el informe aunque no contenga datos.

Haga clic en **Mostrar opciones de impresión** para mostrar las opciones siguientes:

• **Formato de salida**: seleccione el formato de archivo adecuado. Puede elegir entre *.pdf* o *.csv*. CSV solo es adecuado para datos en tabla y usa ; (el punto y coma) como delimitador. Si descarga un informe CSV y ve números en una columna en la que espera ver texto, le recomendamos descargar un informe PDF para ver los valores de texto.

Si selecciona resultados en CSV en los valores de hora y fecha en el informe, se guardarán en formato UTC. Si selecciona PDF, el informe utilizará la hora local del servidor.

• **Lenguaje de salida**: seleccione el idioma para el mensaje. El idioma predeterminado se basa en el idioma seleccionado para ESET PROTECT Web Console.

- **Tamaño de página/Resolución/Orientación del papel/Formato de color/Unidades del margen/Márgenes**: seleccione las opciones adecuadas en función de sus preferencias de impresión. Estas opciones son relevantes si quiere imprimir el informe y solo se aplican al formato PDF, no al formato CSV.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Cambiar nombre de los ordenadores

Puede utilizar la tarea **Cambiar nombre de los ordenadores** para cambiar el nombre de los ordenadores a formato FQDN en ESET PROTECT On-Prem. Puede utilizar la tarea del servidor existente que se ofrece de forma predeterminada con la instalación de ESET PROTECT On-Prem. Si el nombre de un dispositivo cliente es distinto del que se indica en los detalles del dispositivo, la ejecución de esta tarea puede restaurar el nombre correcto.

Esta tarea cambia automáticamente cada hora el nombre de los ordenadores sincronizados que se encuentran en el grupo **Perdidos y encontrados**.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.

- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Nombre del grupo: seleccione un grupo estático o dinámico o cree un nuevo grupo estático o dinámico para los ordenadores cuyo nombre se ha cambiado.

Cambio de nombre basado en:

- **Nombre del ordenador**: cada ordenador está identificado en la red local por su nombre de ordenador exclusivo
- **FQDN (Nombre de dominio completamente cualificado) del ordenador**: comienza con el nombre de host y continúa con los nombres de dominio hasta el nombre de dominio de nivel superior.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Sincronización de grupos estáticos

La tarea **Sincronización de grupos estáticos** buscará ordenadores en su red (Active Directory, Open Directory, LDAP, red local o VMware) y los pondrá en un grupo estático. Si selecciona **Sincronizar con Active Directory** durante la Instalación del servidor, los ordenadores que se encuentren se agregarán al grupo **Todo**. Para sincronizar ordenadores Linux unidos al dominio de Windows, siga estas instrucciones detalladas.

ESET PROTECT On-Prem es compatible con la firma segura LDAP.

Existen 3 **modos de sincronización**:

- Active Directory/Open Directory/LDAP: escriba la información de conexión básica del servidor.

Puede ejecutar la tarea del servidor Implementación de agente para implementar el agente de ESET Management en los ordenadores sincronizados desde Active Directory.

• Red de MS Windows: introduzca el **grupo de trabajo** que se utilizará y las correspondientes credenciales del usuario.

Puede que el modo de sincronización de la **red de MS Windows** no funcione porque faltan requisitos (SMBv1) necesarios para su funcionamiento correcto. ESET eliminará este modo de sincronización en el futuro.

• VMware: escriba la información de conexión del servidor de VMware vCenter.

Modo de sincronización - Active Directory/Open Directory/LDAP

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

• **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.

• **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Configuración común

Haga clic en **Seleccionar** en **Nombre del grupo estático**: de forma predeterminada, se utilizará el grupo principal

del usuario ejecutante para los ordenadores sincronizados. Alternativamente, puede crear un **nuevo grupo estático**.

- **Objeto que sincronizar:** puede ser **Ordenadores y grupos** o **Solo ordenadores**.
- **Gestión de la colisión de creación de ordenadores**: si la sincronización agrega ordenadores que ya son miembros del grupo estático, puede seleccionar el método de resolución de los conflictos:
  - **Omitir** (no se agregarán los ordenadores duplicados)
  - **Mover** (los nuevos ordenadores se moverán a un subgrupo)
  - **Duplicar** (se crea un nuevo ordenador con el nombre modificado)
- **Gestión de la extinción del ordenador**: si un ordenador ya no existe, puede **Quitar** u **Omitir** este ordenador.
- **Gestión de la extinción del ordenador**: si un grupo ya no existe, puede **Quitar** u **Omitir** este grupo.

> Si en **Gestión de la extinción del grupo** selecciona **Omitir** y elimina un grupo (unidad organizativa) de Active Directory, los ordenadores que pertenecieran al grupo en ESET PROTECT On-Prem no se eliminarán, ni siquiera si en **Gestión de la extinción del ordenador** selecciona **Quitar**.

- **Modo de sincronización** - **Active Directory/Open Directory/LDAP**

Lea el artículo de la base de conocimiento sobre la administración de ordenadores con la sincronización con Active Directory en ESET PROTECT On-Prem.

Configuración de conexión del servidor

- **Servidor** - Escriba el nombre de servidor o la dirección IP de su controlador de dominio.
- **Iniciar sesión** - Escriba el nombre de usuario de su controlador de dominio con el siguiente formato:
  - `DOMAIN\username` (ESET PROTECT Server en ejecución en Windows)
  - `username@FULL.DOMAIN.NAME` o `username` (ESET PROTECT Server en ejecución en Linux).

> Escriba el dominio en mayúsculas, ya que este formato es necesario para autenticar las consultas correctamente en un servidor de Active Directory.

- **Contraseña**: escriba la contraseña que se usa para iniciar sesión en su controlador de dominio.

En Windows, ESET PROTECT utiliza el protocolo cifrado LDAPS (LDAP a través de SSL) de forma predeterminada para todas las conexiones de Active Directory (AD). También puede configurar LDAPS en el dispositivo virtual de ESET PROTECT.
Para establecer una conexión con Active Directory a través de LDAPS, realice los siguientes ajustes:
1. El controlador de dominio debe tener instalado un certificado de máquina. Para emitir un certificado para su controlador de dominio, siga los pasos indicados a continuación:
a)Abra el **Administrador de servidores**, haga clic en **Administrar** > **Agregar roles y características** e instale la autoridad (**Servicios de certificados de Active Directory** > **Autoridad certificadora**). Se creará una nueva autoridad certificadora en **Autoridades certificadoras de confianza**.
b)Diríjase a **Inicio** > escriba `certmgr.msc` y pulse **Entrar** para ejecutar el complemento **Certificados** Microsoft Management Console > **Certificados: ordenador local** > **Personal** > haga clic con el botón derecho del ratón en el panel vacío > **Todas las tareas** > **Solicitar nuevo certificado** > rol **Inscribir controlador de dominio** role.
c)Compruebe que el certificado emitido contenga el FQDN del controlador de dominio.
d)En el servidor de ESET PROTECT, importe la autoridad certificadora que generó para el almacén de certificados (con la herramienta `certmgr.msc`) en la carpeta de autoridades certificadoras de confianza.
2. Cuando proporcione la configuración de conexión al servidor de Active Directory, escriba el FQDN del controlador de dominio (como se indica en el certificado del controlador de dominio) en el campo **Servidor** o en el campo **Host**. La dirección IP ya no es suficiente para LDAPS.

Si desea activar el uso del protocolo LDAP, marque la casilla de verificación **Usar LDAP en lugar de Active Directory** e introduzca los atributos específicos que se ajusten a su servidor. También puede seleccionar **Preestablecidos** haciendo clic en **Seleccionar** y los atributos se completarán automáticamente:

- **Active Directory**
- Open Directory para el servidor de macOS (nombres de host del ordenador)
- Open Directory para el servidor de macOS (direcciones IP del ordenador)
- **OpenLDAP con registros informáticos Samba**: configuración de los parámetros de Nombre de DNS en Active Directory.

Cuando selecciona **Usar LDAP en lugar de Active Directory** y el preajuste de **Active Directory,** puede rellenar los detalles del ordenador con atributos de su estructura de Active Directory. Solo pueden usarse atributos del tipo `DirectoryString`. Puede utilizar una herramienta (por ejemplo *ADExplorer*) para inspeccionar los atributos de su controlador de dominio. Consulte los campos correspondientes en la siguiente tabla:

Campos de detalles del ordenador	Campos de la tarea de sincronización
Nombre	**Atributo Nombre de host del ordenador**
Descripción	**Atributo Descripción del ordenador**

Configuración de sincronización

- **Nombre distinguido**: ruta (nombre distinguido) al nodo del árbol de Active Directory. Si se deja esta opción en blanco, se sincroniza el árbol entero de AD. Haga clic en **Examinar** junto a **Nombre distinguido**. Se mostrará su árbol de Active Directory. Seleccione la entrada superior para sincronizar todos los grupos de ESET PROTECT On-Prem o seleccione solo los grupos que quiera agregar. Solo se sincronizan los ordenadores y las unidades organizativas. Haga clic en **Aceptar** cuando haya terminado.

Determinar el nombre distinguido

1.Abra la aplicación **Usuarios y ordenadores de Active Directory**.
2.Haga clic en **Ver** y seleccione **Funciones avanzadas**.
3.Haga clic con el botón derecho en el dominio > haga clic en **Propiedades** > seleccione la ficha **Editor de atributos**.
4.Localice **distinguishedName** la línea. Debe tener el mismo aspecto que el de este ejemplo: `DC=ncop,DC=local`.

- **Nombres distinguidos excluidos:**: puede elegir excluir (ignorar) nodos específicos del árbol de Active Directory.

- **Ignorar ordenadores desactivados (solo en Active Directory)**: puede ignorar los ordenadores desactivados en Active Directory (la tarea omitirá estos ordenadores).

Si se muestra el error `Server not found in Kerberos database` al hacer clic en **Examinar**, utilice el nombre completo de AD del servidor en lugar de la dirección IP.

Sincronización desde servidor Linux

ESET PROTECT Server en ejecución en Linux realiza la sincronización de una forma distinta a los equipos Windows. El proceso es el siguiente:
1. Se deben especificar el nombre de host y las credenciales del controlador de dominio.
2. El servidor verifica las credenciales y las convierte en un ticket de Kerberos.
3. El servidor detecta el nombre distinguido del dominio, en caso de no estar presente.
4. A) Si la opción **Usar LDAP en lugar de Active Directory** no está marcada:
Varias llamadas a `ldapsearch` enumeran el árbol. Un ejemplo simplificado para el proceso de obtener registros de ordenador:

```
kinit <username>
```

(Es 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 la opción **Usar LDAP en lugar de Active Directory** está marcada:
se invoca el mismo proceso que en la opción 4A, pero el usuario puede configurar los parámetros.
5. Kerberos utiliza un mecanismo de enlace para autenticar al usuario y generar un ticket que posteriormente se puede usar con otros servicios para la autorización sin enviar una contraseña en texto no cifrado (a diferencia de la opción **Usar autenticación sencilla**).
6. A continuación, la utilidad `ldapsearch` usa GSSAPI para autenticarse en Active Directory con el ticket Kerberos obtenido.
7. Los resultados de la búsqueda se devuelven mediante un canal no cifrado.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la

aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Puede ejecutar la tarea del servidor Implementación de agente para implementar el agente de ESET Management en los ordenadores sincronizados desde Active Directory.

Modo de sincronización: red de MS Windows

Puede que el modo de sincronización de la **red de MS Windows** no funcione porque faltan requisitos (SMBv1) necesarios para su funcionamiento correcto. ESET eliminará este modo de sincronización en el futuro.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.
- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Configuración común

Haga clic en **Seleccionar** en **Nombre del grupo estático**: de forma predeterminada, se utilizará el grupo principal del usuario ejecutante para los ordenadores sincronizados. Alternativamente, puede crear un **nuevo grupo estático**.

- **Objeto que sincronizar:** puede ser **Ordenadores y grupos** o **Solo ordenadores**.

• **Gestión de la colisión de creación de ordenadores**: si la sincronización agrega ordenadores que ya son miembros del grupo estático, puede seleccionar el método de resolución de los conflictos:

- **Omitir** (no se agregarán los ordenadores duplicados)
- **Mover** (los nuevos ordenadores se moverán a un subgrupo)
- **Duplicar** (se crea un nuevo ordenador con el nombre modificado)

• **Gestión de la extinción del ordenador**: si un ordenador ya no existe, puede **Quitar** u **Omitir** este ordenador.

• **Gestión de la extinción del ordenador**: si un grupo ya no existe, puede **Quitar** u **Omitir** este grupo.

• **Modo de sincronización** - **red de MS Windows**

En la secciónConfiguración de la sincronización de la red de Microsoft Windows, escriba la siguiente información:

• **Grupo de trabajo**: escriba el dominio o grupo de trabajo que contiene los ordenadores a sincronizar. Si no especifica un grupo de trabajo, se sincronizarán todos los ordenadores visibles.

• **Inicio de sesión**: escriba las credenciales de inicio de sesión utilizadas para la sincronización en su red Windows.

• **Contraseña**: escriba la contraseña utilizada para iniciar sesión en su red Windows.

ESET PROTECT Server funciona con privilegios de **Servicio de red** que podrían no ser suficientes para leer todos los ordenadores cercanos. Si no hay credenciales de usuario presentes, el servidor lee todos los ordenadores cercanos de las carpetas de red disponibles en Windows que rellena automáticamente el sistema operativo. Si hay credenciales presentes, el servidor las usa para la sincronización directa.

Puede que el modo de sincronización de la **red de MS Windows** no funcione porque faltan requisitos (SMBv1) necesarios para su funcionamiento correcto. ESET eliminará este modo de sincronización en el futuro.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

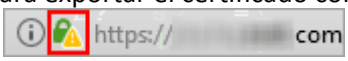
Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Modo de sincronización - VMware

Pueden sincronizarse máquinas virtuales que se ejecuten en VMware vCenter Server.

> Para ejecutar esta tarea correctamente debe importar la autoridad certificadora de vCenter en su ESET PROTECT Server. Puede exportarla desde el navegador web.
> Por ejemplo, para exportar el certificado con Firefox, haga clic en el icono de la conexión segura en la barra de direcciones 
>
> y, a continuación, haga clic en **Mostrar detalles de la conexión** > **Más información** > **Ver certificado** > **Detalles** > **Exportar** > **Guardar**.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.
- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Configuración común

Haga clic en **Seleccionar** en **Nombre del grupo estático**: de forma predeterminada, se utilizará el grupo principal del usuario ejecutante para los ordenadores sincronizados. Alternativamente, puede crear un **nuevo grupo estático**.

- **Objeto que sincronizar:** puede ser **Ordenadores y grupos** o **Solo ordenadores**.
- **Gestión de la colisión de creación de ordenadores**: si la sincronización agrega ordenadores que ya son

miembros del grupo estático, puede seleccionar el método de resolución de los conflictos:

- **Omitir** (no se agregarán los ordenadores duplicados)
- **Mover** (los nuevos ordenadores se moverán a un subgrupo)
- **Duplicar** (se crea un nuevo ordenador con el nombre modificado)

• **Gestión de la extinción del ordenador**: si un ordenador ya no existe, puede **Quitar** u **Omitir** este ordenador.

• **Gestión de la extinción del ordenador**: si un grupo ya no existe, puede **Quitar** u **Omitir** este grupo.

• **Modo de sincronización** - **VMWare**

Configuración de conexión del servidor

• **Servidor**: escriba el DNS o la dirección IP del servidor de VMware vCenter. La dirección debe ser exactamente la misma que el valor **CN** de la autoridad certificadora de vCenter importada. Puede consultar este valor en la columna **Asunto** de la ventana **Más** > **Autoridades certificadoras**.

• **Iniciar sesión**: escriba las credenciales de inicio de sesión del servidor de VMware vCenter.

• **Contraseña**: escriba la contraseña utilizada para iniciar sesión en su servidor de VMware vCenter.

Configuración de sincronización

• **Vista de la estructura**: seleccione el tipo de vista de la estructura, **Carpetas** o **Grupo de recursos**.

• **Ruta de la estructura**: haga clic en **Examinar y vaya a la** carpeta que desee sincronizar. Si se deja el campo vacío, se sincronizará la estructura completa.

• **Vista del ordenador**: seleccione si se muestran los ordenadores por **Nombre**, **Nombre del host** o **Dirección IP después de la sincronización**.

Si se muestra el error `Server not found in Kerberos database` al hacer clic en **Examinar**, utilice el nombre completo de AD del servidor en lugar de la dirección IP.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Sincronización de grupos estáticos: ordenadores Linux

Un ordenador Linux unido a un dominio Windows no muestra ningún texto en Usuarios y Equipos de Active Directory (ADUC) de Propiedades del ordenador, por lo que es necesario introducir el texto manualmente.

Compruebe los Requisitos previos del servidor y los siguientes requisitos previos:

- Los ordenadores Linux se encuentran en Active Directory.
- El controlador de dominio tiene un servidor DNS instalado.
- Editor ADSI está instalado.

1. Abra una ventana de símbolo del sistema y ejecute `adsiedit.msc`
2. Vaya a **Acción** > **Conectar con**. Se mostrarán las ventanas de configuración de la conexión.
3. Haga clic en **Seleccionar un contexto de nomenclatura conocido**.
4. Expanda el cuadro de combinación más abajo y seleccione el contexto de nomenclatura **Predeterminado**.
5. Haga clic en **Aceptar**: el valor de ADSI de la izquierda debe ser el nombre de su controlador de dominio, el contexto de nomenclatura predeterminado (su controlador de dominio).
6. Haga clic en el valor de **ADSI** y expanda su subgrupo.
7. Haga clic en el **subgrupo** y vaya a CN (nombre común) o a OU (unidad organizativa) donde se muestran los ordenadores Linux.
8. Haga clic en **nombre de host** del ordenador Linux y seleccione **Propiedades** en el menú contextual. Vaya al parámetro **dNSHostName** y haga clic en **Modificar**.
9. Cambie el valor **no establecido** por un texto válido (por ejemplo, `ubuntu.TEST`).
10. Haga clic en **Aceptar** > **Aceptar**. Abra **ADUC** y seleccione las **propiedades** del ordenador Linux. El texto nuevo se debería mostrar aquí.

Sincronización de usuarios

Esta tarea del servidor sincroniza la información de los usuarios y los grupos de usuarios desde un origen como Active Directory, parámetros de LDAP, etc.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nuevo** > **Tarea del servidor** o seleccione el tipo de tarea que desee en el lateral izquierdo y haga clic en **Nuevo** > **Tarea del servidor**.

Básico

En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo de tarea específico antes de crear una tarea nueva, la opción de **Tarea** estará preseleccionada en función de la selección anterior. El apartado **Tarea** (consulte la lista de todas las tareas) define la configuración y el comportamiento de la tarea.

También puede seleccionar de los siguientes ajustes de activación de la tarea:

- **Ejecutar tarea inmediatamente después de finalizar**: seleccione esta opción para que la tarea se ejecute automáticamente después de que haga clic en Finalizar.
- **Configurar activador**- Seleccione esta opción para activar la sección Desencadenador, en la que podrá configurar los ajustes del desencadenador.

Para configurar el desencadenador más tarde, no marque estas casillas.

Configuración

Configuración común

Nombre del grupo de usuarios: de forma predeterminada, se utilizará la raíz para los usuarios sincronizados (de forma predeterminada, la raíz es el grupo **Todos**). También puede crear un nuevo grupo de usuarios.

Gestión de la colisión de creación de usuarios: pueden darse dos tipos de conflicto:

- Hay dos usuarios con el mismo nombre en el mismo grupo.
- Hay un usuario con el mismo SID (en cualquier parte del sistema).

Puede configurar la gestión de colisiones para:

- **Omitir**: el usuario no se agrega a ESET PROTECT On-Prem durante la sincronización con Active Directory.
- **Sobrescribir**: el usuario existente en ESET PROTECT On-Prem se sobrescribe con el usuario de Active Directory. En caso de producirse un conflicto de SID, el usuario existente de ESET PROTECT On-Prem se quita de la ubicación anterior (aunque el usuario estuviese en un grupo diferente).

Gestión de la extinción del usuario: si un usuario ya no existe, puede **Quitar** u **Omitir** este usuario.

Gestión de la extinción del grupo de usuarios: si un usuario ya no existe, puede **Quitar** u **Omitir** este grupo de usuarios.

> Si utiliza atributos personalizados para un usuario, configure **Gestión de la colisión de creación de usuarios** como **Omitir**. De lo contrario, el usuario (y todos los detalles) se sobrescribirán con los datos de Active Directory, con lo que se perderán los atributos personalizados. Si desea sobrescribir el usuario, cambie la **gestión de la extinción del usuario** a **Omitir**.

Configuración de conexión del servidor

- **Servidor** - Escriba el nombre de servidor o la dirección IP de su controlador de dominio.
- **Iniciar sesión** - Escriba el nombre de usuario de su controlador de dominio con el siguiente formato:
  - `DOMAIN\username` (ESET PROTECT Server en ejecución en Windows)
  - `username@FULL.DOMAIN.NAME` o `username` (ESET PROTECT Server en ejecución en Linux).

Escriba el dominio en mayúsculas, ya que este formato es necesario para autenticar las consultas correctamente en un servidor de Active Directory.

- **Contraseña**: escriba la contraseña que se usa para iniciar sesión en su controlador de dominio.

En Windows, ESET PROTECT utiliza el protocolo cifrado LDAPS (LDAP a través de SSL) de forma predeterminada para todas las conexiones de Active Directory (AD). También puede configurar LDAPS en el dispositivo virtual de ESET PROTECT.
Para establecer una conexión con Active Directory a través de LDAPS, realice los siguientes ajustes:
1. El controlador de dominio debe tener instalado un certificado de máquina. Para emitir un certificado para su controlador de dominio, siga los pasos indicados a continuación:
a)Abra el **Administrador de servidores**, haga clic en **Administrar** > **Agregar roles y características** e instale la autoridad (**Servicios de certificados de Active Directory** > **Autoridad certificadora**). Se creará una nueva autoridad certificadora en **Autoridades certificadoras de confianza**.
b)Diríjase a **Inicio** > escriba `certmgr.msc` y pulse **Entrar** para ejecutar el complemento **Certificados** Microsoft Management Console > **Certificados: ordenador local** > **Personal** > haga clic con el botón derecho del ratón en el panel vacío > **Todas las tareas** > **Solicitar nuevo certificado** > rol **Inscribir controlador de dominio** role.
c)Compruebe que el certificado emitido contenga el FQDN del controlador de dominio.
d)En el servidor de ESET PROTECT, importe la autoridad certificadora que generó para el almacén de certificados (con la herramienta `certmgr.msc`) en la carpeta de autoridades certificadoras de confianza.
2. Cuando proporcione la configuración de conexión al servidor de Active Directory, escriba el FQDN del controlador de dominio (como se indica en el certificado del controlador de dominio) en el campo **Servidor** o en el campo **Host**. La dirección IP ya no es suficiente para LDAPS.

Si desea activar el uso del protocolo LDAP, marque la casilla de verificación **Usar LDAP en lugar de Active Directory** e introduzca los atributos específicos que se ajusten a su servidor. También puede seleccionar **Preestablecidos** haciendo clic en **Seleccionar** y los atributos se completarán automáticamente:

- **Active Directory**
- Open Directory para el servidor de macOS (nombres de host del ordenador)
- **OpenLDAP con registros informáticos Samba**: configuración de los parámetros de nombre de DNS en Active Directory.

Configuración de sincronización

- **Nombre distinguido**: ruta (nombre distinguido) al nodo del árbol de Active Directory. Si se deja esta opción en blanco, se sincroniza el árbol entero de AD. Haga clic en **Examinar** junto a **Nombre distinguido**. Se mostrará su árbol de Active Directory. Seleccione la entrada superior para sincronizar todos los grupos de ESET PROTECT On-Prem o seleccione solo los grupos que quiera agregar. Solo se sincronizan los ordenadores y las unidades

organizativas. Haga clic en **Aceptar** cuando haya terminado.

> **Determinar el nombre distinguido**
> 1.Abra la aplicación **Usuarios y ordenadores de Active Directory**.
> 2.Haga clic en **Ver** y seleccione **Funciones avanzadas**.
> 3.Haga clic con el botón derecho en el dominio > haga clic en **Propiedades** > seleccione la ficha **Editor de atributos**.
> 4.Localice **distinguishedName** la línea. Debe tener el mismo aspecto que el de este ejemplo: `DC=ncop,DC=local`.

- **Atributos del usuario y el grupo de usuarios**: los atributos predeterminados del usuario son específicos del directorio al que pertenece el usuario. Si desea sincronizar los atributos de Active Directory, seleccione el parámetro de AD en el menú desplegable de los campos correspondientes, o escriba el nombre personalizado del atributo. Junto a cada campo sincronizado hay un marcador de posición de ESET PROTECT On-Prem (por ejemplo: `${display_name}`) que representará este atributo en determinados ajustes de la política de ESET PROTECT On-Prem.

- **Atributos avanzados del usuario**: si desea utilizar atributos personalizados avanzados, seleccione **Agregar nuevo**. Estos campos heredarán la información del usuario, que puede tratarse en el editor de directivas de MDM para iOS como marcador de posición.

> Si se muestra el error `Server not found in Kerberos database` al hacer clic en **Examinar**, utilice el nombre completo de AD del servidor en lugar de la dirección IP.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutan tareas. Cada **Tarea del servidor** puede tener un desencadenador como máximo. Cada desencadenador puede ejecutar solo una **tarea del servidor**. Si no se selecciona **Configurar activador** en la sección **Básico**, no podrán crearse desencadenadores. Pueden crearse tareas sin desencadenadores. Dichas tareas pueden ejecutarse posteriormente manualmente, o puede agregarse un desencadenador más tarde.

Configuración avanzada: Límites

Al configurar la Aceleración puede definir reglas avanzadas para el desencadenador creado. La configuración de la aceleración es opcional.

Resumen

Todas las opciones configuradas se muestran aquí. Revise la configuración y haga clic en **Finalizar**.

Puede ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.

Tipos de desencadenadores de tarea

Los desencadenadores son, básicamente, sensores que reaccionan a determinados sucesos de una forma predefinida. Se utilizan para ejecutar la tarea a la que están asignados. Pueden activarse por medio de tareas programadas (sucesos de tiempo) o cuando se produce un suceso determinado en el sistema.

No puede reutilizar un desencadenador. Cada tarea debe desencadenarse con un desencadenador diferente. Cada desencadenador puede ejecutar solo una tarea.

El desencadenador no ejecuta las tareas recién asignadas inmediatamente (excepto el desencadenador Lo antes posible o ASAP): la tarea se ejecuta en cuanto se activa el desencadenador. Mediante la aceleración se puede reducir la sensibilidad que el desencadenador presenta ante los sucesos.

Tipos de desencadenadores

- **Lo antes posible**: disponible únicamente para tareas del cliente. La tarea se ejecutará en cuanto haga clic en **Finalizar**. El valor **Fecha de caducidad** especifica la fecha tras la que dejará de ejecutarse la tarea.

Programado

El desencadenador planificado ejecutará la tarea según la configuración de fecha y hora. Las tareas se pueden planificar para **ejecutarse una vez**, de forma recurrente o según una expresión CRON.

- **Programar una vez**: este desencadenador se invoca una vez en la fecha y la hora planificadas. Puede retrasarse mediante un intervalo aleatorio.

- **Diariamente** - Este desencadenador se invoca todos los días seleccionados. Puede configurar el inicio y el fin del intervalo. Por ejemplo, puede ejecutar una tarea durante diez fines de semana consecutivos.

- **Semanalmente** - Este desencadenador se invoca el 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 los días seleccionados de la semana del mes seleccionada, durante el período de tiempo seleccionado. El valor **Repetir el** indica el día de la semana del mes (por ejemplo, el segundo lunes) en el que debe ejecutarse la tarea.

- **Anualmente** - Este desencadenador se invoca todos los años en la fecha de **inicio** especificada.

El ajuste **Intervalo de demora aleatorio** está disponible para los desencadenadores de tipo Programado. Define el intervalo de demora máxima para la ejecución de la tarea. La aleatoriedad puede prevenir la sobrecarga del servidor.

Si *John* configura la **Tarea** para que se desencadene **Semanalmente** los *lunes*, se **inicie** el *10 de febrero de 2017 a las 8:00:00*, con **Intervalo de demora aleatorio** configurado en *1 hora*, y **finalice el** *6 de abril de 2017 a las 00:00:00,* la tarea se ejecutará con una demora aleatoria de una hora entre las 8:00 y las 9:00 todos los lunes hasta la fecha de finalización especificada.

- Marque la casilla **Invocar lo antes posible si se pierde un evento** para ejecutar la tarea inmediatamente si no se ha ejecutado en el tiempo definido.
- Cuando se configura un desencadenador, se utiliza la zona horaria de ESET PROTECT Web Console de forma predeterminada. También puede marcar la casilla de verificación **Usar la hora local del destino** para usar la zona horaria local del dispositivo de destino en lugar de la zona horaria de ESET PROTECT Web Console para el desencadenador.

Grupo dinámico

Los desencadenadores de grupo dinámico solo están disponibles para las tareas del servidor:

• **Los miembros del grupo dinámico** cambiaron: este desencadenador se invoca cuando el contenido de un grupo dinámico cambia. Por ejemplo, si los clientes se unen a un grupo dinámico específico o lo abandonan.

• **El tamaño del grupo dinámico ha cambiado de acuerdo al umbral**: este desencadenador se invoca cuando el número de clientes de un grupo dinámico es mayor o menor que el umbral especificado. Por ejemplo, si hay más de 100 ordenadores en un grupo determinado.

• **El tamaño del grupo dinámico cambió con el período de tiempo**: este desencadenador se invoca cuando el número de clientes de un grupo dinámico cambia a lo largo de un periodo de tiempo definido. Por ejemplo, si el número de ordenadores de un grupo determinado aumenta un 10 % en una hora.

• **El tamaño del grupo dinámico cambió de acuerdo al grupo comparado**: este desencadenador se invoca cuando el número de clientes de un grupo dinámico observado cambia de acuerdo con un grupo comparado (estático o dinámico). Por ejemplo, si más del 10 % de todos los ordenadores están infectados (el grupo **Todo** comparado con el grupo **Infectados**).

Otros

• **Servidor iniciado**: solo está disponible para tareas del servidor. Se invoca cuando se inicia el servidor. Este desencadenador se utiliza, por ejemplo, para la tarea Sincronización de grupos estáticos.

• **Desencadenador de grupo dinámico unido**: solo está disponible para tareas del cliente. Este desencadenador se invoca cada vez que un dispositivo se une al grupo dinámico.

> **Desencadenador de grupo dinámico unido** solo está disponible si se selecciona un grupo dinámico en la sección Destino. El desencadenador solo ejecutará la tarea en los dispositivos que se unan al grupo dinámico después de que se cree dicho desencadenador. Para los dispositivos que ya estén en el grupo dinámico, tendrá que ejecutar la tarea manualmente.

• **Desencadenador de registro de eventos** - Este desencadenador se invoca cuando tiene lugar un suceso determinado en los registros. Por ejemplo, si hay una detección en el registro de **Análisis**. Este tipo de desencadenador ofrece un conjunto de ajustes especiales en la configuración de aceleración.

• **Expresión CRON** - Este desencadenador se invoca en una hora y una fecha determinadas.

Intervalo de la expresión CRON

Las expresiones CRON se utilizan para configurar instancias específicas de un desencadenador. Principalmente se utiliza para desencadenar varias repeticiones programadas. Es una cadena compuesta de 6 o 7 campos que representan valores de la programación. Los campos están separados por un espacio y contienen cualquiera de los valores permitidos con varias combinaciones.

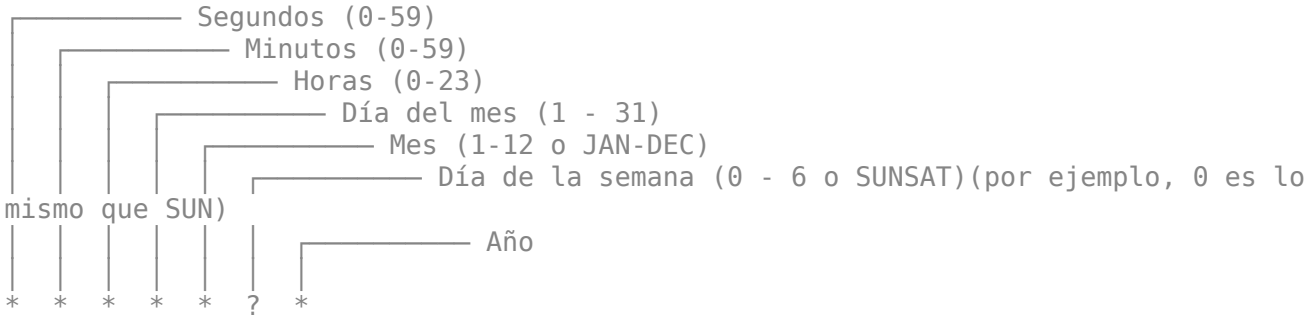
La expresión CRON puede ser tan sencilla como: `* * * * ? *` o más compleja, como: `0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020`

Lista de valores que puede utilizar en la expresión CRON:

Nombre	Requerido	Valor	Se permiten caracteres especiales
Segundos	Sí	0-59	`, - * / R`
Minutos	Sí	0-59	`, - * / R`
Horas	Sí	0-23	`, - * / R`
Día del mes	Sí	1-31	`, - * / ? L W`

Nombre	Requerido	Valor	Se permiten caracteres especiales
Mes	Sí	1-12 o JAN-DEC	, - */
Día de la semana	Sí	0-6 o SUN-SAT	, - / ? L #
Año	Sí	1970-2099	, - * /

La sintaxis de la expresión CRON es la siguiente:



- 0 0 0 equivale a medianoche (segundos, minutos y horas).
- Utilice ? cuando no se pueda definir un valor porque se ha definido en otro campo (día del mes o día de la semana).
- El * equivale a todos los valores posibles (segundos, minutos, horas, día del mes, mes, día de la semana, año).
- SUN equivale al domingo.

> Los nombres de meses y días de la semana no distinguen entre mayúsculas y minúsculas. Por ejemplo, MON es lo mismo que mon, o JAN es lo mismo que jan.

Caracteres especiales:

Coma (,)

Las comas se utilizan para separar los elementos de una lista. Por ejemplo, utilizar "MON,WED,FRI" en el sexto campo (día de la semana), equivale a los lunes, miércoles y viernes.

Guion (-)

Define intervalos. Por ejemplo, 2012-2020 indica todos los años desde el 2012 hasta el 2020, ambos incluidos.

Comodín (*)

Se utiliza para seleccionar todos los valores posibles de un campo. Por ejemplo, la inclusión de * en el campo de minuto equivale a todos los minutos. El comodín no se puede utilizar en el campo del día de la semana.

Signo de interrogación (?)

Al elegir un día concreto puede especificar un día del mes o de la semana. No puede especificar los dos a la vez. Si especifica un día del mes, debe utilizar ? para el día de la semana, y viceversa. Por ejemplo, si quiere que el desencadenador se active un día concreto del mes (por ejemplo el día 10), pero no le importa el día de la semana que sea, introduzca 10 en el campo del día del mes y ? en el campo del día de la semana.

Almohadilla (#)

Se utiliza para especificar "el día x" del mes. Por ejemplo, el valor 4#3 en el campo del día de la semana significa el tercer jueves del mes (día 4 = jueves y #3 = el tercer jueves del mes). Si especifica #5 y no hay una quinta aparición del día de la semana en el mes en cuestión, el desencadenador no se activará en ese mes.

Barra diagonal (/)

Describe incrementos de un intervalo. Por ejemplo, la inclusión del valor 3-59/15 en el segundo campo (minutos) indica el tercer minuto de la hora y cada 15 minutos después.

Último (L)

Cuando se utiliza en el campo del día de la semana, le permite especificar estructuras como el último viernes (5L) de un mes determinado. En el campo del día del mes especifica el último día del mes. Por ejemplo, el día 31 en enero, el día 28 en febrero, cuando se trata de años no bisiestos.

Día de la semana (W)

El carácter W se permite en el campo del día del mes. Este carácter se utiliza para especificar el día de la semana (de lunes a viernes) más próximo al día en cuestión. Por ejemplo, si especifica 15W como valor del campo del día del mes, equivale al día de la semana más cercano al día 15 del mes. Por lo tanto, si el día 15 del mes es sábado, el desencadenador se activa el viernes 14. Si el 15 es domingo, el desencadenador se activa el lunes 16. Sin embargo, si especifica 1W como valor del día del mes y el primer día del mes es sábado, el desencadenador se activa el lunes 3, ya que no salta el límite que representan los días de un mes.

Los caracteres L y W también se pueden combinar en el campo del día del mes, con lo que se obtiene LW, lo que equivale al último día de la semana del mes.

Aleatorio (R)

R es un carácter especial de expresión CRON de ESET PROTECT On-Prem que le permite especificar momentos aleatorios en el tiempo. Por ejemplo, el desencadenador R 0 0 * * ? * se activa todos los días a las 00:00, pero en un segundo aleatorio (0-59).

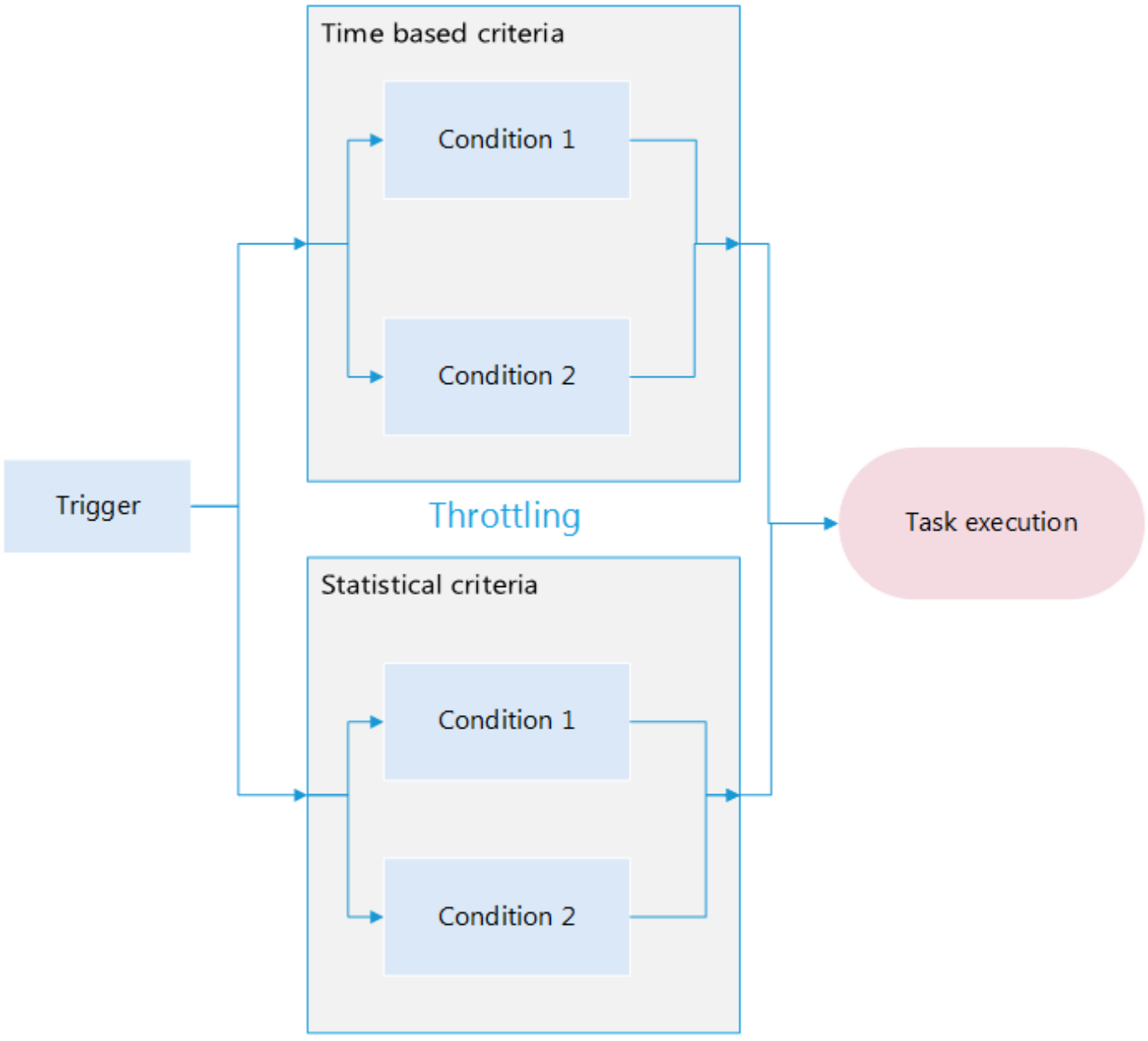
Se recomienda utilizar los momentos de tiempo aleatorios para evitar que todos los ESET Management Agent se conecten a la vez a su ESET PROTECT Server.

Algunos ejemplos reales que ilustran variaciones de la expresión CRON:

Expresión CRON	Significado
`0 0 12 * * ? *`	Activación a las 12 p. m. (mediodía) todos los días.
`R 0 0 * * ? *`	Activación a las 00:00 pero en un segundo aleatorio (0-59).
`R R R 15W * ? *`	Activación el día 15 de todos los meses a una hora aleatoria (segundos, minutos, horas). Si el día 15 del mes es sábado, el desencadenador se activa el viernes 14. Si el 15 es domingo, el desencadenador se activa el lunes 16.
`0 15 10 * * ? 2016`	Activación a las 10:15 a. m. todos los días durante al año 2016.
`0 * 14 * * ? *`	Activación cada minuto a partir de las 2 p. m. y hasta las 2:59 p. m., todos los días.
`0 0/5 14 * * ? *`	Activación 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 * * ? *`	Activación cada 5 minutos a partir de las 2 p. m. y hasta las 2:55 p. m., y activación cada 5 minutos a partir de las 6 p. m. y hasta las 6:55 p. m., todos los días.
`0 0-5 14 * * ? *`	Activación 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 *`	Activación a las 2:10 p. m. y a las 2:44 p. m. todos los miércoles de marzo.
`0 15 10 ? * MON-FRI *`	Activación a las 10:15 a. m. todos los lunes, martes, miércoles, jueves y viernes.
`0 15 10 15 * ? *`	Activación a las 10:15 a. m. el día 15 de cada mes.
`0 15 10 ? * 5L *`	Activación a las 10:15 a. m. el último viernes de cada mes.
`0 15 10 ? * 5L 2016-2020`	Activación a las 10:15 a. m. el último viernes de cada mes desde el año 2016 hasta el 2020, ambos incluidos.
`0 15 10 ? * 5#3 *`	Activación a las 10:15 a. m. el tercer viernes de cada mes.
`0 0 * * * ? *`	Activación cada hora de todos los días.

Configuración avanzada: Límites

La aceleración se utiliza para impedir que se ejecute una tarea. Normalmente, la aceleración se utiliza cuando un evento que sucede con frecuencia desencadena una tarea. En determinadas circunstancias la aceleración puede impedir que se active un desencadenador. Cada vez que se activa el desencadenador, se evalúa de acuerdo con el esquema que aparece a continuación. A continuación, solo los desencadenadores que cumplan las condiciones especificadas harán que se ejecute la tarea. Si no se configura ninguna condición de aceleración, todos los eventos de desencadenador ejecutarán la tarea.



Hay tres tipos de condiciones para los límites:

- **Criterios basados en el tiempo**
- **Criterios estadísticos**
- **Criterios del registro de eventos**

Para que una tarea se ejecute:

- Debe cumplir todos los tipos de condiciones
- Deben configurarse las condiciones; si una condición está vacía, se omite
- Deben cumplirse todas las condiciones temporales, pues se evalúan con el operador AND
- Deben cumplirse todas las condiciones estadísticas evaluadas con el operador AND; debe cumplirse al menos una condición estadística con el operador OR
- Deben cumplirse las condiciones estadísticas y temporales configuradas conjuntamente, pues se evalúan con el operador AND: solo entonces se ejecuta la tarea

Si se cumple alguna de las condiciones, se restablece la información apilada de todos los observadores (el recuento comienza desde 0). Esto se aplica tanto a las condiciones temporales como a las estadísticas. Esta información también se restablece si se reinician el agente o ESET PROTECT Server. Todas las modificaciones efectuadas en un desencadenador restablecen su estado. Le recomendamos que solo utilice una condición estadística y varias condiciones basadas en el tiempo. Tener varias condiciones estadísticas puede ser una complicación innecesaria y modificar los resultados del desencadenador.

Preajuste

Hay tres preajustes disponibles. Cuando selecciona un preajuste, la configuración de límite actual se elimina y se sustituye por los valores preajustados. Estos valores se pueden seguir modificando y utilizando, pero no se puede crear un preajuste nuevo.

Criterios basados en el tiempo

Periodo de tiempo (T2): para permitir el desencadenamiento una vez durante el periodo especificado. Si esta opción se configura, por ejemplo, en diez segundos, y durante este tiempo se producen diez invocaciones, solo la primera desencadenará el evento.

Debe configurar la regulación con criterios temporales para limitar la ejecución de tareas a como máximo una vez cada minuto (un icono de bloqueo indica la limitación):
- Tareas del servidor (incluida la generación de informes): todos los tipos de desencadenadores.
- Tareas del cliente: tipos de desencadenadores **expresión CRON** y **programados**.

Si ha actualizado desde la versión 8.x o 9.x de ESET PROTECT On-Prem, se aplicarán automáticamente 1 minutos a todas las tareas existentes con el periodo de tiempo establecido en menos de 1 minutos.
El periodo de tiempo mínimo de 15 minutos no se aplica a las notificaciones.

Programar (T1): solo permite el desencadenamiento dentro del intervalo de tiempo definido. Haga clic en **Agregar periodo** y se mostrará una ventana emergente. Ajuste una **Duración de intervalo** en las unidades de tiempo seleccionadas. Seleccione una opción en la lista **Recurrencia** y rellene los campos, que cambiarán en función de la recurrencia seleccionada. También puede definir la recurrencia en forma de Expresión CRON. Haga clic en **Aceptar** para guardar el intervalo. Puede agregar varios rangos de tiempo a la lista y se ordenarán cronológicamente.

Todas las condiciones configuradas deben cumplirse para desencadenar la tarea.

Criterios estadísticos

Condición: pueden combinarse condiciones estadísticas mediante:

- **Enviar notificación cuando se cumplan todos los criterios estadísticos: AND** se utiliza como operador lógico para la evaluación.

- **Enviar notificación cuando se cumpla al menos un criterio estadístico**: **OR** se utiliza como operador lógico para la evaluación.

Número de ocurrencias (S1): solo se permite cada x invocaciones del desencadenador. Por ejemplo, si introduce diez, solo se desencadenará cada diez invocaciones del desencadenador.

Número de ocurrencias en un periodo de tiempo

N.º de ocurrencias (S2): solo permite el desencadenamiento dentro del periodo de tiempo definido. Esta opción define la frecuencia mínima que deben tener los eventos para desencadenar la tarea. Por ejemplo, puede utilizar este ajuste para permitir la ejecución de la tarea si el evento se detecta 10 veces en una hora. La activación del desencadenante provoca el reinicio del contador.

Periodo de tiempo: defina el periodo de tiempo para la opción descrita anteriormente.

Hay una tercera condición estadística disponible solo para determinados tipos de desencadenador. Consulte **Desencadenador** > **Tipo de desencadenador** > **Desencadenador de registro de eventos**.

Criterios del registro de eventos

ESET PROTECT On-Prem evalúa estos criterios como terceros criterios estadísticos (S3). Se aplica el operador de **Aplicación de criterios estadísticos** (AND/OR) para evaluar las tres condiciones estadísticas juntas. Se recomienda utilizar los criterios del registro de eventos en combinación con la tarea **Generar informe**. Para que los criterios funcionen son necesarios los tres campos. El búfer de símbolos se restablece si el desencadenador se activa y ya hay un símbolo en el búfer.

Condición: esta opción define qué eventos o conjuntos de eventos desencadenarán la condición. Las opciones disponibles son:

- **Recibidos seguidos**: el número de eventos especificado deben producirse seguidos. Estos eventos deben ser independientes.

- **Recibidos desde la última ejecución del desencadenador**: la condición se desencadena cuando se alcanza el número seleccionado de eventos independientes desde la última vez que se desencadenó la tarea.

Número de ocurrencias: introduzca el número entero de eventos independientes con los símbolos seleccionados para ejecutar la tarea.

Símbolo: de acuerdo con el **Tipo de registro**, que se configura en el menú **Desencadenador**, puede elegir un símbolo en el registro y, a continuación, puede buscarlo. Haga clic en **Seleccionar** para ver el menú. Puede quitar el símbolo seleccionado haciendo clic en **Quitar**.

> Cuando se utiliza con una tarea del servidor, se consideran todos los ordenadores cliente. Es poco probable recibir más símbolos distintivos seguidos. Utilice el ajuste **Recibidos seguidos** únicamente en casos razonables. Un valor ausente (N/D) se considera "no exclusivo" y, por lo tanto, el búfer se restablece en este punto.

Propiedades adicionales

Como se ha indicado anteriormente, no todos los sucesos provocarán la activación de un desencadenador. Las medidas adoptadas con sucesos que no activen sucesos pueden ser:

- Si hay más de un suceso omitido, agrupar los últimos **N** sucesos en uno (almacenar datos de marcas suprimidas) [**N** <= 100]
- Si **N** == 0, solo se procesa el último suceso (**N** equivale a la duración del historial, donde el último suceso siempre se procesa)
- Todos los sucesos que no activen desencadenadores se fusionan (la última marca se fusiona con **N** marcas históricas)

Si el desencadenador se activa con demasiada frecuencia o si quiere recibir notificaciones con menos frecuencia, puede tener en cuenta las siguientes sugerencias:

- Si el usuario solo desea reaccionar si hay más sucesos, no solo uno, consulte la condición estadística S1
- Si el desencadenador solo se debe activar cuando se produce un conjunto de eventos, siga la condición estadística S2
- Si se supone que los eventos con valores no deseados deben ignorarse, consulte la condición estadística S3
- Cuando se deban ignorar los sucesos fuera de un horario determinado (por ejemplo, horas laborables), consulte la condición temporal T1
- Para establecer un tiempo mínimo entre activaciones del desencadenador, utilice la condición temporal T2

> Las condiciones también se pueden combinar para crear situaciones de aceleración más complejas. Consulte los ejemplos de aceleración para obtener más información.

Ejemplos de aceleración

Los ejemplos de aceleración explican cómo se combinan y evalúan las condiciones de aceleración (T1, T2, S1, S2, S3).

> "Marca" significa impulso procedente del desencadenador. "T" significa criterios temporales, "S" significa criterios estadísticos. "S3" significa criterios del registro de eventos.

S1: Criterio de ocurrencias (permitir cada tercera marca)

Hora	00	01	02	03	04	05	06	El desencadenador se modifica	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 para ocurrencias durante un periodo de tiempo (permitir si se producen tres marcas en un periodo de cuatro segundos)

Hora	00	01	02	03	04	05	06	El desencadenador se modifica	07	08	09	10	11	12	13
Marcas	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Criterio para valores de símbolo exclusivo (permitir si hay tres valores exclusivos consecutivos)

Hora	00	01	02	03	04	05	06	El desencadenador se modifica	07	08	09	10	11	12	13
Valor	A	B	B	C	D	G	H		J	K	n/d	L	M	N	N
S3					1									1	

S3: Criterio para valores de símbolo exclusivo (permitir si hay tres valores exclusivos desde la última marca)

Hora	00	01	02	03	04	05	06	07	El desencadenador se modifica	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: permitir una marca en intervalos de tiempo determinados (permitir todos los días a partir de las 8:10, 60 segundos de duración)

Hora	8:09:50	8:09:59	8:10:00	8:10:01	El desencadenador se modifica	8:10:59	8:11:00	8:11:01
Marcas	x	x	x	x		x	x	x
T1			1	1		1		

Este criterio no presenta estado, y por lo tanto las modificaciones del desencadenador no tienen consecuencias en los resultados.

T2: Permitir una sola marca en un intervalo de tiempo (permitir como máximo una vez cada cinco segundos)

Hora	00	01	02	03	04	05	06	El desencadenador se modifica	07	08	09	10	11	12	13
Marcas	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Combinación de S1+S2

- S1: Cada quinta marca
- S2: Tres marcas en cuatro segundos

Hora	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 se enumera como: S1 (o lógico) S2

Combinación de S1+T1

- S1: Permitir cada tres marcas
- T1: permitir todos los días a partir de las 8:08, 60 segundos de duración

Hora	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	
T1					1	1	1	1	1	
Resultado						1			1	

El resultado se enumera como: S1 (y lógico) T1

Combinación de S2+T1

- S2: Tres marcas en diez segundos
- T1: permitir todos los días a partir de las 8:08, durante un periodo de 60

Hora	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 se enumera como: S2 (y lógico) T1.

Tenga en cuenta que el estado de S2 se restablece solo cuando el resultado global es 1.

Combinación de S2+T2

- S2: Tres marcas en diez segundos
- T2: permitir como máximo una vez cada 20 segundos

Hora	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 se enumera como: S2 (y lógico) T2.

Tenga en cuenta que el estado de S2 se restablece solo cuando el resultado global es 1.

Instaladores

Esta sección le muestra cómo crear paquetes de instaladores de Agent para implementar ESET Management Agent en ordenadores cliente. Los paquetes de instaladores se guardan en ESET PROTECT Web Console, y puede modificarlos y descargarlos de nuevo cuando sea necesario.

Haga clic en **Instaladores** > **Crear instalador** y seleccione el sistema operativo.

Windows

- Descargar el instalador o utilizar ESET Remote Deployment Tool: el paquete del instalador de Agent y productos de seguridad de ESET ofrece opciones de configuración avanzadas, como la configuración de políticas para ESET Management Agent y los productos de ESET, el nombre de cliente y el puerto de ESET PROTECT Server y la posibilidad de seleccionar un grupo principal. Puede implementar el instalador de forma local o remota (con ESET Remote Deployment Tool).

- Implementar primero el agente (instalador de scripts del agente) –Este tipo de implementación del agente es útil cuando las opciones de implementación remota y local no le convienen. Puede distribuir el instalador de scripts del agente por correo electrónico y dejar que el usuario lo implemente. También puede ejecutar el instalador de scripts del agente desde un medio extraíble (una unidad de memoria USB, por ejemplo).

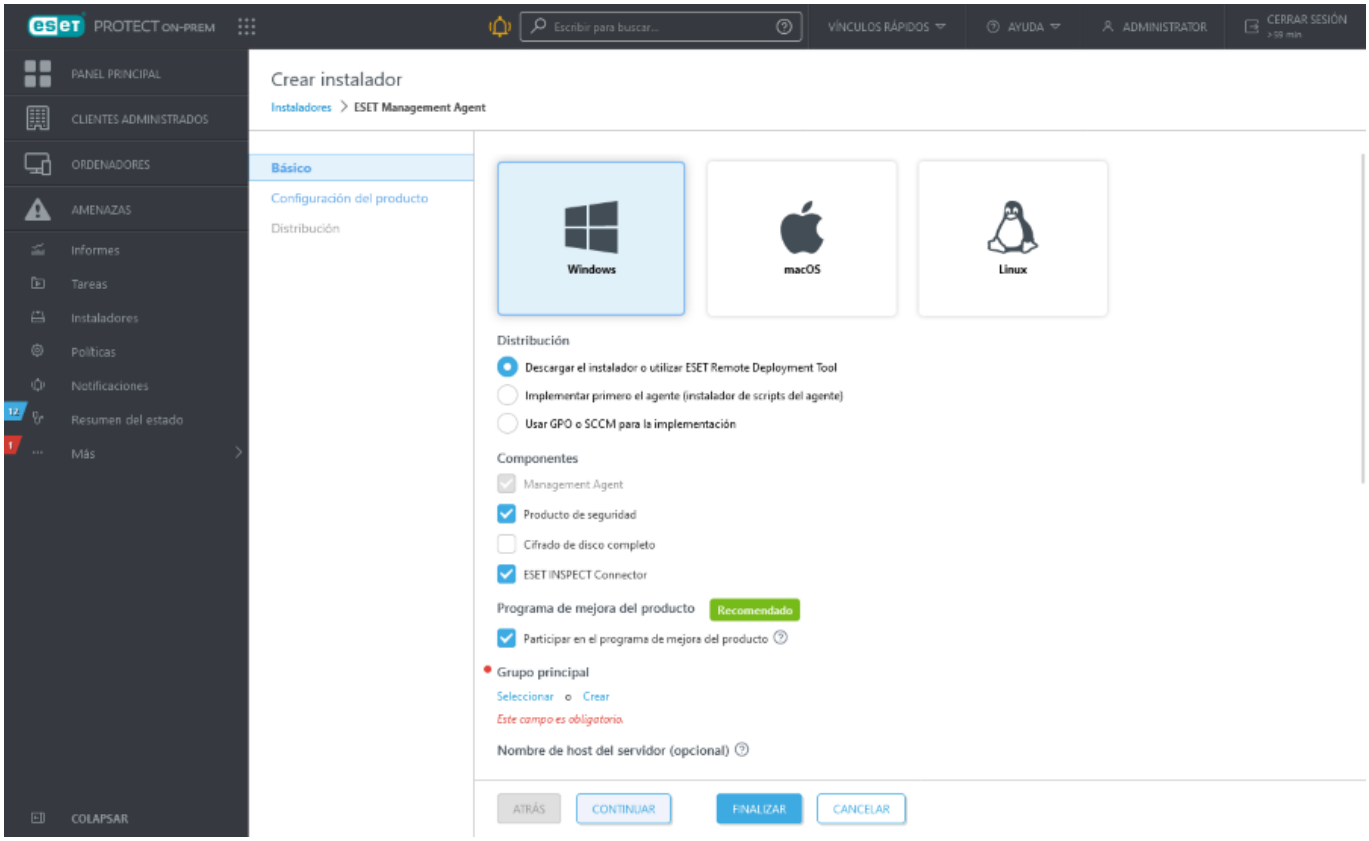
- Usar GPO o SCCM para la implementación –Utilice esta opción para la implementación masiva de ESET Management Agent en ordenadores cliente.

macOS

- El paquete del Descargar o enviar instalador instalador de Agent y productos de seguridad de ESET permite utilizar opciones de configuración avanzadas, como la configuración de políticas para ESET Management Agent y los productos de ESET, el nombre de cliente y el puerto de Server y la posibilidad de seleccionar un grupo principal.

Linux

- Implementar primero el agente (instalador de scripts del agente) –Este tipo de implementación del agente es útil cuando las opciones de implementación remota y local no le convienen. Puede distribuir el instalador de scripts del agente por correo electrónico y dejar que el usuario lo implemente. También puede ejecutar el instalador de scripts del agente desde un medio extraíble (una unidad de memoria USB, por ejemplo).



Instaladores y permisos

Un usuario puede crear o editar instaladores contenidos en grupos en los que dicho usuario tenga permiso de **Escritura** sobre **Grupos y ordenadores** e **Instaladores almacenados**.

Para descargar instaladores ya creados, el usuario necesita permiso de **Uso** sobre **Grupos y ordenadores** e **Instaladores almacenados**.

- Asigne a un usuario el permiso de **Uso** de las **Políticas** seleccionadas en **Opciones avanzadas** > **Configuración inicial del instalador** > **Tipo de configuración** al crear un instalador todo en uno, un instalador de GPO o un script de SCCM.
- Asigne a un usuario el permiso de **Uso** de las **Licencias** si se especifica la licencia correspondiente al 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.
- Recuerde que el usuario podrá trabajar con Certificados al crear instaladores. Asigne a un usuario el permiso de **Uso** de los **Certificados** con acceso al grupo estático que contiene los certificados. Si un usuario quiere implementar ESET Management Agent, deberá tener permisos de **Uso** de la autoridad certificadora que ha firmado el certificado del servidor. Para obtener información acerca de la división del acceso a certificados y autoridades certificadoras, lea este ejemplo.

Grupo de inicio – El grupo de inicio 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 derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "Department_1" como **grupo de inicio** de la tarea del cliente.

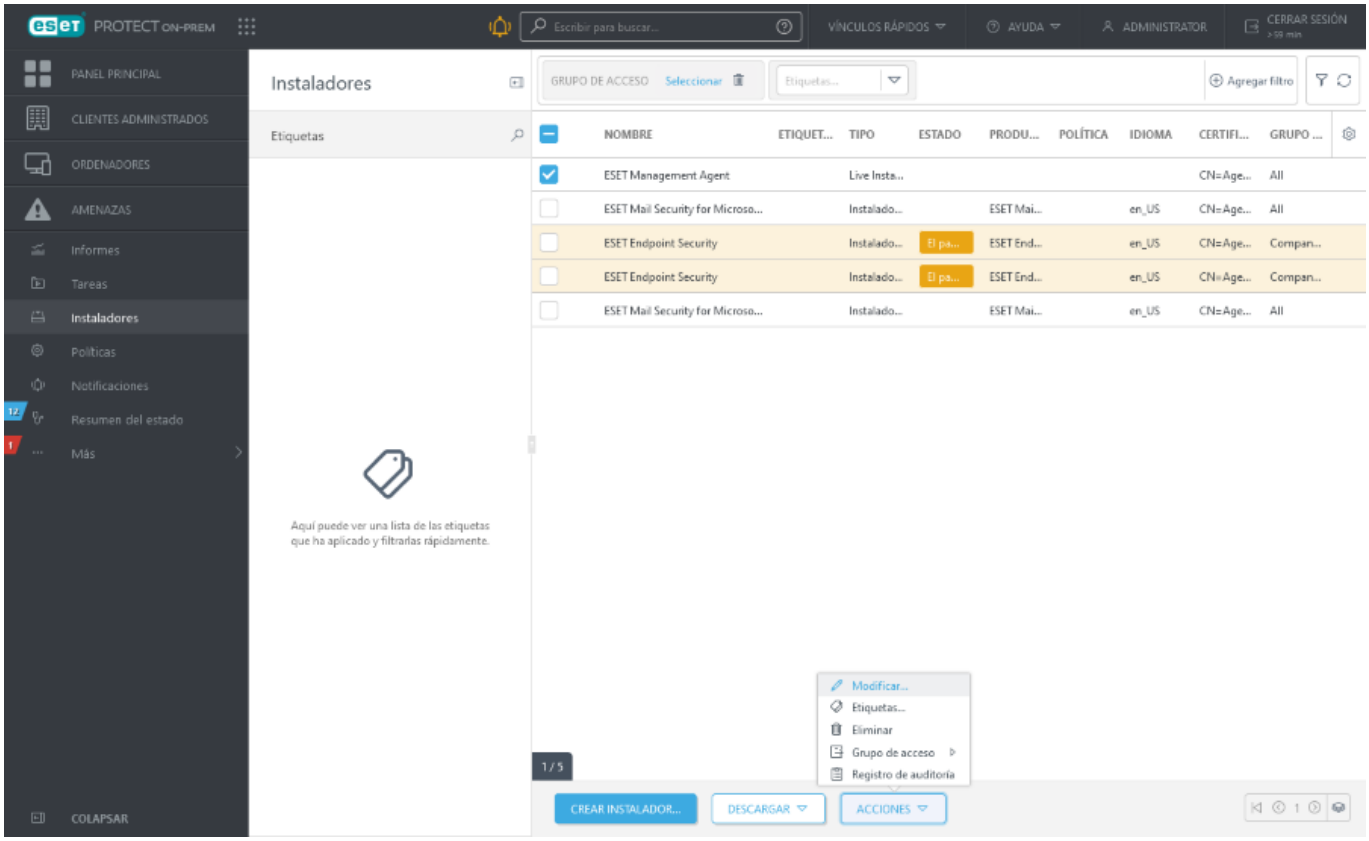
Si el grupo de inicio preseleccionado no cumple sus expectativas, puede seleccionar uno manualmente.

Permitir que los usuarios creen instaladores

El *administrador* quiere permitir que el usuario *John* cree o modifique nuevos instaladores en el *Grupo de John*. El *administrador* debe seguir estos pasos:

1. Crear un nuevo Grupo estático llamado *Grupo de John*
2. Crear un nuevo conjunto de permisos
   a. Llamar al nuevo conjunto de permisos *Permisos de John: crear instaladores*
   b. Agregar el grupo *Grupo de John* a la sección **Grupos estáticos**
   c. En la sección **Funcionalidad**, seleccionar
      - **Escritura** en **Instaladores almacenados**
      - **Uso** en **Certificados**
      - **Escritura** en **Grupos y ordenadores**
   d. Hacer clic en **Finalizar** para guardar el conjunto de permisos
3. Crear un nuevo conjunto de permisos
   a. Llamar al nuevo conjunto de permisos *Permisos de John: certificados*
   b. Agregar el grupo *Todo* a la sección **Grupos estáticos**
   c. En la sección **Funcionalidad**, seleccionar **Uso** para **Certificados**.
   d. Hacer clic en **Finalizar** para guardar el conjunto de permisos

   Estos permisos son los requisitos mínimos para poder utilizar plenamente (crear y modificar) los instaladores.
4. Crear un nuevo usuario
   a. Nombrar al nuevo usuario *John*
   b. En la sección **Básico**, seleccionar *Grupo de John* como grupo principal
   c. Configurar la contraseña del usuario *John*
   d. En la sección **Conjuntos de permisos**, seleccionar *Permisos de John: certificados* y *Permisos de John: crear instaladores*
   e. Hacer clic en **Finalizar** para guardar el usuario



Descargar instaladores del menú de instaladores

1.Haga clic en **Instaladores**.

2.Marque la casilla situada junto al instalador que quiera descargar.

3.Haga clic en **Descargar** y elija el paquete de instalación correcto (en función del valor 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, ESET Inspect Connector o ESET Full Disk Encryption), aparecerá una ventana. Marque la casilla **Acepto el Acuerdo de licencia para el 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.Marque la casilla situada junto al instalador que quiera modificar.

3.Haga clic en **Acciones** > **Modificar** para modificar el paquete de instaladores.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.

- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Políticas

Las políticas se utilizan para aplicar configuraciones específicas de productos de seguridad de ESET a sus ordenadores cliente. Esto le permite tener que configurar el producto de ESET manualmente. Una política se puede aplicar directamente a ordenadores individuales así como grupos (Estáticos y Dinámicos). Asimismo, puede asignar varias políticas a un ordenador o un grupo.

Políticas y permisos

El usuario debe tener permisos suficientes para crear y asignar políticas. Permisos necesarios para determinadas acciones relacionadas con políticas:

- Para leer la lista de políticas y su configuración, el usuario necesita permiso de **Lectura**.
- Para asignar políticas a destinos, el usuario necesita permiso de **Uso**.
- Para crear, modificar o editar políticas, el usuario necesita permiso de **Escritura**.

Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Hay un icono de bloqueo junto a las políticas bloqueadas (no editables): políticas integradas específicas (por ejemplo, la política de actualizaciones automáticas o las políticas ESET LiveGuard) o políticas para las que el usuario tiene permiso de **Lectura**, pero no de **Escritura**.

- Si el usuario *John* solo necesita leer las políticas creadas por él mismo, se necesita el permiso de **Lectura** en **Políticas**.
- Si el usuario *John* quiere asignar determinadas políticas a los ordenadores, necesita permiso de **Uso** de **Políticas** y permiso de **Uso** de **Grupos y ordenadores**.
- Para otorgar a *John* acceso total a las políticas, el *administrador* debe configurar el permiso de **Escritura** en **Políticas**.

Aplicación de las políticas

Las políticas se aplican en el orden de disposición de los grupos estáticos. Este no es el caso de los grupos dinámicos, ya que se aplican primero a los grupos dinámicos secundarios. Esto le permite aplicar aquellas políticas que tienen más consecuencias en la parte superior del árbol de grupos, y aplicar políticas más específicas para los subgrupos. Utilizando indicadores, un usuario de ESET PROTECT On-Prem con acceso a los grupos situados más arriba en el árbol puede anular las políticas de los grupos inferiores. El algoritmo se explica de forma detallada en Cómo se aplican las políticas a los clientes.

Reglas de eliminación de políticas

Si cuenta con una política y posteriormente decide quitarla, la configuración resultante de los ordenadores cliente dependerá de la versión del producto de seguridad de ESET instalado en los ordenadores administrados:

- Al quitar una política o seleccionar el indicador **No se aplica**, la configuración vuelve automáticamente a los valores locales anteriores. Cuando un ordenador deja un grupo dinámico en el que había una configuración de política concreta, esta configuración de política se quitará del ordenador. Este

comportamiento se aplica a:

Productos de seguridad de ESET Windows	versión 7 y posteriores
Productos de seguridad de ESET macOS	versión 7 y posteriores
Productos de seguridad de ESET Linux	versión 8.1 y posteriores

• Productos de seguridad ESET anteriores (a los mencionados previamente): La configuración no recuperará automáticamente los ajustes originales tras la eliminación de la política. La configuración se conservará según la última política aplicada a los clientes. Esta misma situación tiene lugar cuando un ordenador se convierte en miembro de un Grupo dinámico al que se aplica una política determinada que modifica la configuración del ordenador. Esta configuración se conserva incluso si el ordenador abandona el grupo dinámico. Por ello, recomendamos crear una política con la configuración predeterminada y asignarla al grupo raíz (**Todos**) para que en una situación de este tipo se recupere la configuración predeterminada. De esta forma, cuando un ordenador sale de un grupo dinámico que modificó su configuración, este ordenador vuelve a adoptar su configuración predeterminada.

Fusión de políticas

Las políticas que se aplican a un cliente habitualmente son el resultado de varias políticas fusionadas en una política final.

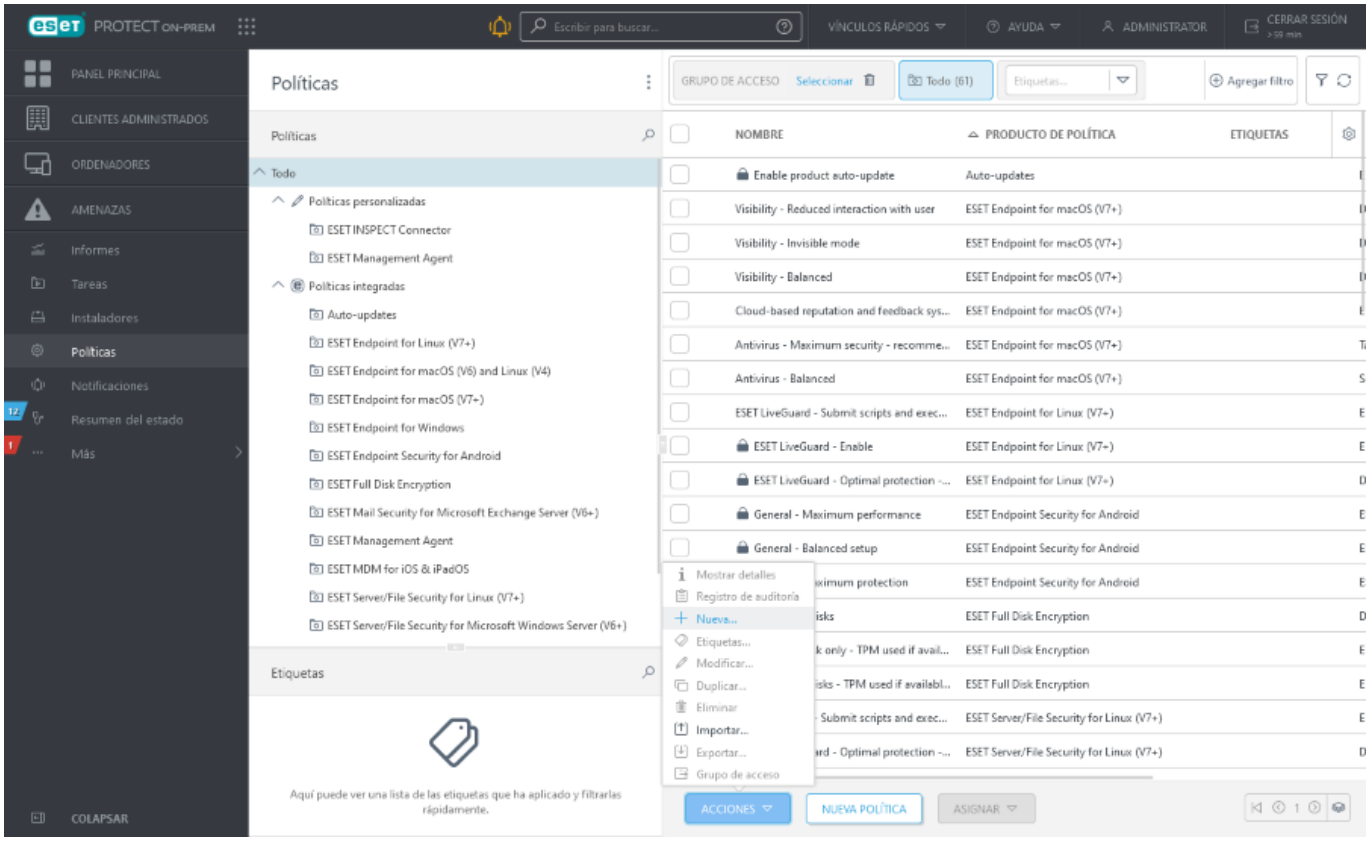
Le recomendamos que asigne políticas más genéricas (por ejemplo, el servidor de actualización) a grupos que están más arriba en el árbol de grupos. Políticas más específicas (por ejemplo, configuración del control de dispositivos) más abajo en el árbol de grupos. Las políticas más bajas suelen reemplazar la configuración de las políticas superiores cuando se fusionan (excepto cuando se define de otra forma con indicadores de política).

Asistente para políticas

Las políticas se agrupan o clasifican por producto de ESET. **Políticas integradas** contiene las políticas predefinidas y **personalizadas**, y muestra las categorías de todas las políticas que ha creado o modificado manualmente.

Utilice las políticas para configurar su producto ESET de la misma forma que lo haría en la ventana Configuración avanzada de la interfaz gráfica de usuario del producto. A diferencia de las políticas de Active Directory, las políticas de ESET PROTECT On-Prem no pueden contener scripts ni series de comandos.

Escriba para buscar un elemento en Configuración avanzada (por ejemplo, HIPS). Se mostrarán todos los ajustes de HIPS. Cuando haga clic en el icono ⓘ de la esquina superior derecha, aparecerá la página de ayuda en línea del ajuste en cuestión.



Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Crear una política nueva

1.Haga clic en **Acciones** > **Nueva**.

2.Introduzca información básica acerca de la política, como el **Nombre** y la **Descripción** (opcional). Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

3.Seleccione el producto correcto en la sección **Configuración**.

4.Utilice indicadores para agregar los ajustes que gestionará la política.

5.Especifique los clientes que recibirán esta política. Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione el ordenador en el que quiera aplicar una política y haga clic en **Aceptar**.

6.Revise las opciones de esta directiva y haga clic en **Finalizar**.

Indicadores

Al fusionar políticas, puede cambiar el comportamiento utilizando indicadores de política. Los indicadores definen la forma en la que la política tratará una configuración.

Para cada configuración, puede seleccionar uno de los siguientes indicadores:

No aplicar: la política no configurará ningún ajuste con este indicador. Dado que este ajuste no se aplica, otras políticas pueden cambiarlo más tarde.

Aplicar: los ajustes que presenten este indicador se envían al cliente. No obstante, al fusionar políticas, una política posterior lo puede sobrescribir. Cuando se aplica una política a un ordenador cliente y un ajuste concreto tiene este indicador, el ajuste cambia independientemente de lo que se hubiera configurado localmente en el cliente. Dado que este ajuste no se aplica, otras políticas pueden cambiarlo más tarde.

Forzar: los ajustes que tengan este indicador tendrán prioridad y no podrán sobrescribirse con una política posterior (aunque también tenga este indicador establecido). Esta práctica garantiza que el ajuste no se verá modificado por posteriores políticas a la hora de ejecutar la fusión.

Se cuentan todas las reglas para facilitar la navegación. El número de reglas que haya definido en una sección determinada se mostrará automáticamente. Verá también un número junto a los nombres de categorías en el árbol de la izquierda. Este número indica la suma de las reglas de todas las secciones. De esta forma sabrá rápidamente dónde hay ajustes y reglas definidos, así como su número.

También puede usar las siguientes sugerencias para facilitar la edición de políticas:

- Use para configurar el indicador **Aplicar** en todos los elementos de la sección
- Use la marca **No aplicar** para eliminar las reglas aplicadas a los elementos de la sección actual.

Consulte también las reglas de eliminación de políticas.

Cómo puede el administrador permitir que los usuarios vean todas las políticas

El *administrador* quiere permitir que el usuario *John* cree o modifique políticas en su grupo principal y quiere permitir que *John* vea las políticas creadas por el *administrador*. Las políticas creadas por el *administrador* incluyen los indicadores **Forzar**. El usuario *John* puede ver todas las políticas, pero no puede modificar las políticas creadas por el *administrador* porque se ha configurado el permiso de **Lectura** en las **Políticas** con acceso al grupo estático *Todo*. El usuario *John* puede crear o modificar políticas en su grupo principal, *San Diego*.

El *administrador* debe seguir estos pasos:

Crear entorno

1.Cree un nuevo Grupo estático llamado *San Diego*.

2.Cree un nuevo Conjunto de permisos llamado *Políticas: Todo John* con acceso al grupo estático *Todo* y con permiso de **Lectura** en **Políticas**.

3.Cree un nuevo Conjunto de permisos llamado *Política John* con acceso al grupo estático *San Diego* y con acceso a la funcionalidad del permiso de **Escritura** en **Grupo y ordenadores** y **Políticas**. Este conjunto de permisos otorga a *John* el derecho de crear o modificar políticas en su grupo principal, *San Diego*.

4.Cree un nuevo usuario *John* y, en la sección **Conjuntos de perrmisos**, seleccione *Políticas: Todo John* y *Política John*.

Crear políticas

5.Cree la nueva política *Todo: activar el cortafuegos*, despliegue la sección **Configuración**, seleccione **ESET Endpoint para Windows**, desplácese hasta **Protección de la red** > **Cortafuegos** > **Básico** y aplique toda la configuración mediante el indicador **Forzar**. Despliegue la sección **Asignar** y seleccione el grupo estático *Todo*.

6.Cree la nueva política *Grupo de John: activar el cortafuegos*, despliegue la sección **Configuración**, seleccione **ESET Endpoint para Windows**, vaya a **Protección de la red** > **Cortafuegos** > **Básico** y aplique toda la configuración mediante la marca **Aplicar**. Despliegue la sección **Asignar** y seleccione el grupo estático *San Diego*.

Resultado

Las políticas creadas por el *administrador* se aplicarán primero porque se han asignado al grupo *Todo*. La configuración con el indicador **Forzar** tiene prioridad, y ninguna política posterior puede sobrescribirla. A continuación, se aplicarán las políticas creadas por el usuario *John*.

Desplácese hasta **Más** > **Grupos** > **San Diego**, haga clic en el ordenador y seleccione **Detalles**. En **Configuración** > **Políticas aplicadas** está el orden final de aplicación de políticas.

ORDEN...	PRODUCTO DE ...	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 creó el *administrador* y la segunda, la creó el usuario *John*.

Grupo de inicio – El grupo de inicio 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 derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "Department_1" como **grupo de inicio** de la tarea del cliente.

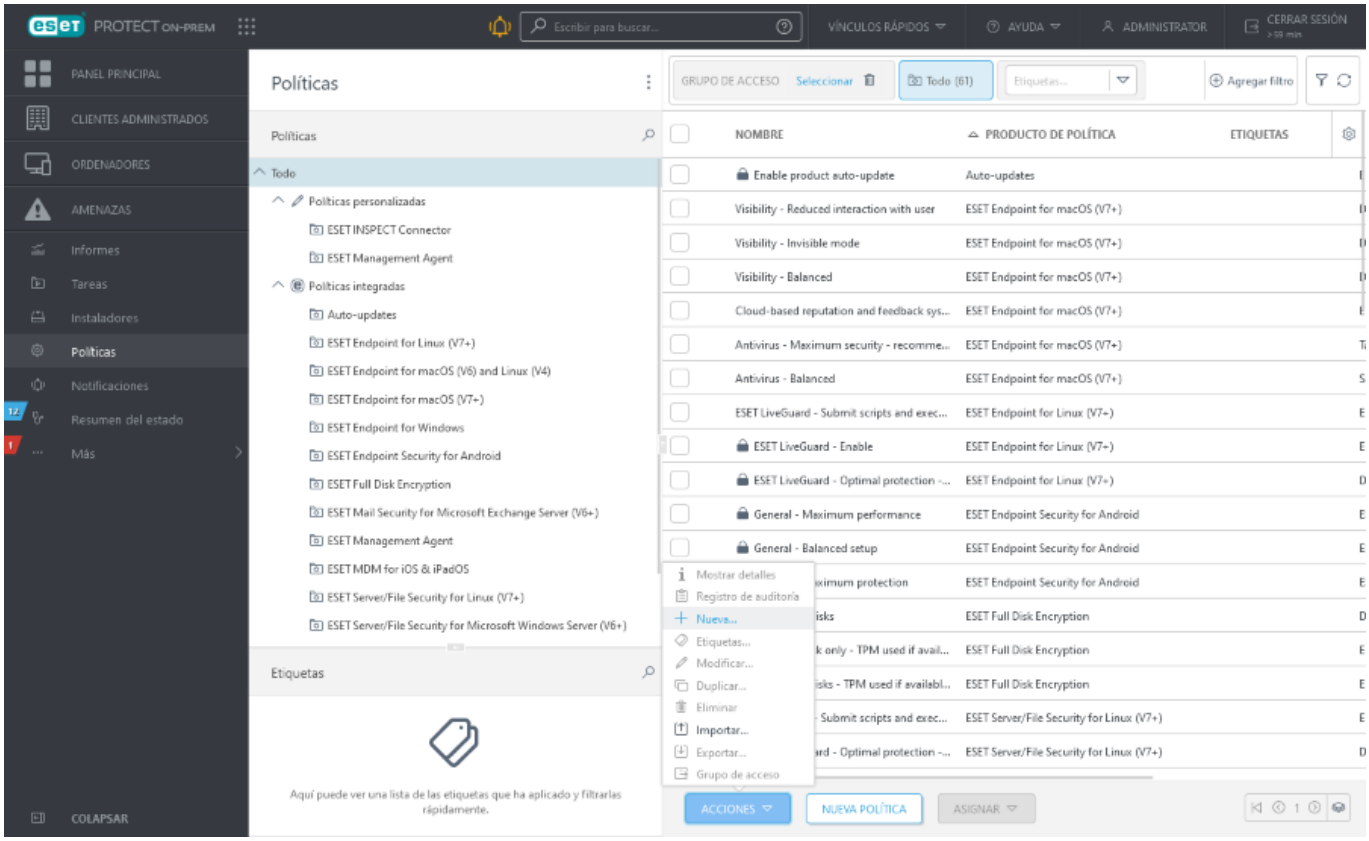
Si el grupo de inicio preseleccionado no cumple sus expectativas, puede seleccionar uno manualmente.

Administrar políticas

Las políticas se agrupan o clasifican por producto de ESET. **Políticas integradas** contiene las políticas predefinidas y personalizadas, y muestra las categorías de todas las políticas que ha creado o modificado manualmente.

Acciones disponibles para las políticas:

Mostrar detalles	muestra detalles de la política.
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Nuevo	Crear una política nueva.
Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Modificar...	Modificar una política existente.
Duplicar	Crear una nueva política a partir de una política existente que ha seleccionado. Para duplicar una política es necesario un nuevo nombre.
Cambiar asignaciones	Asignar una política a un grupo o un cliente.
Eliminar	Eliminar una política. Consulte también las reglas de eliminación de políticas.
Importar	Haga clic en **Políticas** > **Importar**, haga clic en **Elegir archivo** y busque el archivo que quiera importar. Solo puede importar un archivo *.dat* que contenga las políticas exportadas desde la Consola web de ESET PROTECT. No puede importar un archivo *.xml* que contenga las políticas exportadas desde el producto de seguridad de ESET. Las políticas importadas aparecerán en **Políticas personalizadas**.
Exportar	Marque en la lista las casillas de verificación situadas junto a las políticas que quiera exportar y haga clic en **Acciones** > **Exportar**. Las políticas se exportarán 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 suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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

Los grupos y los ordenadores pueden tener varias políticas asignadas. Además, un ordenador puede estar en un grupo anidado a mucha profundidad, y sus grupos principales tener sus propias políticas.

A la hora de aplicar las políticas, el aspecto más importante es el orden. Este se deriva del orden del grupo y del orden de las políticas asignadas al grupo.

Para ver todas las políticas aplicadas a un ordenador seleccionado, consulte Políticas aplicadas en los detalles del ordenador.

Siga los pasos indicados a continuación para determinar la política activa de cualquier cliente:

1. Buscar el orden de los grupos en el que reside el cliente
2. Sustituir los grupos con las políticas asignadas
3. Combine políticas para obtener los ajustes finales

Orden de los grupos

Las políticas pueden asignarse a grupos, **y se aplican en un orden determinado. Las reglas escritas a continuación determinan el orden en el que se aplican las políticas a los clientes**.

Regla 1: Los grupos estáticos se recorren desde el grupo estático raíz (**Todo**).

Regla 2: En cada nivel, los grupos estáticos de dicho nivel se recorren en primer lugar siguiendo el orden en el que aparecen en el árbol (esto también se denomina búsqueda "en anchura").

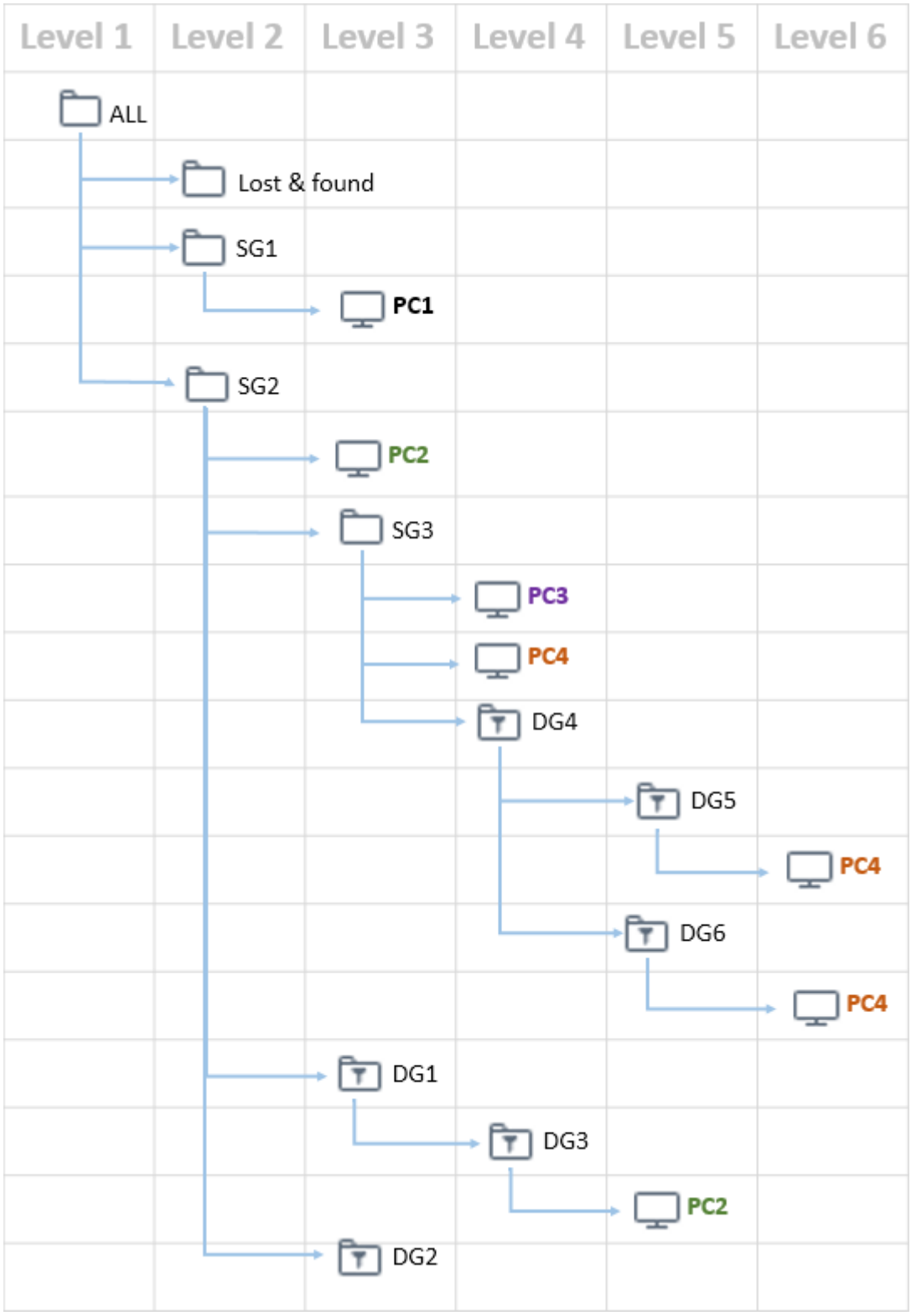
Regla 3: Cuando se han contabilizado todos los grupos estáticos de un nivel concreto, se recorren los grupos dinámicos.

Regla 4: En cada grupo dinámico, se recorren todos sus grupos secundarios en el orden en el que aparecen en la lista.

Regla 5: A cualquier nivel de un grupo dinámico, se enumerarán los grupos secundarios y se buscarán sus grupos secundarios. Cuando ya no hay más grupos secundarios, se enumeran los siguientes grupos dinámicos al nivel principal (esto también se denomina búsqueda "en profundidad").

Regla 6: El recorrido finaliza en un ordenador.

La política se aplica al ordenador. Esto significa que el recorrido finaliza en el ordenador en el que quiere aplicar la política.



Utilizando las reglas escritas anteriormente, el orden en el que se aplicarán las políticas en cada ordenador sería el siguiente:

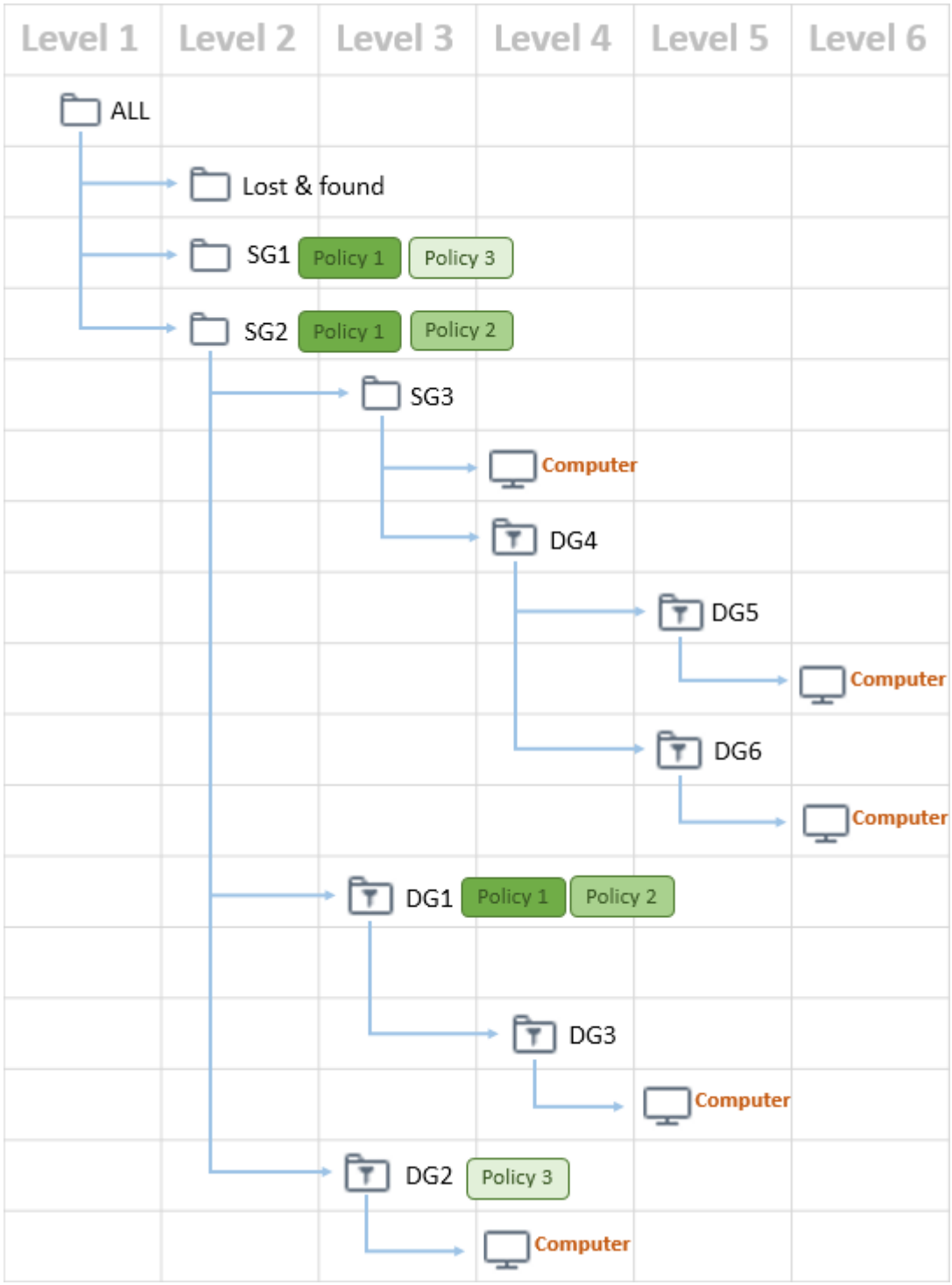
PC1:	PC2:	PC3:	PC4:
1.ALL 2.SG1 3.PC1	1.ALL 2.SG2 3.DG1 4.DG3 5.PC2	1.ALL 2.SG2 3.SG3 4.PC3	1.ALL 2.SG2 3.SG3 4.DG4 5.DG5 6.DG6 7.PC4

Enumeración de políticas

Una vez se conoce el orden de los grupos, el próximo paso consiste en sustituir cada grupo con las políticas que tiene asignado. Las políticas aparecen en el mismo orden en el que están asignadas al grupo. Es posible editar la prioridad de las políticas de un grupo que tiene más políticas asignadas. Cada política configura solo un producto (agente ESET Management, ESET Endpoint Security, etc.).

Si un grupo no tiene ninguna política, se quita de la lista.

Tenemos tres políticas aplicadas a los grupos estáticos y dinámicos (consulte la siguiente ilustración):



El orden en el que se aplicarán las políticas en el ordenador

La siguiente lista muestra grupos y políticas aplicadas en ellos:

1.Todo -> eliminado, sin política

2.GE 2 -> Política 1, Política 2

3.GE 3 -> eliminado, sin política

4.GD 1 – Política 1, Política 2

5.GD 3 – eliminado, sin política

6.GD 2 – Política 1, Política 3

7.GD 4 – eliminado, sin política

8.GD 5 – eliminado, sin política

9.GD 6 – eliminado, sin política

10. Ordenador -> eliminado, sin política

La lista final de políticas es la siguiente:

1.Política 1

2.Política 2

3.Política 1

4.Política 2

5.Política 3

Fusión de políticas

Cuando aplica una política a un producto de seguridad de ESET en el que ya se ha aplicado otra política, se combinan los ajustes de la política que se superponen. Las políticas se fusionan de una en una. Al fusionar políticas, la regla general es que la política más reciente siempre sustituye la configuración establecida por la más antigua. Si desea cambiar este comportamiento, puede usar los indicadores de política (disponibles para todos los ajustes). Algunos ajustes tienen otra regla (sustituir/anexar/anteponer) que puede configurar.

Tenga en cuenta que la estructura de los grupos (su jerarquía) y la secuencia de las políticas determinan el método de fusión de las políticas. La fusión de dos políticas podría tener resultados distintos, en función del orden de aplicación.

Al crear políticas, notará que algunos ajustes tienen reglas adicionales que puede configurar. Estas reglas le permiten realizar los mismos ajustes en distintas políticas.

- **Sustituir**: la regla predeterminada que se utiliza al fusionar políticas. Sustituye los ajustes configurados por la política anterior.

- **Añadir**: al aplicar la misma configuración en más de una política, puede añadir la configuración con esta regla. El ajuste se anexará al final de la lista creada fusionando políticas.

- **Anteponer**: al aplicar la misma configuración en más de una política, puede anteponer la configuración con esta regla. El ajuste se incluirá al principio de la lista creada fusionando políticas.

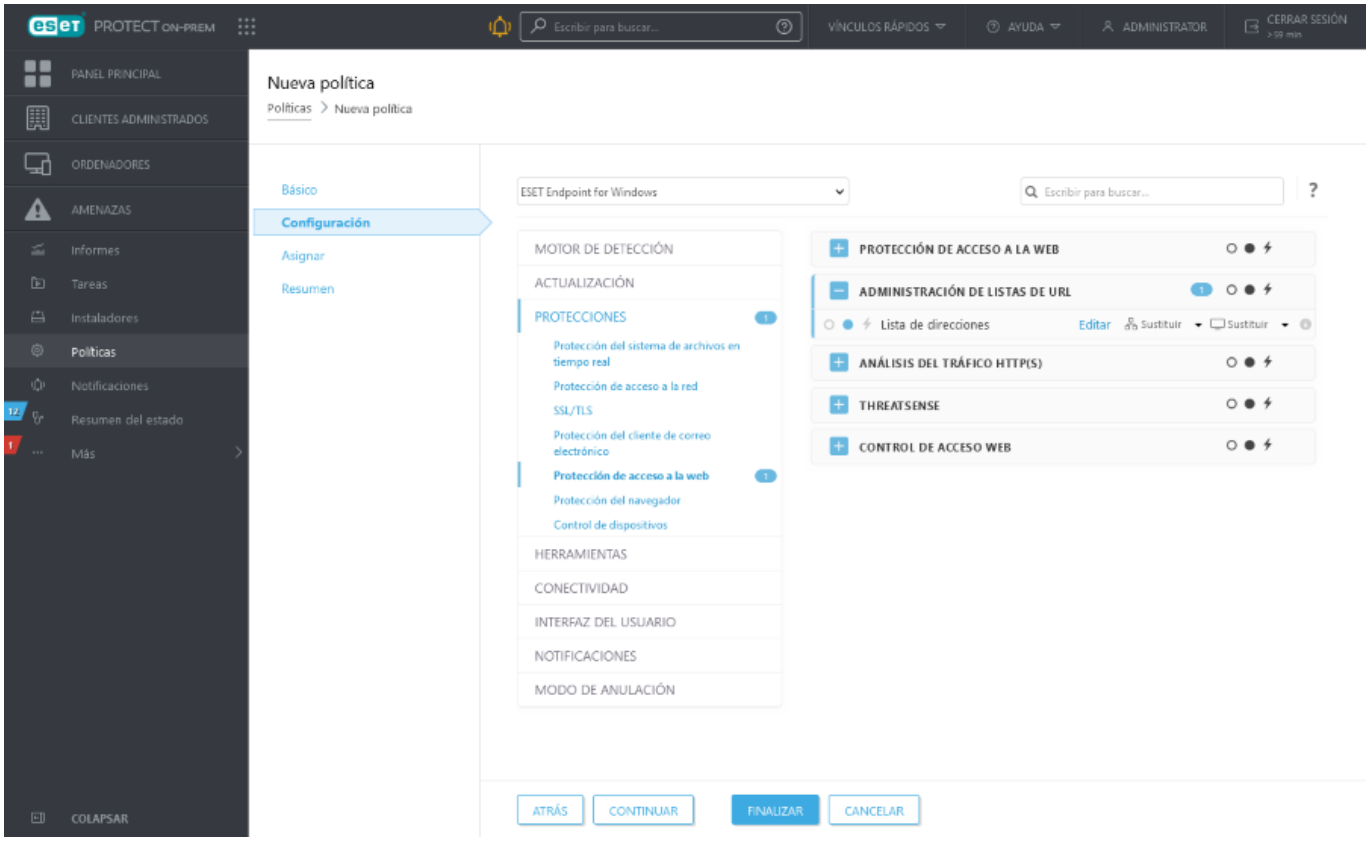
Fusión de listas locales y remotas

Los productos de seguridad de ESET recientes (consulte las versiones compatibles en la tabla que aparece a continuación) permiten fusionar configuraciones locales con las políticas remotas de una nueva forma. Si la configuración es una lista (por ejemplo, una lista de sitios web) y una política remota entra en conflicto con una configuración local existente, la política remota la sobrescribe. Puede elegir cómo combinar listas locales y

remotas. Puede seleccionar diferentes reglas de fusión para:

- Fusionar configuraciones para políticas remotas.
- Fusionar políticas remotas y locales y configuraciones locales con la política remota resultante.

Las opciones son las mencionadas anteriormente: **Sustituir**, **Anexar** y **Anteponer**.



Consulte también las reglas de eliminación de políticas.

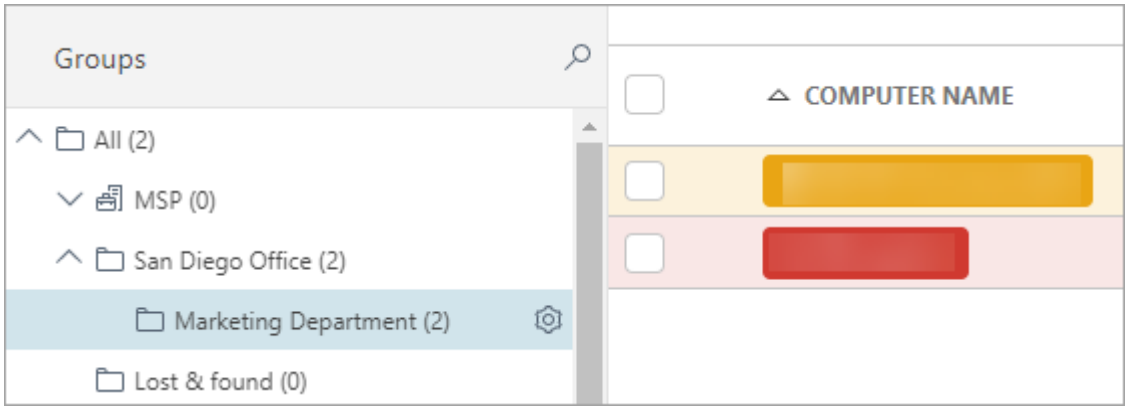
Situación hipotética de fusión de políticas

Este ejemplo describe:

- Instrucciones sobre cómo aplicar ajustes de políticas a productos de seguridad ESET Endpoint
- Cómo se fusionan las políticas cuando se aplican indicadores y reglas

Cuando el *administrador* quiere:

- Denegar el acceso a *Oficina de San Diego* a los sitios web *www.forbidden.uk, www.deny-access.com, www.forbidden-websites.uk* y *www.forbidden-website.com*
- Permitir el acceso a *Departamento de marketing* a los sitios web *www.forbidden.uk* y *www.deny-access.com*



El *administrador* debe seguir estos pasos:

1. Crear el nuevo grupo estático *Oficina de San Diego* y, a continuación, crear *Departamento de marketing* como subgrupo del grupo estático *Oficina de San Diego*.

2. Desplazarse hasta **Políticas** y crear una nueva política como se indica a continuación:

   i)Llamarla *Oficina de San Diego*.

   ii)Desplegar **Configuración** y seleccionar **ESET Endpoint para Windows**

   iii)Ir a **Protecciones** > **Protección de acceso a la web** > **Administración de listas de URL**

   iv)Hacer clic en el botón **Aplicar** política y modificar **Lista de direcciones** haciendo clic en **Modificar**

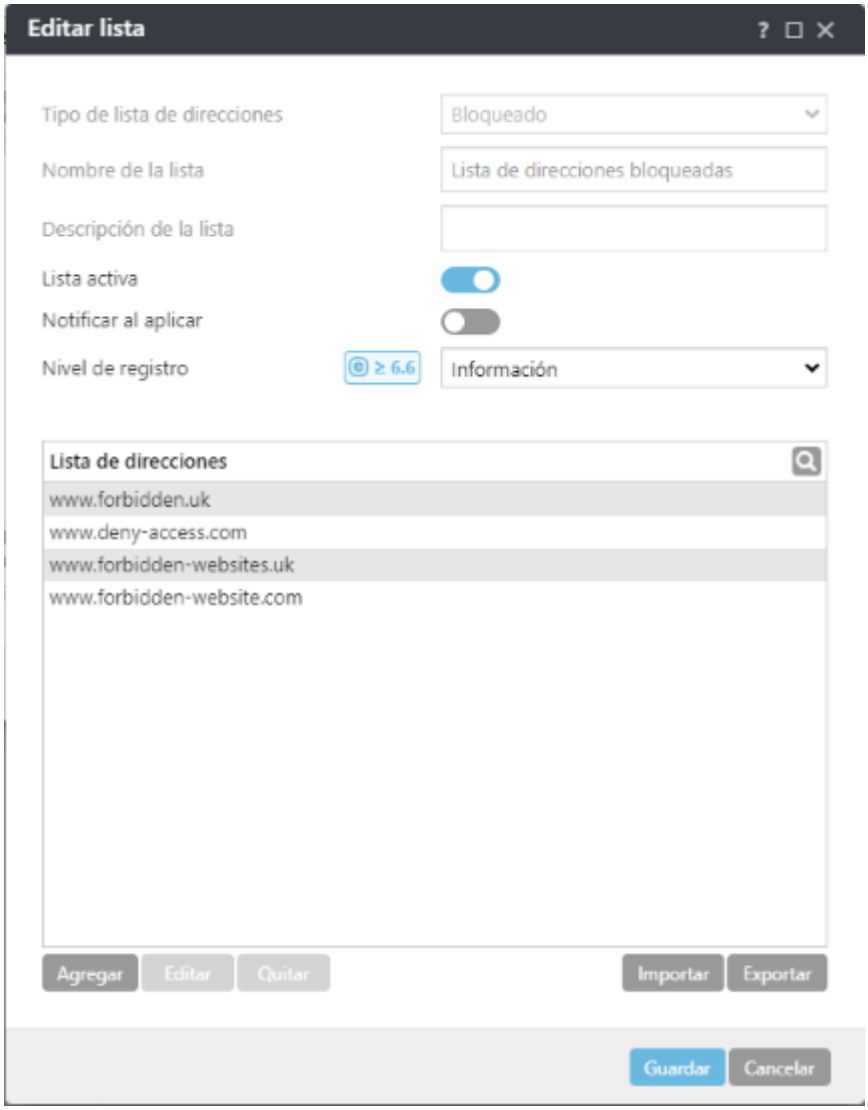
   v)Hacer clic en **Lista de direcciones bloqueadas** y seleccionar **Modificar**.

   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, a continuación, la lista de direcciones.

   vii) Desplegar **Asignar** y asignar la política a *Oficina de San Diego* y a su subgrupo *Departamento de marketing*.

   viii) Haga clic en **Finalizar** para guardar la política.

Esta política se aplicará a *Oficina de San Diego* y a *Departamento de marketing* y bloqueará los sitios web como se indica a continuación.

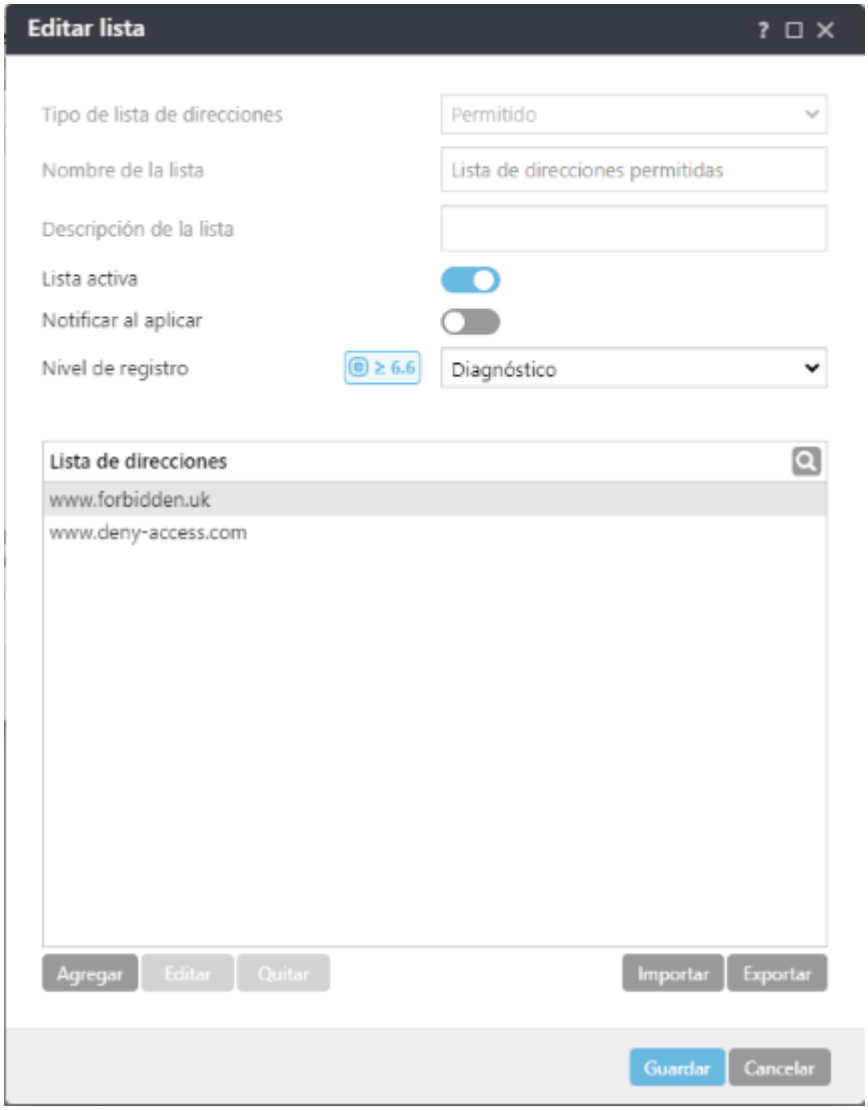


3. Desplazarse hasta **Políticas** y crear una nueva política:

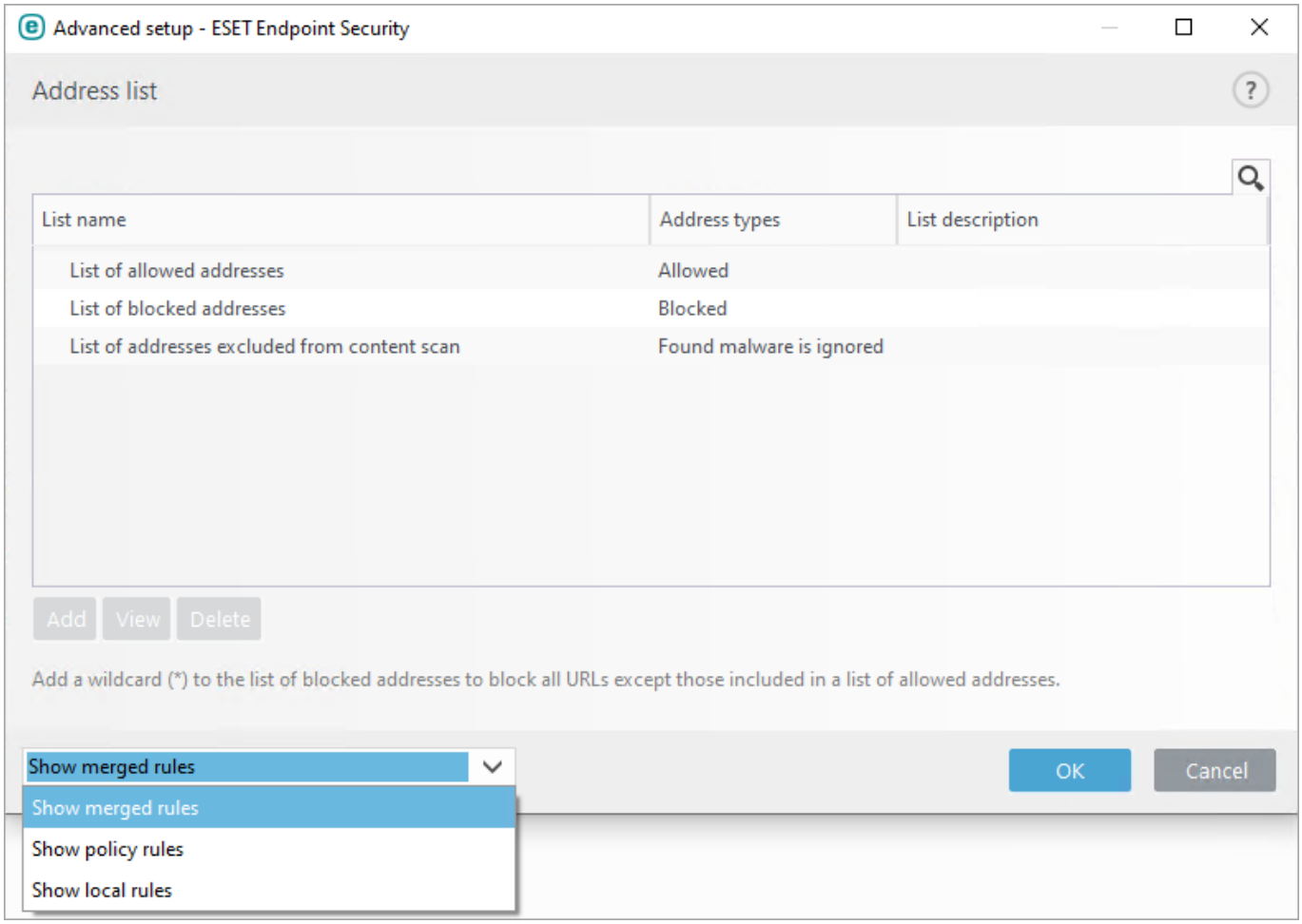
i)Llamarla *Departamento de marketing*.
ii)Desplegar **Configuración** y seleccionar **ESET Endpoint para Windows**
iii)Ir a **Protecciones** > **Protección de acceso a la web** > **Administración de listas de URL**
iv)Hacer clic en el botón para **Aplicar** la política, seleccionar la regla Anexar y luego modificar la **Lista de direcciones** haciendo clic en **Modificar** La regla Anexar causa que la lista de direcciones se coloque al final al fusionar políticas.
v)Hacer clic en **Lista de direcciones permitidas** > **Modificar**.
vi)Agregar las siguientes direcciones web: *www.forbidden.uk* y *www.deny-access.com*. Guardar la lista de direcciones permitidas y, a continuación, la lista de direcciones.
vii) Desplegar **Asignar** y asignar la política a *Departamento de marketing*

viii) Haga clic en **Finalizar** para guardar la política.

Esta política se aplicará a *Departamento de marketing* y otorgará acceso a los sitios web como se muestra a continuación.



4. La política final incluirá las dos políticas aplicadas a *Oficina de San Diego* y *Departamento de marketing*. Abra **ESET Endpoint Security** y vaya a **Configuración** > **Configuración avanzada** > **Protecciones** > **Protección de acceso a la web** > expanda **Administración de listas de URL**. Se mostrará la configuración final del producto Endpoint.



La configuración final incluye:

- Lista de direcciones de la política *Oficina de San Diego*
- Lista de direcciones de la política *Departamento de marketing*

Configuración de un producto desde ESET PROTECT On-Prem

Puede utilizar las políticas para configurar su producto ESET de la misma forma que lo haría en la ventana Configuración avanzada de la interfaz gráfica de usuario del producto. A diferencia de las políticas de Active Directory, las políticas de ESET PROTECT On-Prem no pueden contener scripts ni series de comandos.

En la versión 6 y en versiones más recientes de los productos de ESET puede configurar que se informe de determinados estados en el cliente o en Web Console. Esto se configura en una política para el producto v6 dentro de **Interfaz de usuario** > **Elementos de la interfaz de usuario** > **Estados**:

- **Mostrar**: se informa del estado en la GUI del cliente.
- **Enviar**: se informa del estado a ESET PROTECT On-Prem.

Ejemplos de uso de políticas para configurar productos de ESET:

- Configuración de política de ESET Management Agent

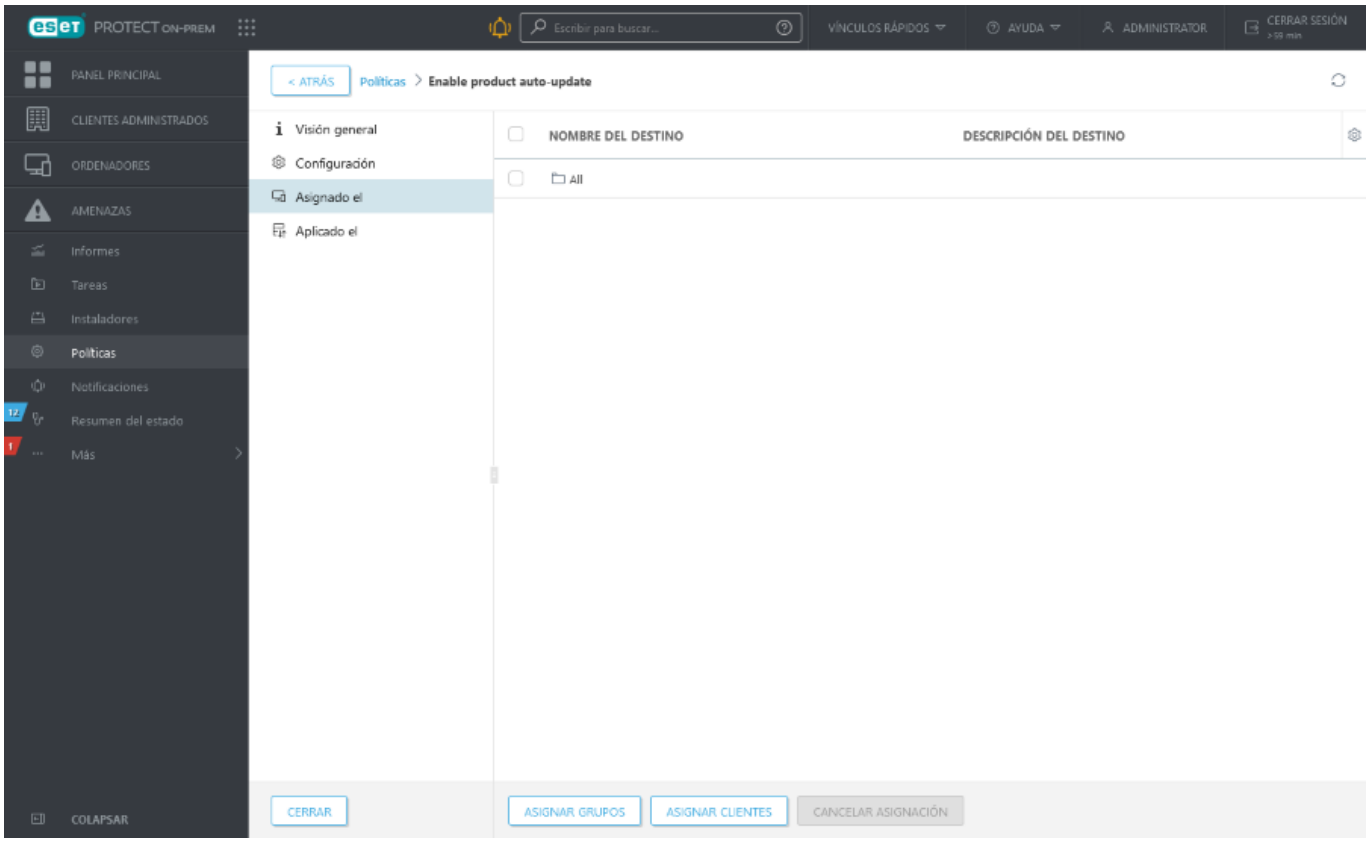
- Configuración de políticas de ESET Rogue Detection Sensor
- Crear una directiva para el MDM de iOS: cuenta de Exchange ActiveSync
- Crear una directiva para que MDC active APNS para la inscripción de iOS

Asignar una directiva a un grupo

Después de crear una política, puede asignarla a un **grupo estático** o **dinámico**. Hay dos formas de asignar una política:

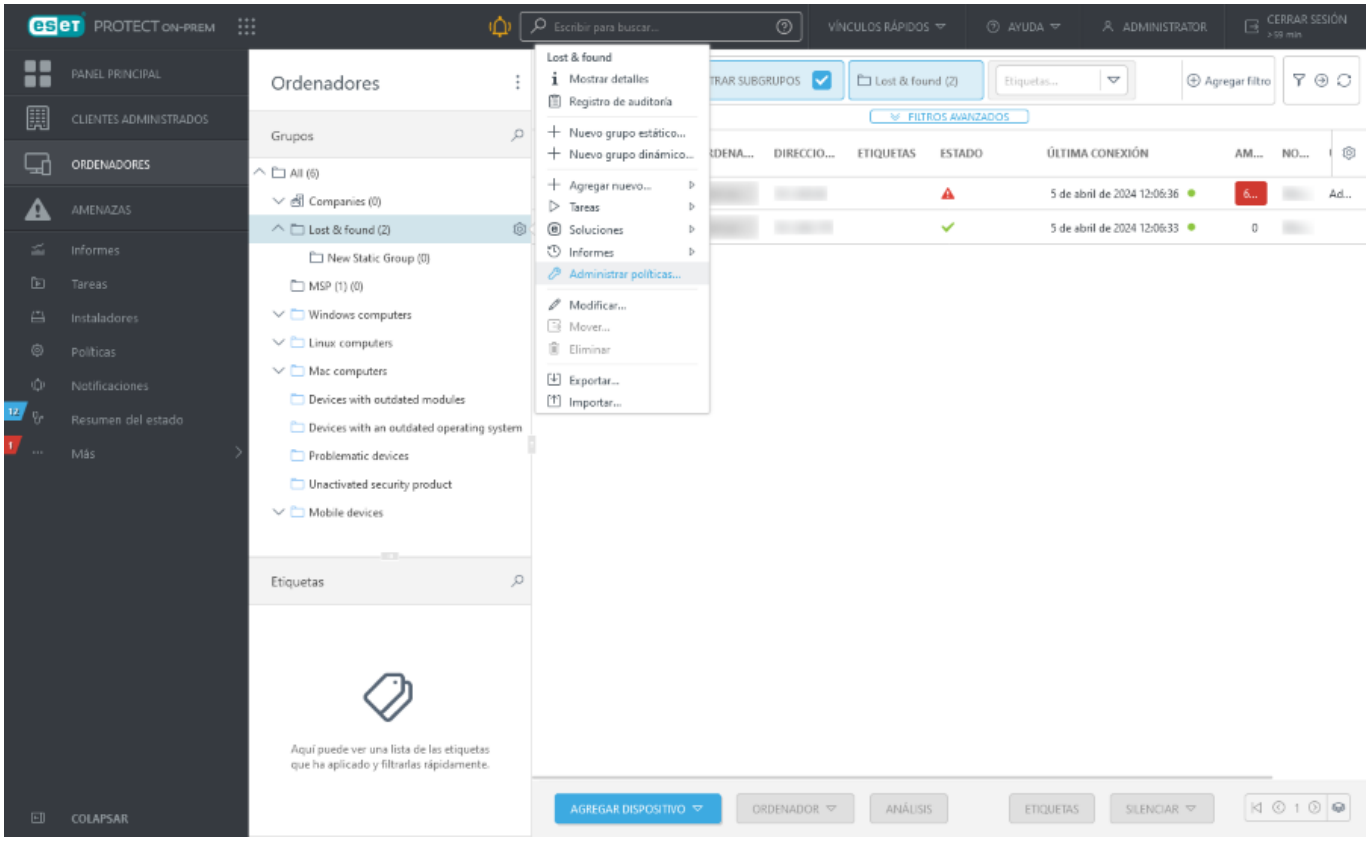
Método I.

En **Políticas**, seleccione una política y haga clic en **Acciones** > **Mostrar detalles** > **Asignado el** > **Asignar grupos**. Seleccione un grupo estático o dinámico en la lista (puede seleccionar más grupos) y haga clic en **Aceptar**.



Método II.

1. Haga clic en **Ordenadores**, haga clic en el icono del engranaje junto al nombre del grupo y seleccione **Administrar políticas**.



2. En la ventana **Orden de aplicación de directiva** haga clic en **Agregar directiva**.

3. Marque la casilla de verificación situada junto a la política que desea asignar a este grupo y haga clic en **Aceptar**.

4. Haga clic en **Cerrar**.

Para ver qué políticas están asignadas a un grupo determinado, seleccione ese grupo y haga clic en la ficha **Políticas** para ver una lista de políticas asignadas al grupo.

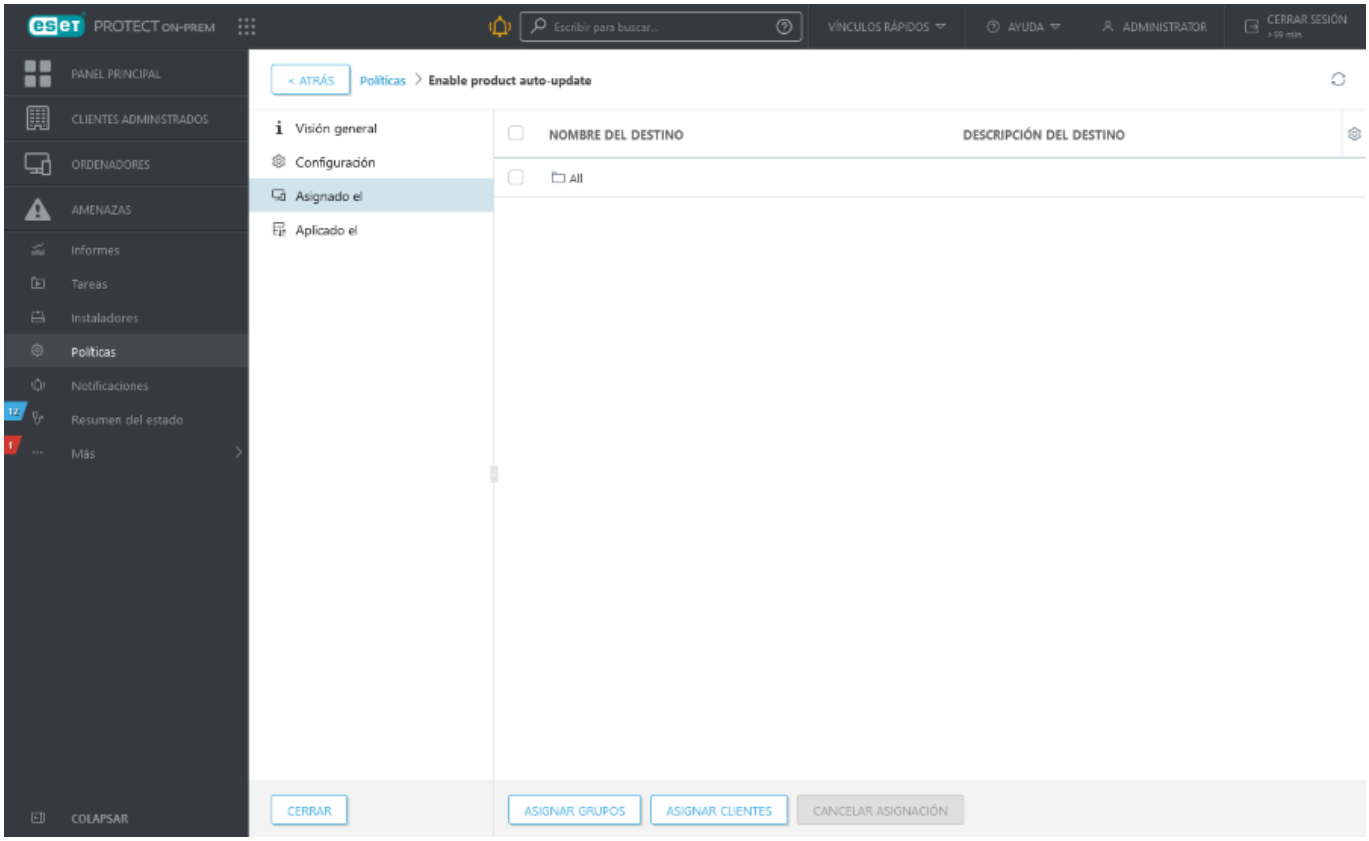
Para ver qué grupos están asignados a una política concreta, seleccione la política y haga clic en **Mostrar detalles** > **Aplicada a**.

para obtener más información acerca de las políticas, consulte el capítulo Políticas.

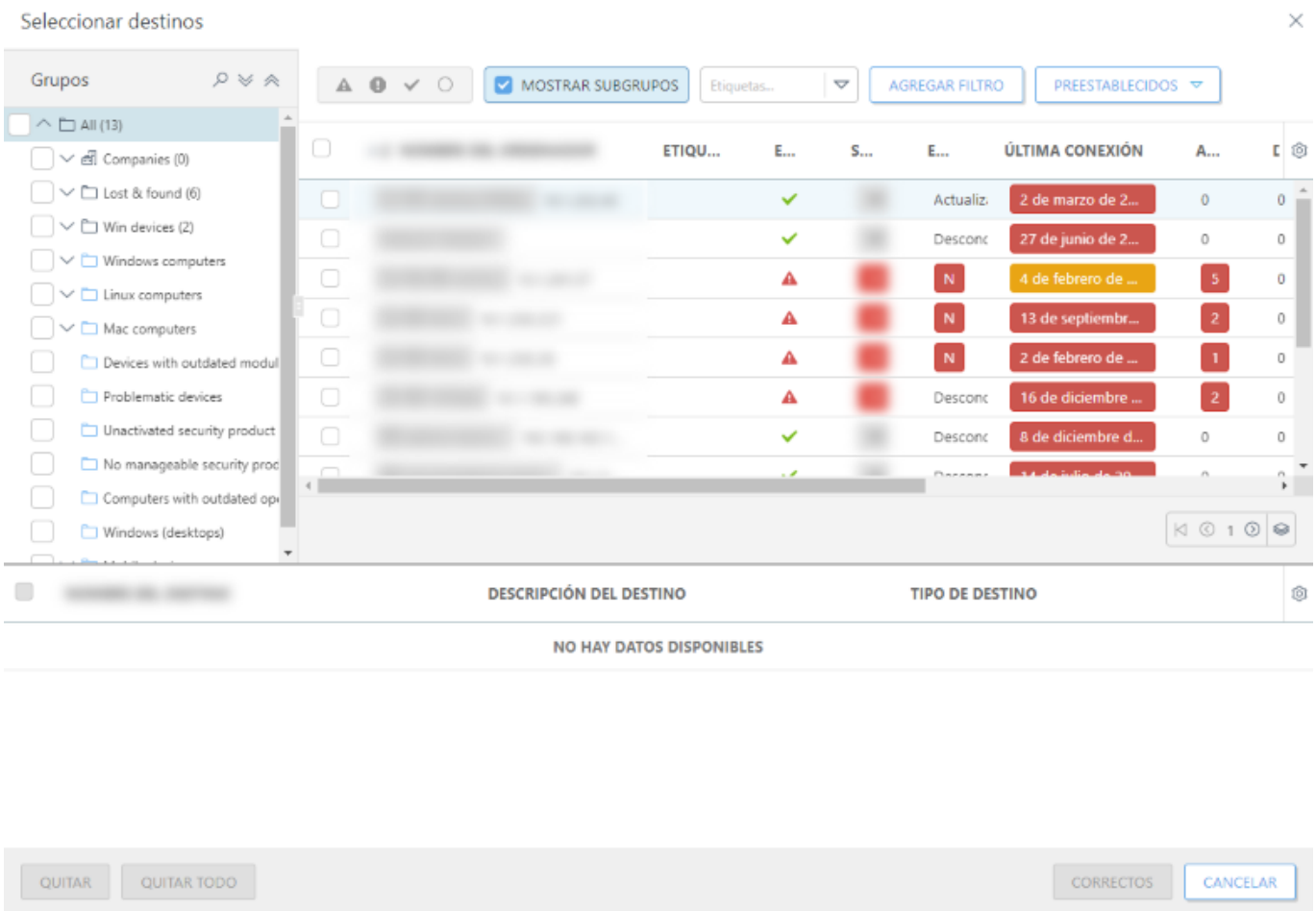
Asignar una política a un cliente

Para asignar una política a una estación de trabajo cliente, haga clic en **Políticas**, seleccione una política y haga clic en **Acciones** > **Mostrar detalles** > **Asignado a** > **Asignar clientes**.

Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Seleccione los ordenadores cliente y haga clic en **Aceptar** y la política se aplicará a todos los ordenadores que haya seleccionado.



Para ver qué clientes están asignados a una política concreta, seleccione la política y consulte la primera ficha, **Asignado a**.

Cómo utilizar el modo de anulación

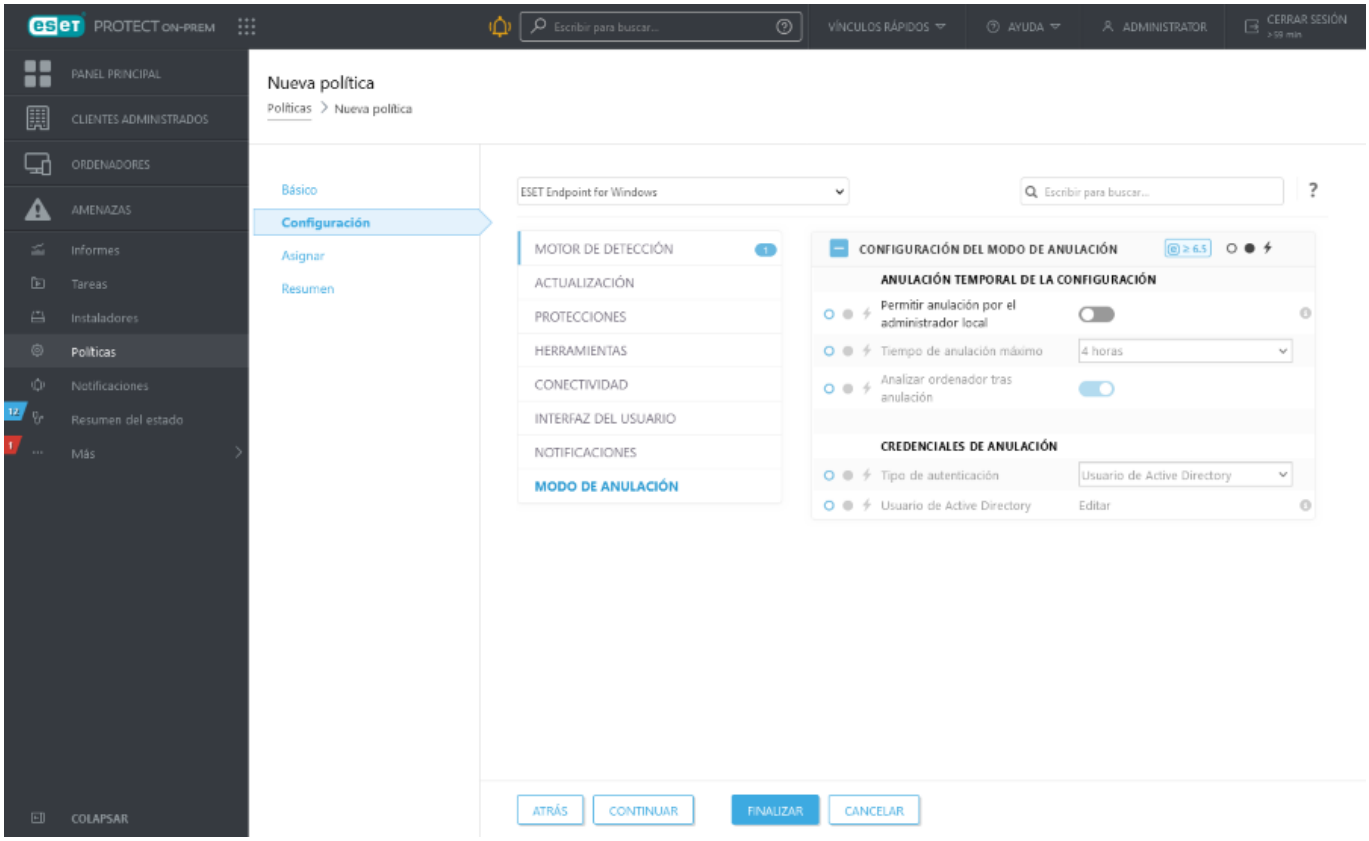
Los usuarios con productos ESET Endpoint para Windows instalados en sus máquinas podrán utilizar la función de anulación. Puede activar el modo de anulación solo de forma remota desde ESET PROTECT Web Console. El modo de anulación permite a los usuarios de nivel de ordenador cliente cambiar la configuración del producto ESET instalado, incluso si hay una política aplicada a dicha configuración. El modo de anulación puede activarse para usuarios de AD o protegerse mediante contraseña. La función no puede activarse durante más de cuatro horas.

Limitaciones del modo de anulación

- El modo de anulación no puede detenerse desde ESET PROTECT Web Console una vez activado. La anulación solo se desactiva cuando transcurre el tiempo de anulación, o cuando se desactiva en el propio cliente.
- El usuario que utiliza el modo de anulación también debe tener derechos de administrador de Windows. De lo contrario, dicho usuario no podrá guardar los cambios realizados en la configuración del producto de ESET.
- La autenticación de grupos de Active Directory está permitida para 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 configurar el **Modo de anulación**:

1. Vaya a **> Políticas** > **Nueva política**.
2. En la sección **Básico**, escriba un **Nombre** y una **Descripción** para esta política.
3. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
4. Haga clic en **Modo de anulación** y configure reglas para el modo de anulación.
5. En la sección **Asignar**, seleccione el ordenador o el grupo de ordenadores a los que se aplicará esta política.
6. Revise la configuración en la sección **Resumen** y haga clic en **Finalizar** para aplicar la política.



Si *John* tiene un problema porque la configuración de Endpoint está bloqueando algunas funciones importantes o el acceso web en su máquina, el Administrador podrá permitir que *John* anule su política de Endpoint existente y ajuste la configuración manualmente en su máquina. Después ESET PROTECT On-Prem podrá solicitar la nueva configuración, por lo que el Administrador podrá crear una nueva política a raíz de la misma.

Para hacerlo, siga estos pasos:

1.Vaya a **> Políticas** > **Nueva política**.

2.Complete los campos **Nombre** y **Descripción**. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.

3.Haga clic en **Modo de anulación**, active el modo de anulación durante una hora y seleccione *John* como usuario de AD.

4.Asigne la política al *Ordenador de John* y haga clic en **Finalizar** para guardar la política.

5.*John* deberá activar el **Modo de anulación** en su ESET Endpoint y cambiar la configuración manualmente en su máquina.

6.En ESET PROTECT Web Console, vaya a **Ordenadores**, seleccione *Ordenador 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 del cliente lo antes posible.

8.Poco después aparecerá la nueva configuración. Haga clic en el producto cuya configuración desea guardar y, a continuación, haga clic en **Abrir configuración**.

9.Puede revisar la configuración y, a continuación, hacer clic en **Convertir en política**.

10. Complete los campos **Nombre** y **Descripción**.

11. En la sección **Configuración**, puede modificar la configuración en caso necesario.

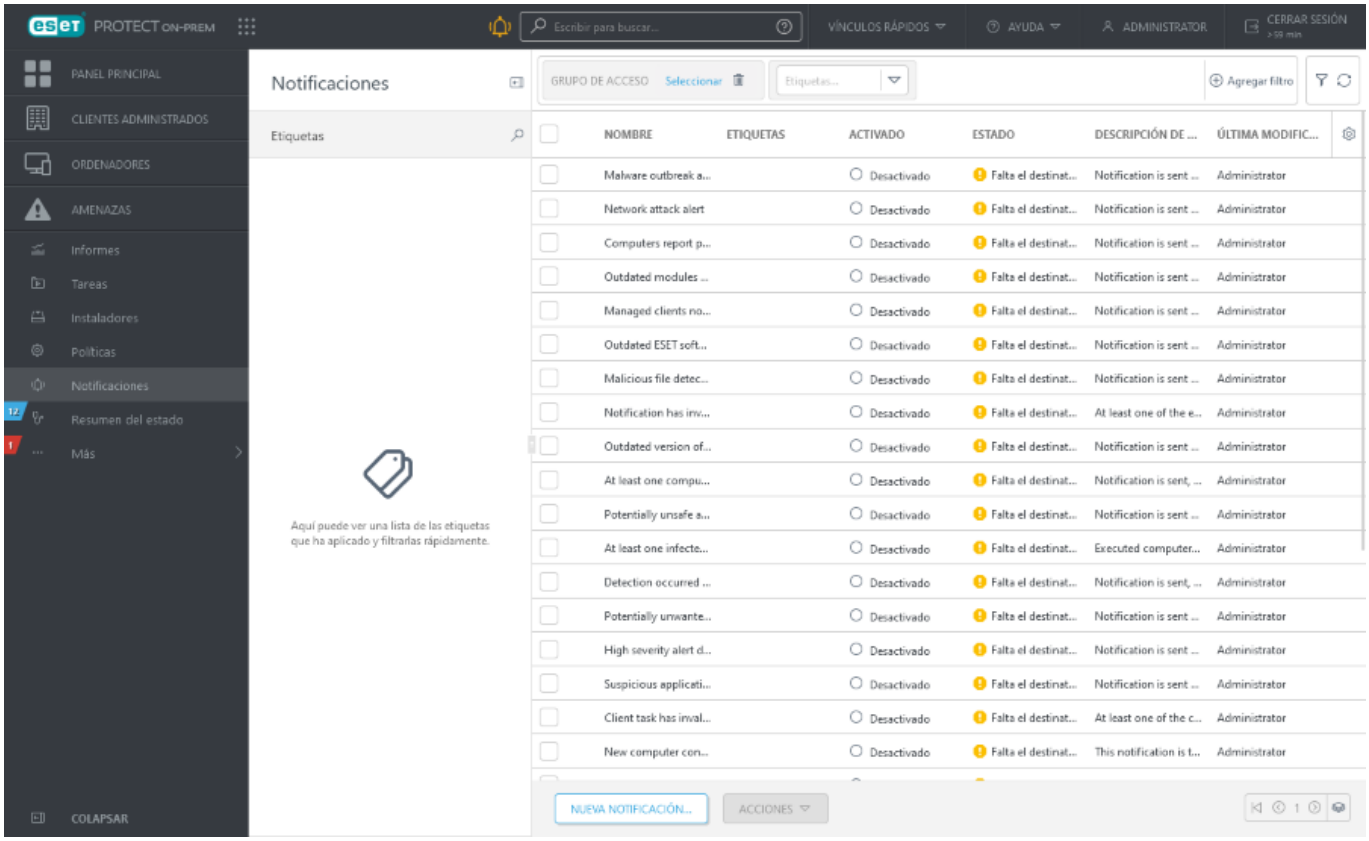
12. En la sección **Asignar**, puede asignar esta política al *Ordenador de John* (o a otros).

13. Haga clic en **Finalizar** para guardar la configuración.

14. No olvide eliminar la política de anulación cuando ya no la necesite.

Notificaciones

Las **notificaciones** son vitales para mantener el estado general de la red. Cuando se produzca un nuevo evento (y según la configuración de notificaciones), se le informará de él por medio del método definido (mediante una captura de SNMP, un mensaje de correo electrónico o un envío al servidor syslog) para que pueda responder debidamente. Puede configurar notificaciones automáticas basadas en eventos concretos como detecciones, instancias de Endpoint no actualizadas, etc. Consulte la descripción de la notificación para obtener más información sobre una notificación específica y su desencadenador.



Si desea crear una notificación nueva, haga clic en **Nueva notificación** en la parte inferior de la página.

Seleccione una notificación y haga clic en **Acciones** para gestionar la notificación.

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

Notificaciones, usuarios y permiso

El uso de Notificaciones está restringido por los permisos del usuario actual. Cada vez que se ejecuta la notificación, hay un usuario ejecutante cuyos permisos se tienen en cuenta. El usuario ejecutante es siempre el que modificó por última vez la notificación. El usuario solo puede ver las notificaciones contenidas en grupos en los que tenga permisos de **Lectura**.

Para que una notificación funcione bien, es necesario que el usuario ejecutante tenga permisos suficientes en todos los objetos a los que se hace referencia (dispositivos, grupos y plantillas). Normalmente, son necesarios permisos de **Lectura** y **Uso**. Si el usuario no tiene estos permisos, o si los pierde posteriormente, la notificación fallará. Las notificaciones que fallen se resaltarán y desencadenarán un mensaje de correo electrónico para notificar al usuario.

Crear notificación: el usuario debe tener permisos de **Escritura** sobre las notificaciones de su grupo de inicio. Las nuevas notificaciones se crean en el grupo principal del usuario.

Modificar notificación: el usuario debe tener permisos de **Escritura** sobre las notificaciones del grupo en el que se encuentre dicha notificación.

Quitar notificación: el usuario debe tener permisos de **Escritura** sobre las notificaciones del grupo en el que se encuentre dicha notificación.

John, cuyo **Grupo principal** es *Grupo de John*, quiere quitar (o modificar) la *Notificación 1*. La notificación la creó *Larry*, por lo que está en el grupo principal de Larry, *Grupo de Larry*. Deben cumplirse las siguientes condiciones para que *John* pueda quitar (o modificar) la *Notificación 1*:
• *John* debe tener asignado un conjunto de permisos en el que se incluyan permisos de **Escritura** sobre las **notificaciones**
• El conjunto de permisos debe contener *Grupo de Larry* en **Grupos estáticos**

Grupo de inicio – El grupo de inicio 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 derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "Department_1" como **grupo de inicio** de la tarea del cliente.

Si el grupo de inicio preseleccionado no cumple sus expectativas, puede seleccionar uno manualmente.

Clonación y VDI

Hay tres notificaciones preparadas para notificar al usuario eventos relacionados con la clonación. El usuario también puede crear una nueva notificación personalizada.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Administrar notificaciones

Las notificaciones se administran desde la sección **Notificaciones**. Puede realizar las siguientes acciones:

- Haga clic en **Nueva notificación** para crear una nueva notificación.
- Haga clic en una notificación y seleccione una acción en el menú desplegable:

Mostrar detalles	muestra detalles de la notificación, como su configuración y los parámetros de distribución. Haga clic en **Ver vista previa del mensaje** para ver una vista previa de la notificación.
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Activar / Desactivar	Cambie el estado de la notificación. Las notificaciones desactivadas no se evalúan. Todas las notificaciones están configuradas como **Desactivada** de forma predeterminada.
Modificar...	Configure los ajustes y la distribución de la notificación.
Duplicar	Crea una notificación duplicada en el grupo principal.
Eliminar	Quita la notificación.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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.

Nueva notificación

Básico

Escriba un **Nombre** y una **Descripción** para su notificación de forma que resulte más sencillo filtrar las distintas notificaciones.

Si está editando una notificación activada y desea desactivar la notificación, haga clic en el conmutador de alternancia y su estado cambiará a **Deshabilitado** .

Configuración

Evento – Hay tres tipos básicos de evento que pueden desencadenar una notificación. Cada tipo de evento ofrece opciones distintas en la sección **Configuración**. Seleccione uno de los siguientes tipos de evento:

- Sucesos en ordenadores o grupos administrados
- Cambios de estado del servidor
- Cambios en el grupo dinámico

Configuración avanzada: límites

Los límites le permiten configurar reglas avanzadas que determinan cuándo se desencadena una notificación. Consulte la sección de límites para obtener más información.

Distribución

Configure los ajustes de distribución de notificaciones. Configure su servidor SMTP si desea enviar las notificaciones por correo electrónico.

Sucesos en ordenadores o grupos administrados

Esta opción se usa para notificaciones no asociadas a un grupo dinámico pero basadas en sucesos del sistema filtrados del registro de sucesos. Seleccione la categoría de registro en la que estará basada la notificación y un operador lógico para los filtros.

Categoría: elija entre las siguientes categorías de evento:

- **Detección de cortafuegos**
- **Detección antivirus**
- **Análisis**
- **HIPS**
- **ESET Inspect alertas**
- **Archivo bloqueado**
- **Ordenador conectado en primer lugar**
- **Identidad del ordenador recuperada**
- **Pregunta de clonación de ordenador creada**
- **Nuevo cliente de MSP encontrado**

Los eventos disponibles en **Configuración** > **Filtrar por** varían en función de la categoría seleccionada. Los valores de los filtros se comparan directamente con los eventos enviados por los clientes. No hay una lista definida de valores disponibles.

Grupos estáticos supervisados: haga clic en **Seleccionar** o **Crear nuevo grupo** y seleccione los grupos estáticos para limitar los dispositivos supervisados sobre los que desea recibir una notificación. Si no selecciona ningún grupo estático, recibirá notificaciones sobre todos los dispositivos a los que tenga acceso.

Omitir dispositivos silenciados: si marca esta casilla de verificación, no recibirá notificaciones de ordenadores silenciados (los ordenadores silenciados se excluirán de las notificaciones).

Configuración

En **Configuración**, seleccione un **Operador** y valores para el filtro (**Filtrar por**). Solo se puede seleccionar un operador, y se evaluarán juntos todos los valores con ese operador. Haga clic en **Agregar filtro** para agregar un nuevo valor para el filtro.

El contenido del mensaje predeterminado tiene un propósito informativo y no se puede personalizar. Puede personalizar el mensaje enviado mediante una notificación en la sección Distribución.

Cambios de estado del servidor

Esta opción le informa de cambios de estado del objeto. El intervalo de notificación depende de la **Categoría** seleccionada. Puede seleccionar una de las configuraciones existentes o configurar sus propios parámetros.

Cargar configuraciones preestablecidas: haga clic en Seleccionar para elegir una de las configuraciones existentes o déjelo en blanco. Haga clic en Borrar para borrar la sección Configuración.

Categoría: seleccione una categoría de objetos. De acuerdo con una categoría seleccionada, los objetos se muestran en la sección Configuración que aparece 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 sobre todos los dispositivos a los que tenga acceso.

Configuración

Seleccione un **Operador** y valores para el filtro (**Filtrar por**). Solo se puede seleccionar un operador, y se evaluarán juntos todos los valores con ese operador. Haga clic en **Agregar filtro** para agregar el nuevo valor para el filtro. Si se seleccionan más filtros, la ejecución de una notificación se evalúa con el operador *AND* (la notificación solo se envía si todos los campos del filtro se evalúan como *true*).

> Algunos filtros pueden hacer que la notificación se envíe con demasiada frecuencia. Se recomienda utilizar Limitación para agregar las notificaciones.

Lista de valores de filtro disponibles

Categoría	Valor	Comentario
Certificados de autoridades de certificación	Intervalo de tiempo relativo (Autoridad certificadora válida hasta, Certificado de igual válido hasta)	Seleccione un intervalo de tiempo relativo.
Certificados de iguales	Intervalo de tiempo relativo (Autoridad certificadora válida hasta, Certificado de igual válido hasta)	Seleccione un intervalo de tiempo relativo.
Clientes administrados	Intervalo de tiempo relativo (última conexión)	Seleccione un intervalo de tiempo en el que deba supervisarse la **Última conexión**.
	Porcentaje de ordenadores que no se conectan	Un valor entre 0 y 100. Solo puede utilizarse en combinación con el filtro **Intervalo de tiempo relativo**.
Licencias	Intervalo de tiempo relativo (fecha de caducidad de la licencia)	Seleccione un intervalo de tiempo que debe supervisarse para una caducidad de licencia.
	Porcentaje de uso de licencias	Un valor entre 0 y 100 calculado en función de las **Unidades** de licencia utilizadas para la activación. En el caso de los productos de ESET Mail Security, el uso de licencias se calcula en función de las **Unidades secundarias** que se utilizan para la activación.
	Tipo de usuario de la licencia	Seleccione **Empresa**, **Cliente MSP** o **Sitio**.
Tareas del cliente	Tarea	Seleccione tareas para el filtro de validez. Si no se selecciona nada, se tienen en cuenta todas.
	La tarea es válida	Seleccione **Sí**/**No**. Si se selecciona **No**, la notificación se activa cuando una tarea de la selección (filtro **Tarea**) como mínimo no es válida.
Tareas del servidor	Recuento (errores)	Número de errores de las tareas seleccionadas.
	Último estado	Último estado notificado de la tarea seleccionada.
	Tarea	Seleccione tareas para este filtro. Si no se selecciona nada, se tienen en cuenta todas.
	La tarea es válida	Seleccione **Sí**/**No**. Si se selecciona **No**, la notificación se activa cuando una tarea de la selección (filtro **Tarea**) como mínimo no es válida.
	Intervalo de tiempo relativo (hora de la ocurrencia)	Seleccione un intervalo de tiempo que deba supervisarse.
Software instalado	Nombre de la aplicación	Nombre completo de la aplicación. Si se supervisan más aplicaciones, utilice el operador **in** y agregue más campos.
	Proveedor de la aplicación	Nombre completo del proveedor. Si se supervisan más proveedores, utilice el operador **in** y agregue más campos.
	Estado de comprobación de versión	Si se selecciona **Versión obsoleta**, la notificación se activa cuando una aplicación como mínimo está obsoleta.
Iguales de red	Igual	Si tiene más instancias de ESET PROTECT Server en la red, seleccione una de ellas.
	Estado del servidor	Si ESET PROTECT Server está sobrecargado escribiendo registros, cambia su estado: • **Normal**: respuesta inmediata del servidor • **Limitado**: el servidor responde al agente una vez cada hora • **Sobrecargado**: el servidor no responde a los agentes
Notificaciones	Notificación	Seleccione la notificación para este filtro. Si no se selecciona nada, se tienen en cuenta todas.
	La notificación está activada	Seleccione **Sí**/**No**. Si se selecciona **No**, la notificación se activa cuando una notificación de la selección (filtro **Notificación**) como mínimo está desactivada.
	La notificación es válida	Seleccione **Sí**/**No**. Si se selecciona **No**, la notificación se activa cuando una notificación de la selección (filtro **Notificación**) como mínimo no es válida.

El contenido del mensaje predeterminado tiene un propósito informativo y no se puede personalizar. Puede

personalizar el mensaje enviado mediante 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 supervisarla para un grupo dinámico concreto.

Grupo dinámico: seleccione el grupo dinámico que desea evaluar.

Configuración - Condiciones

Seleccione el tipo de condición que desencadenará una notificación.

- **Notificarme cada vez que cambia el contenido del grupo dinámico** – Active esta opción para recibir notificaciones cuando los miembros del grupo seleccionado se agreguen, quiten o cambien.

> ESET PROTECT On-Prem comprueba el estado del grupo dinámico una vez cada 20 minutos.
> Por ejemplo, si la primera comprobación se realiza a las 10:00, las demás comprobaciones se realizan a las 10:20, las 10:40 y las 11:00. Si el contenido del grupo dinámico cambia a las 10:05 y, a continuación, vuelve a su estado original a las 10:13, durante la siguiente comprobación, realizada a las 10:20, ESET PROTECT On-Prem no reconocerá el cambio anterior y no lo notificará.

- **Notificarme cuando el tamaño del grupo supere un número específico**: seleccione el operador Tamaño del grupo y el Umbral para la notificación:
  - **Más de**: envía una notificación cuando el tamaño del grupo es mayor que el umbral.
  - **Menos de**: envía una notificación cuando el tamaño del grupo es menor que el umbral.
- **Notificarme cuando el crecimiento del grupo supere una velocidad específica**: defina el umbral y el periodo de tiempo que activarán una notificación. Puede definir tanto un número de clientes como un porcentaje de clientes (miembros del grupo dinámico). Defina el periodo de tiempo (en minutos, horas o días) para la comparación con el nuevo estado. Por ejemplo, hace siete días, el número de clientes con productos de seguridad obsoletos era de 10 y el umbral estaba definido en 20. Si el número de clientes con un producto de seguridad obsoleto llega a 30, se le informará de ello.
- **Notificarme cuando el número de clientes del grupo dinámico cambie en comparación con otro grupo**: si el número de clientes de un grupo dinámico cambia en relación con un grupo de comparación (ya sea estático o dinámico), se enviará una notificación. Umbral: permite definir el umbral que activará el envío de una notificación.

> Solo puede asignar una notificación a un grupo dinámico en el que tenga permisos suficientes. Para ver un grupo dinámico debe tener permiso de **Lectura** de su grupo estático principal.

Distribución

Debe elegir al menos un medio de distribución.

Enviar captura de SNMP

Envía una captura de SNMP. La captura SNMP informa al servidor por medio de un mensaje SNMP no solicitado. Si desea obtener más información, consulte Cómo configurar un servicio de captura de SNMP.

Enviar correo electrónico

Envía un mensaje de correo electrónico basado en su configuración de correo electrónico. De forma predeterminada, el correo electrónico de notificaciones se envía en formato HTML e incluye 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 selecciona **Enviar correo electrónico**, inserte al menos un destinatario de 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 (agregue la dirección del usuario desde Usuarios del ordenador), o en **Más** > **Importar CSV** o **Pegar del portapapeles** (**importe** una lista personalizada de direcciones desde un archivo CSV estructurado con delimitadores).
- **Más** > **Pegar del portapapeles**: importa una lista personalizada de direcciones con delimitadores personalizados. Esta función tiene un comportamiento similar al de la importación de CSV.

Enviar Syslog

Puede usar ESET PROTECT On-Prem para enviar notificaciones y mensajes de eventos a su servidor de Syslog. También puede exportar registros desde el producto de ESET de un ordenador cliente y enviarlos al servidor de Syslog. **Gravedad de syslog**: elija el nivel de gravedad en el menú desplegable. Posteriormente, las notificaciones aparecerán con la gravedad seleccionada en el servidor de Syslog.

Campos básicos en la distribución

- **Vista previa del mensaje**: una vista previa del mensaje que aparece en la notificación, que contiene los ajustes configurados en forma de texto. Puede personalizar el contenido y el asunto del mensaje y utilizar variables que se convertirán en valores reales al generarse la notificación. Es opcional, pero se recomienda para mejorar el filtrado.
  - **Asunto**: asunto de un mensaje de notificación. Haga clic en el icono de modificación para modificar el contenido; un asunto impreciso puede afectar a la ordenación y el filtrado de los mensajes.
  - **Contenido**: haga clic en el icono de modificación para modificar el contenido. Después de modificarlo, puede hacer clic en el icono de restablecimiento para restablecer el contenido predeterminado del mensaje.

> En **Sucesos en ordenadores o grupos administrados**, puede agregar variables a **Asunto** y **Contenido** para incluir información específica en la notificación. Haga clic en **Agregar variable** o empiece a escribir $ para ver la lista de variables.

- **General**

  o**Configuración regional**: idioma del mensaje predeterminado. El contenido del mensaje no está traducido.

  o**Zona horaria**: establezca la zona horaria para la variable **Hora de ocurrencia** `${timestamp}`, que se puede usar en el mensaje personalizado.

Si el evento tiene lugar a las 3:00 de la hora local, la hora local es UTC+2, la zona horaria seleccionada es UTC+4, y la hora que figura en la notificación será las 5:00.

Haga clic en **Finalizar** para crear una nueva notificación basada en la plantilla que está modificando.

Cómo configurar un servicio de captura de SNMP

Para recibir correctamente mensajes SMNP, es necesario configurar el servicio de captura de SNMP. Siga los pasos de configuración indicados a continuación según corresponda a su sistema operativo:

WINDOWS

Requisitos previos

- El servicio **Protocolo de Administración Simple de Red** debe estar instalado en el ordenador en el que esté instalado ESET PROTECT Server, así como en el ordenador en el que se instalará el software de captura SNMP.
- Ambos ordenadores (arriba) deberían estar en la misma subred.
- El servicio SMTP debe estar configurado en el ordenador de ESET PROTECT Server.

Configuración del servicio SNMP (ESET PROTECT Server)

1.Pulse la tecla de Windows + R para abrir el cuadro de diálogo Ejecutar, escriba Services.msc en el campo **Abrir** y pulse **Intro**. Busque SNMP Service.

2.Abre la ficha **Capturas**, escriba **público** en el campo **Nombre de la comunidad** y haga clic en **Agregar a la lista**.

3.Haga clic en **Agregar**, escriba el **nombre de cliente, dirección IP o IPX** del ordenador en el que está instalado el software de captura de SNMP en el campo adecuado y haga clic en **Agregar**.

4.Vaya a la ficha **Seguridad**. Haga clic en **Agregar** para ver la ventana **Configuración del servicio SNMP**. Escriba **público** en el campo **Nombre de la 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 SNMP no está configurado.

Configuración del software de captura de SNMP (cliente)

1.Asegúrese de que el servicio SNMP está instalado en el equipo cliente.

2.Instale una aplicación de recepción de capturas.

3.Configure la aplicación de recepción de capturas para recibir capturas SNMP de ESET PROTECT Server (esto puede incluir la configuración de IP y puerto de ESET PROTECT Server).

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 de recepción de capturas ahora le permite recibir mensajes de ESET PROTECT Server.

SNMP Trap no es compatible con el dispositivo virtual de ESET PROTECT.

LINUX

1. Instale el paquete snmpd ejecutando uno de los siguientes comandos:
`apt-get install snmpd snmp`(distribuciones Debian, Ubuntu)
`yum install net-snmp` (distribuciones Red Hat, CentOS)

2. Abra el archivo */etc/default/snmpd* y realice las siguientes modificaciones en los atributos:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```

Si se añade # se desactivará 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 de archivo snmpd.conf original. El archivo se editará más tarde.

```
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 del administrador de SNMP y el registro de las capturas entrantes:

```
 /etc/init.d/snmpd restart
```

o

```
service snmpd restart
```

7. Para comprobar si la captura funciona y está atrapando los mensajes, ejecute el siguiente comando:

```
tail -f /var/log/syslog | grep -i TRAP
```

Resumen del estado

ESET PROTECT Server realiza comprobaciones de diagnóstico periódicas. Utilice el **Resumen del estado** para ver estadísticas de uso y un estado general de su ESET PROTECT On-Prem. También puede resultar útil en la configuración inicial de ESET PROTECT On-Prem. Haga clic en **Resumen del estado** para ver información de estado detallada sobre ESET PROTECT On-Prem.

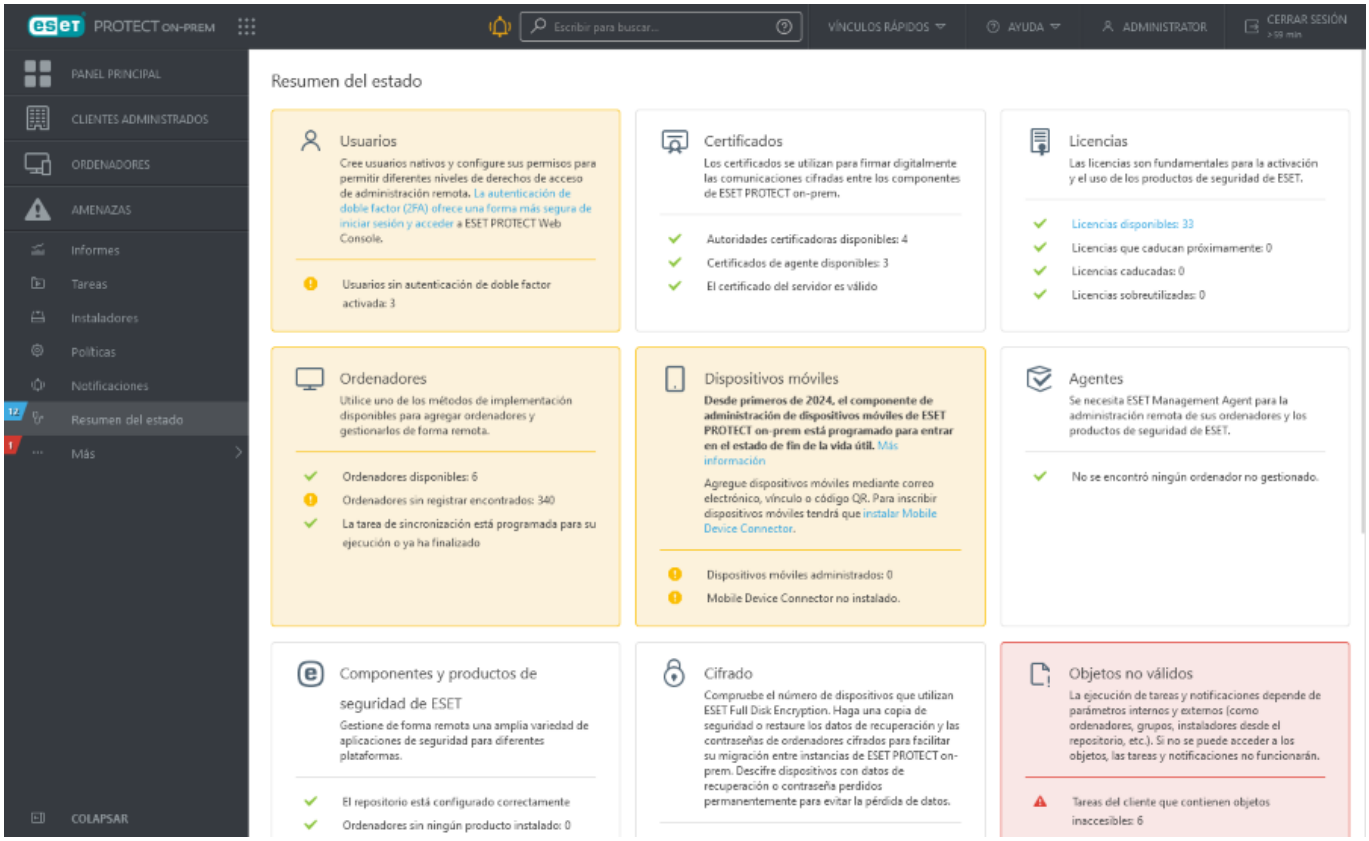
Haga clic en la ventana dinámica de una sección para mostrar una barra de tareas a la derecha con acciones. Cada ventana dinámica de sección puede tener un color de los varios existentes, según el estado de gravedad más alta de los elementos incluidos:

Color	Icono	Significado de los iconos	Descripción
Verde		OK	Ningún elemento de la sección tiene problemas.
Amarillo		Advertencia	Al menos un elemento de la sección aparece marcado con una advertencia.
Rojo		Error	Al menos un elemento de la sección aparece marcado con un error.
Gris		Contenido no disponible	El contenido no está disponible porque el usuario de ESET PROTECT Web Console no tiene derechos de acceso suficientes. El administrador debe configurar permisos adicionales para el usuario, y también puede iniciar sesión como otro usuario que tenga los derechos de acceso adecuados.
Azul		Información	Hay una pregunta relacionada con los ordenadores conectados (consulte la sección **Preguntas** a continuación).

Resumen del estado contiene las siguientes secciones:

Usuarios	Cree diferentes usuarios y configure sus permisos para permitir diferentes niveles de administración en ESET PROTECT On-Prem. La cuenta de administrador de ESET PROTECT On-Prem predeterminada se creó durante la instalación. No recomendamos utilizar la cuenta de administrador de ESET PROTECT On-Prem predeterminada como cuenta de usuario normal. Haga clic en **Ver usuarios**, cree una nueva cuenta de usuario nativo con autenticación de doble factor y utilícela como la cuenta predeterminada en ESET PROTECT On-Prem.
Certificados	Si desea utilizar certificados que no sean los predeterminados facilitados por ESET PROTECT On-Prem, puede crear Autoridades certificadoras y Certificados de igual para componentes individuales de ESET PROTECT y así permitir la comunicación con ESET PROTECT Server.
Licencias	ESET PROTECT On-Prem utiliza el sistema de licencias de ESET. Seleccione el método que desee utilizar para agregar las licencias que se utilizarán para activar los componentes de ESET PROTECT y los productos de seguridad de ESET en los ordenadores cliente.
Ordenadores	• **Agregar equipo**: agregue equipos en su red a la estructura de ESET PROTECT On-Prem. Puede agregar ordenadores y dispositivos móvilesM manualmente 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 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) (solo local) llega al fin de la vida útil en enero de 2024. Más información. 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 de 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 la pérdida de 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 no válidos	Contiene la lista de tareas del cliente y del servidor, desencadenadores, notificaciones o instaladores con referencias a objetos a los que no es posible acceder o que no son válidos. Haga clic en cualquier de los campos del resultado para ver un menú con la lista de objetos seleccionada.
Servicios externos	ESET PROTECT On-Prem se puede configurar para conectarse a servicios externos y ofrecer una 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 > Configuración. Si le resulta necesario, puede crear un repositorio sin conexión. • **Configurar actualizaciones**: las actualizaciones son necesarias para que ESET PROTECT On-Prem se mantenga actualizado. Las actualizaciones estarán disponibles solo si ESET PROTECT On-Prem ha importado una licencia de producto empresarial no caducada. Puede cambiar la configuración de actualización en **Más** > Configuración. • **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.
Preguntas	Cuando se detectan un dispositivo clonado o un cambio de hardware en un dispositivo cliente, se genera una pregunta. Más información sobre resolución de ordenadores clonados.
Estado de MSP	Si importa una cuenta MSP, dispondrá de una ventana dinámica con 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 utilizar para administrar las soluciones de seguridad del cliente, así como la configuración de ESET PROTECT On-Prem. Puede usar estas herramientas para configurar el entorno de red de forma que no necesite mucho mantenimiento.

La sección ··· **Más** contiene los siguientes elementos:

Detecciones oArchivos enviados oExclusiones oCuarentena
Ordenadores oUsuarios del ordenador oPlantillas de grupos dinámicos
Licencias oAdministración de licencias
Derechos de acceso oUsuarios oConjuntos de permisos
Certificados oCertificados de iguales oAutoridades certificadoras
Auditoría de actividad oRegistro de auditoría

Admin
o[Configuración]

Archivos enviados

ESET LiveGuard Advanced es un servicio que ofrece protección avanzada ante detecciones nunca vistas. Un usuario de ESET PROTECT On-Prem puede enviar archivos para analizarlos en busca de malware en el entorno de la nube y recibir un informe sobre el comportamiento de la muestra. Consulte en la Guía del usuario de ESET LiveGuard Advanced las instrucciones detalladas. Puede enviar de forma remota un archivo directamente desde ESET PROTECT Web Console en **Detecciones** > haga clic en un elemento de la categoría > **Archivos bloqueados** > **Enviar archivo a ESET LiveGuard**.

En la ventana **Archivos enviados** verá una lista de todos los archivos enviados a los servidores ESET. Entre ellos se incluyen los archivos enviados automáticamente a ESET LiveGrid® desde ordenadores cliente (en el caso de que ESET LiveGrid® esté activado en el producto de seguridad de ESET) y los archivos enviados a ESET LiveGuard Advanced de forma manual desde ESET PROTECT Web Console.

Ventana Archivos enviados

Puede ver la lista de los archivos enviados e información relacionada con esos archivos, como el usuario que envió el archivo y la fecha de envío. Haga clic en el archivo enviado y seleccione una acción en el menú desplegable.

Mostrar detalles	Haga clic par ver la ficha **Último envío**.
Ver comportamiento	Vea el informe del análisis de comportamiento de una muestra dada. Esta opción solo está disponible para los archivos enviados a ESET LiveGuard Advanced.
Exportar informe	Descargue el informe del análisis de comportamiento de una muestra dada. 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 a una política existente.

Ventana Detalles del archivo

La ventana Detalles del archivo contiene una lista de detalles del archivo seleccionado. Si un archivo se envía varias veces, se muestran los detalles del último envío.

Estado	Resultado del análisis de malware. **Desconocido**: el archivo no se analizó. **Limpio**: ninguno de los motores de detección evaluó el archivo como malware. **Sospechoso**, **Altamente sospechoso**: el archivo muestra comportamiento sospechoso, pero quizá no sea malware. **Malicioso**: el archivo muestra comportamiento peligroso.
Estado	Estado del análisis. El estado **Repetición del análisis** significa que el resultado está disponible, pero puede cambiar tras un nuevo análisis.
Procesado por última vez el	Un archivo puede enviarse para su análisis muchas veces y desde más ordenadores. Esta es el momento del último análisis.

Enviado el	El momento del envío.
Comportamientos	Haga clic en Ver comportamiento para ver el análisis de ESET LiveGuard Advanced o en **Exportar informe** para descargar el informe. Esto solo es válido si el ordenador que envió el archivo tiene una licencia de ESET LiveGuard Advanced activa.
Ordenador	El nombre del ordenador desde el que se envió el archivo.
Usuario	Usuario del ordenador que envió el archivo.
Motivo	El motivo por el que se envió el archivo.
Enviado a	Parte de la nube de ESET que ha recibido el archivo. No todos los archivos enviados se analizan en busca de malware.
Hash	SHA1 hash of the submitted file.
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, consulte la documentación.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Exclusiones

En esta sección puede ver una lista de todas las exclusiones creadas para detecciones del **Antivirus** y reglas de IDS del **Cortafuegos**. Esta nueva sección contiene todas las exclusiones, aumenta su visibilidad y simplifica su administración.

Haga clic en una exclusión o seleccione más exclusiones y haga clic en el botón **Detección** para administrarlas:

- **Cambiar asignación** : cambie los ordenadores de destino en los que se aplicará la exclusión.
- **Mostrar ordenadores afectados**: vea los ordenadores en los que se aplica la exclusión.
- **Registro de auditoría**: muestre el registro de auditoría de la exclusión seleccionada.
- **Eliminar**: elimine la exclusión.
- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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 la detección excluida o el cortafuegos aparece de nuevo en los ordenadores administrados, la columna **Número de coincidencias** muestra el número de veces que se ha aplicado la exclusión.

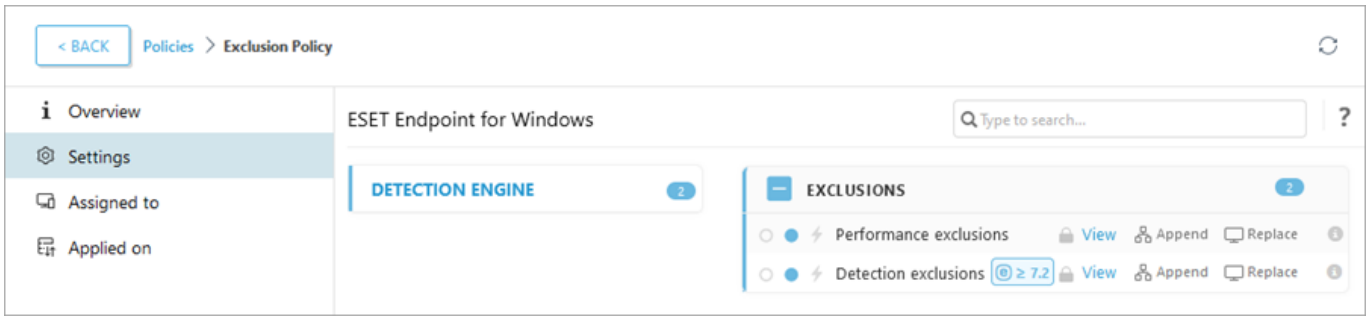
Migrar exclusiones desde una política

En ESET PROTECT On-Prem no puede crear exclusiones de detección de Antivirus mediante una Política. Si sus políticas ya contenían exclusiones, siga estos pasos para migrar exclusiones de políticas a la lista de **Exclusiones** en ESET PROTECT On-Prem:

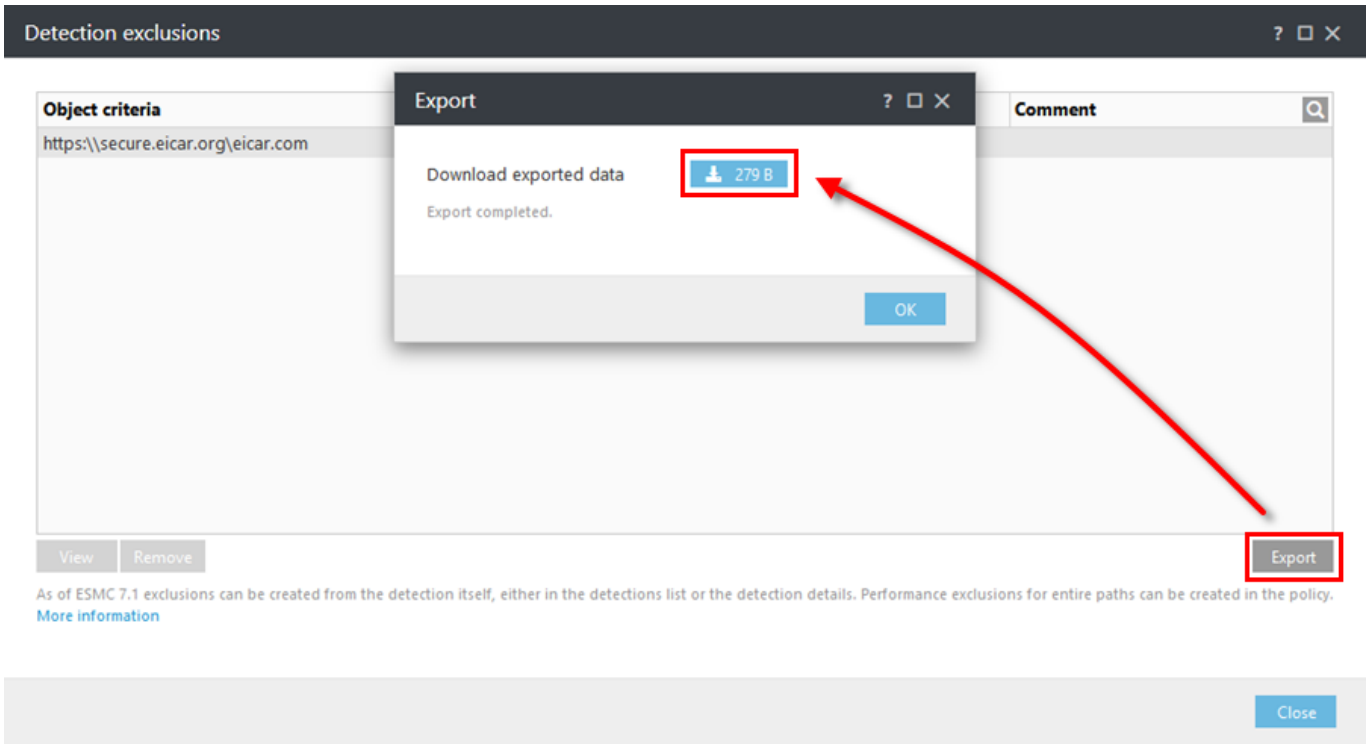
1. Vaya a **Políticas** y haga clic en la política que contenga las exclusiones. Seleccione **Mostrar detalles**.

2. Haga clic en **Configuración** > **Motor** de **detección**.

3. Haga clic en **Ver** junto a **Exclusiones de detección**.

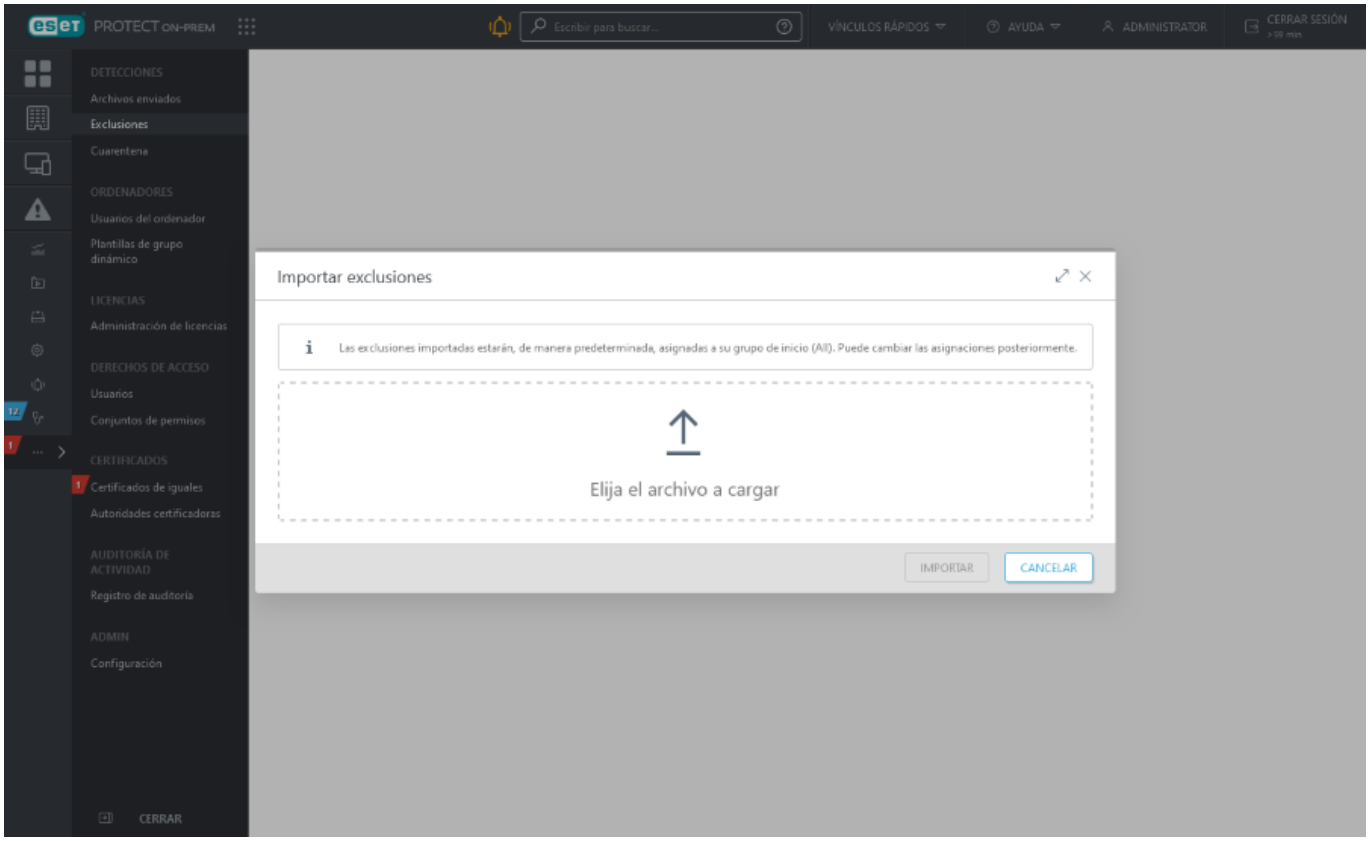


4. Haga clic en el botón **Exportar** y, a continuación, haga clic en el botón situado junto a **Descargar los datos exportados** y guarde el archivo *export.txt*. Haga clic en **Aceptar**.



5. En ESET PROTECT Web Console, vaya a **Más** > **Exclusiones**.

6. Haga clic en el botón **Importar** para importar exclusiones de detección desde un archivo. Haga clic en **Elija el archivo que cargar** y vaya al archivo *export.txt* o arrastre y coloque el archivo.



7. Haga clic en el botón **Importar** para importar las exclusiones de detección. Las exclusiones de detección importadas aparecerán en la lista de exclusiones.

Limitaciones de la asignación de exclusiones

- Las asignaciones de exclusiones originales no se conservan. De forma predeterminada, las exclusiones de detección importadas se asignan a ordenadores de su grupo de inicio. Para cambiar la asignación de exclusiones, haga clic en una exclusión y seleccione **Cambiar asignación**.
- Puede asignar exclusiones (para las detecciones de **Antivirus** y reglas de IDS del **Cortafuegos**) únicamente a los ordenadores que tengan un producto de seguridad de ESET compatible instalado. Las exclusiones no se aplicarán a los productos de seguridad de ESET incompatibles, y se ignorarán en dichos productos.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

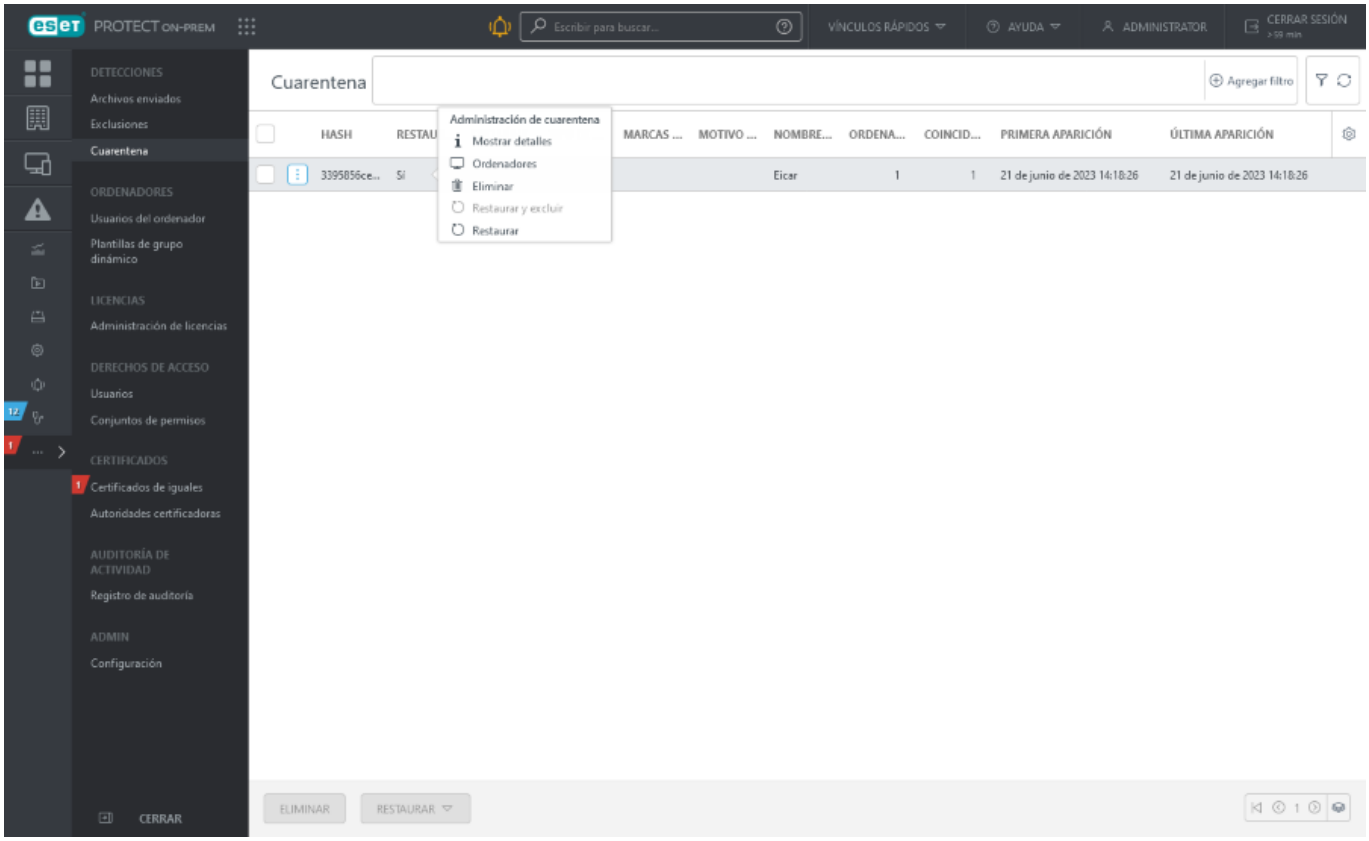
- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Cuarentena

En esta sección se muestran todos los archivos que están en cuarentena en dispositivos cliente. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si un producto de ESET los detecta incorrectamente como infectados.

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

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



Puede **Eliminar** el archivo en cuarentena o **Restaurarlo** en su ubicación anterior. Puede utilizar la opción de **Restaurar y excluir** el archivo en cuarentena para impedir que el producto de ESET vuelva a informar sobre él.

Puede usar varios filtros para filtrar la lista de los archivos que están en cuarentena.

Existen dos formas de acceder a **Cuarentena**:

1. **Más** > **Cuarentena**.

2. **Detalles del ordenador** > **Detecciones y cuarentena** > ficha **Cuarentena**.

Si hace clic en un elemento de la sección **Cuarentena**, abrirá el menú **Gestión de cuarentena**.

Mostrar detalles: muestra el dispositivo de origen, el nombre y el tipo de la detección, el nombre del objeto con la ruta completa al archivo, el hash, el tamaño, etc.

Ordenadores: abre la sección **Ordenadores** con los dispositivos filtrados conectados con el archivo en cuarentena.

Eliminar: quita el archivo de la cuarentena y el dispositivo afectado.

Restaurar: restaura el archivo en su ubicación original.

Restaurar y excluir: restaura el archivo en su ubicación original y lo excluye del análisis.

Cargar: abre la tarea Cargar archivo en cuarentena. Esta acción estará disponible después de hacer clic en **Mostrar detalles**.

La función **Cargar** solo se recomienda a los usuarios con experiencia. Si quiere investigar en más detalle el archivo en cuarentena, puede **cargarlo** en un directorio compartido.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Usuarios del ordenador

La sección Usuarios del ordenador le permite administrar usuarios y grupos de usuarios. Puede emparejar un usuario con un dispositivo para sincronizar algunos ajustes específicos del usuario. Se recomienda sincronizar los usuarios con Active Directory primero. Tras crear un nuevo ordenador, puede emparejarlo con un usuario específico. A continuación, puede buscar el usuario para ver detalles acerca de los ordenadores asignados a dicho usuario y su actividad.

También puede administrar usuarios y grupos de usuarios a efectos de la Administración de dispositivos móviles iOS mediante políticas asignadas a dispositivos iOS. Podrá modificar los usuarios o agregar Atributos personalizados.

Los **usuarios del ordenador** no son los **usuarios de la Consola web de ESET PROTECT**. Para administrar los usuarios y conjuntos de permisos de ESET PROTECT Web Console, diríjase a **Más** > **Usuarios**.

- Los usuarios resaltados no tienen ningún dispositivo asignado. Haga clic en el usuario, seleccione Modificar... y haga clic en**Ordenadores asignados** para ver los detalles de ese usuario. Haga clic en **Agregar ordenadores** para asignar dispositivos a este usuario.

- También puede agregar o quitar **Usuarios asignados** desde Detalles del ordenador. Mientras está en **Ordenadores**, seleccione un dispositivo y haga clic en **Mostrar detalles**. El usuario puede asignarse a más de un dispositivo. También puede utilizar **Asignar usuario** para asignar un usuario directamente a determinados dispositivos. Si hay un dispositivo asignado a un usuario, puede hacer clic en el nombre del dispositivo para ver información detallada sobre ese dispositivo.

- Puede arrastrar y colocar usuarios y grupos de usuarios. Seleccione el usuario (o grupo), mantenga pulsado el botón del ratón y muévalo al otro grupo.

Acciones de administración de usuarios

Seleccione un usuario para abrir un menú desplegable en el que puede ejecutar acciones. Consulte Leyenda de los iconos si desea obtener información detallada sobre las acciones.

Mostrar detalles: el menú muestra información como **Dirección de correo electrónico**, **Oficina o ubicación** y **Ordenadores asignados**. El usuario puede tener más de un dispositivo asignado. Puede modificar el **nombre** de usuario, la **descripción** o el **grupo principal del usuario**. Puede usar los **atributos personalizados** al crear políticas de administración de dispositivos móviles de iOS.

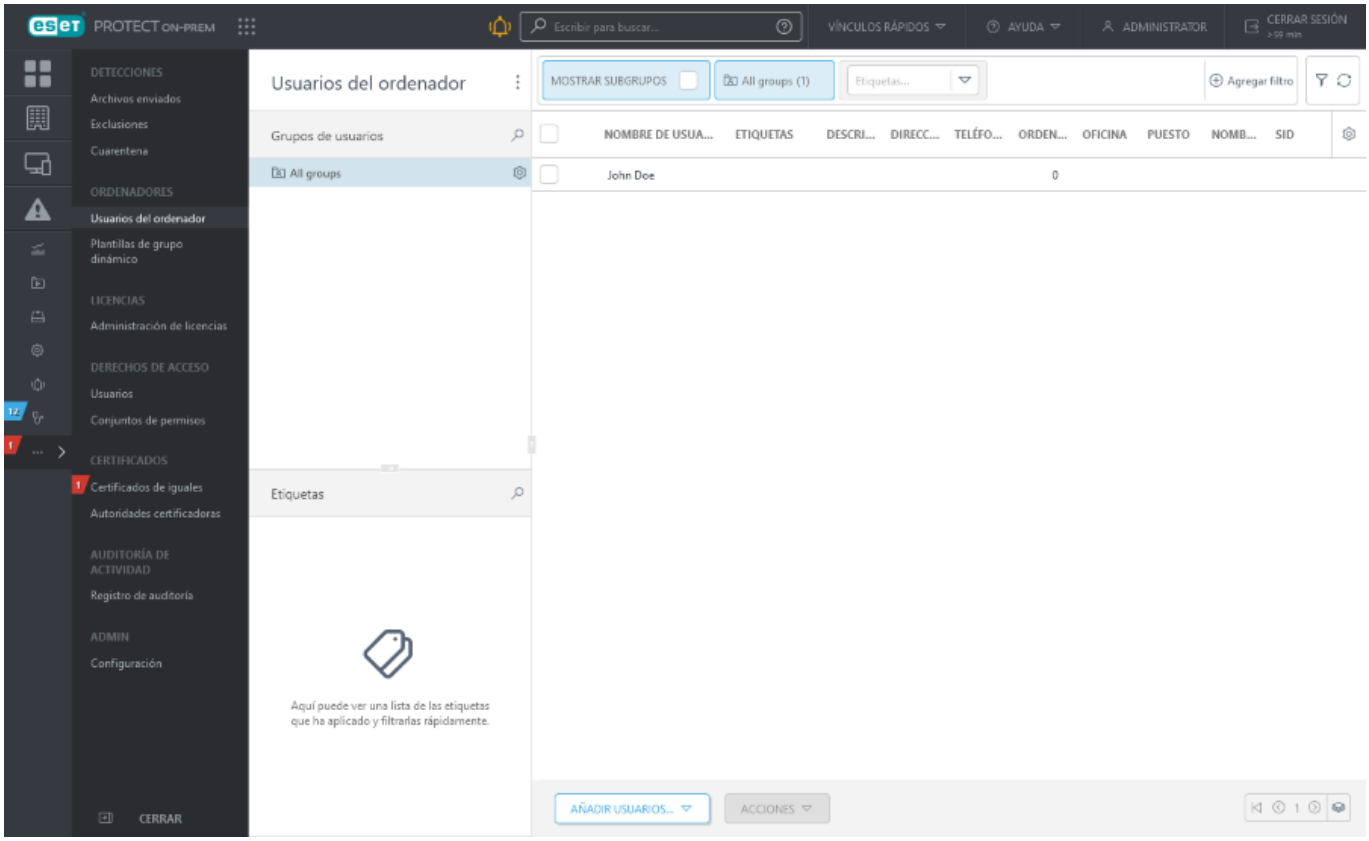
Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Agregar nuevos usuarios

1. Haga clic en **Usuarios del ordenador** > **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. Escriba el nombre del usuario que quiera agregar en el campo **Nombre de usuario**. Haga clic en + **Agregar** para agregar más usuarios. Si desea agregar varios usuarios simultáneamente, haga clic en Importar CSV para cargar un archivo *.csv* que incluya la lista de usuarios que desea agregar. Haga clic en **Copiar y pegar** para

importar una lista personalizada de direcciones separadas por delimitadores personalizados (esta función tiene un comportamiento similar al de la importación de CSV). Opcionalmente puede escribir una **Descripción** de los usuarios para facilitar su identificación.

3. Puede seleccionar un **Grupo principal** existente o crear un grupo nuevo.

4. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

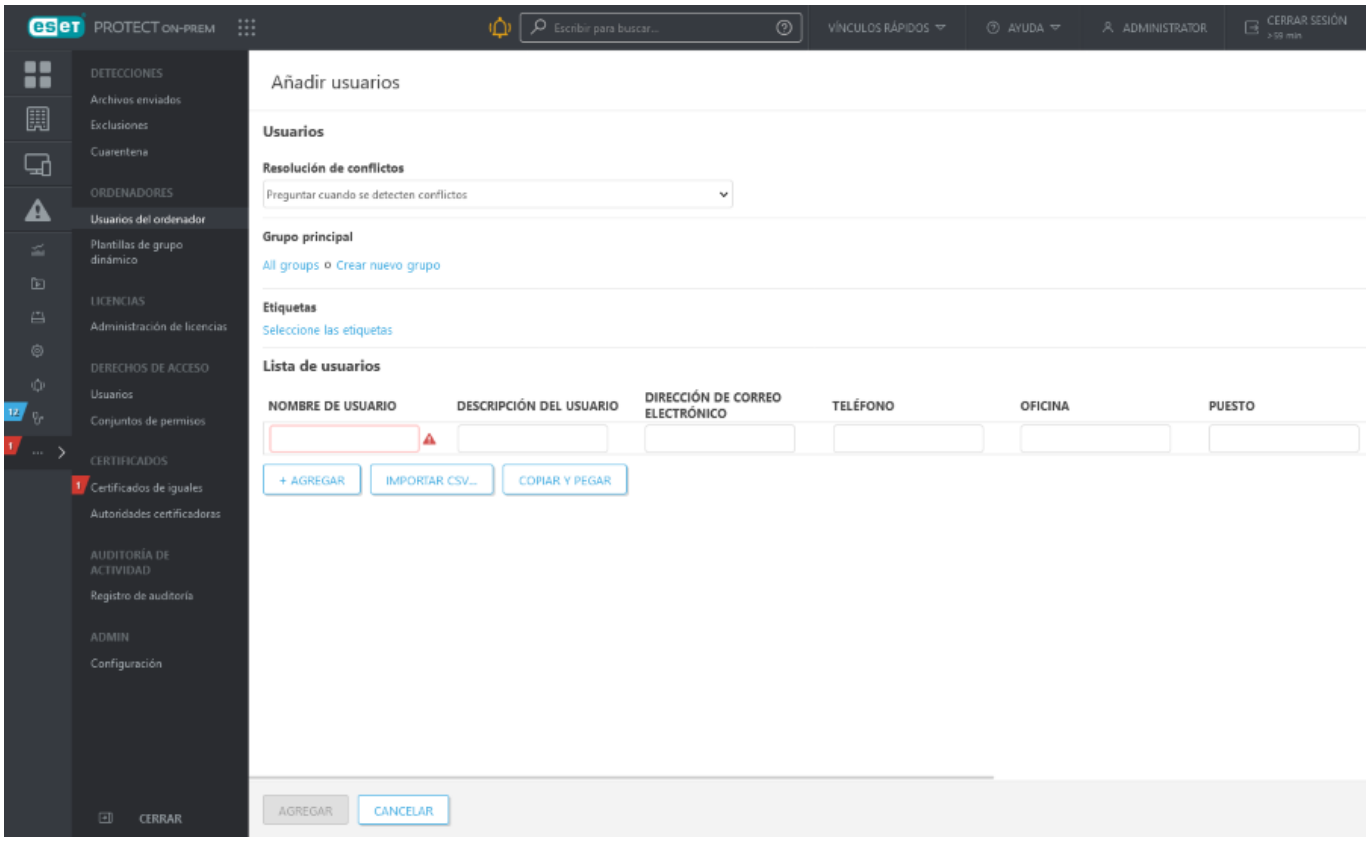
5. Utilice el menú desplegable **Resolución de conflictos** para seleccionar la acción que desee realizar si un usuario que está agregando ya existe en ESET PROTECT On-Prem:

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

- **Omitir usuarios que causan conflictos**: no se agregarán usuarios con el mismo nombre. Así se garantiza que los atributos personalizados de un usuario existente en ESET PROTECT On-Prem se conservarán (no se sobrescribirán con los datos de Active Directory).

- **Sobrescribir usuarios que causan conflictos:**: los usuarios existentes en ESET PROTECT On-Prem se sobrescribirán por los usuarios de Active Directory. Si hay dos usuarios con 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 distinto).

6. Haga clic en **Agregar** cuando haya terminado de hacer cambios. Los usuarios aparecerán en el grupo principal que haya especificado.



Modificar usuarios

Puede modificar detalles del usuario tales como la información **básica** y los **Ordenadores asignados**.

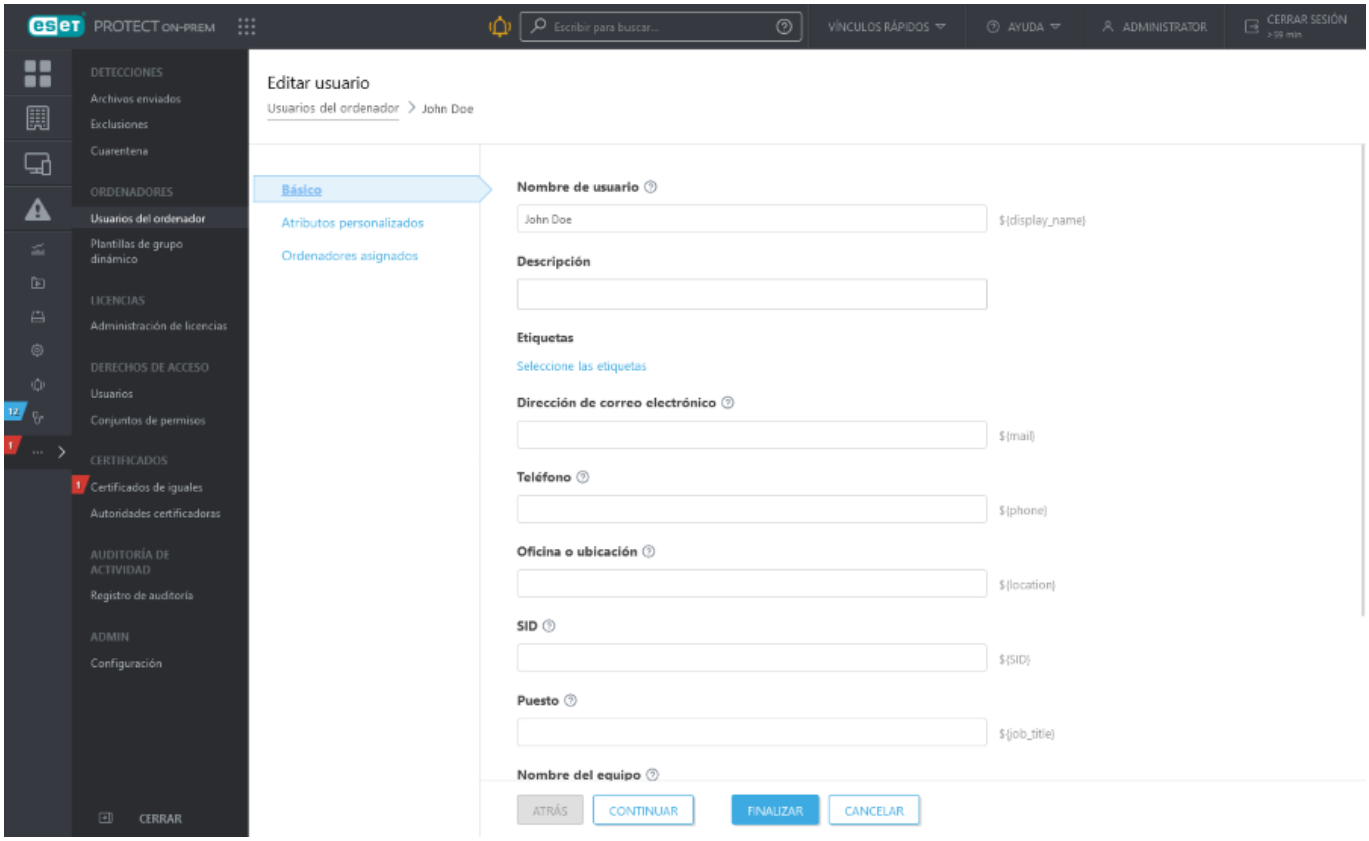
> Cuando ejecute una tarea de sincronización de usuarios para usuarios con atributos personalizados definidos, configure **Gestión de la colisión de creación de usuarios** como **Omitir**. De lo contrario, los datos del usuario se sobrescribirán con los datos de su Active Directory.

Básico

Si ha utilizado una tarea de sincronización de usuarios para crear el usuario y algunos campos están en blanco, puede especificarlos manualmente según sea necesario.

Aquí puede editar detalles del usuario como:

- **Nombre de usuario** y **descripción**: para fines informativos únicamente.
- **Etiquetas**:Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
- **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 los atributos personalizados existentes o añadir atributos nuevos. Para agregar atributos nuevos, haga clic en **Añadir nuevo** y seleccione entre las categorías:

- **Cuentas de Wi-Fi**: los perfiles se pueden usar para enviar la configuración Wi-Fi 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 utiliza un servidor de Exchange, utilice la configuración de Exchange ActiveSync indicada a continuación.

- **Cuentas de 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.

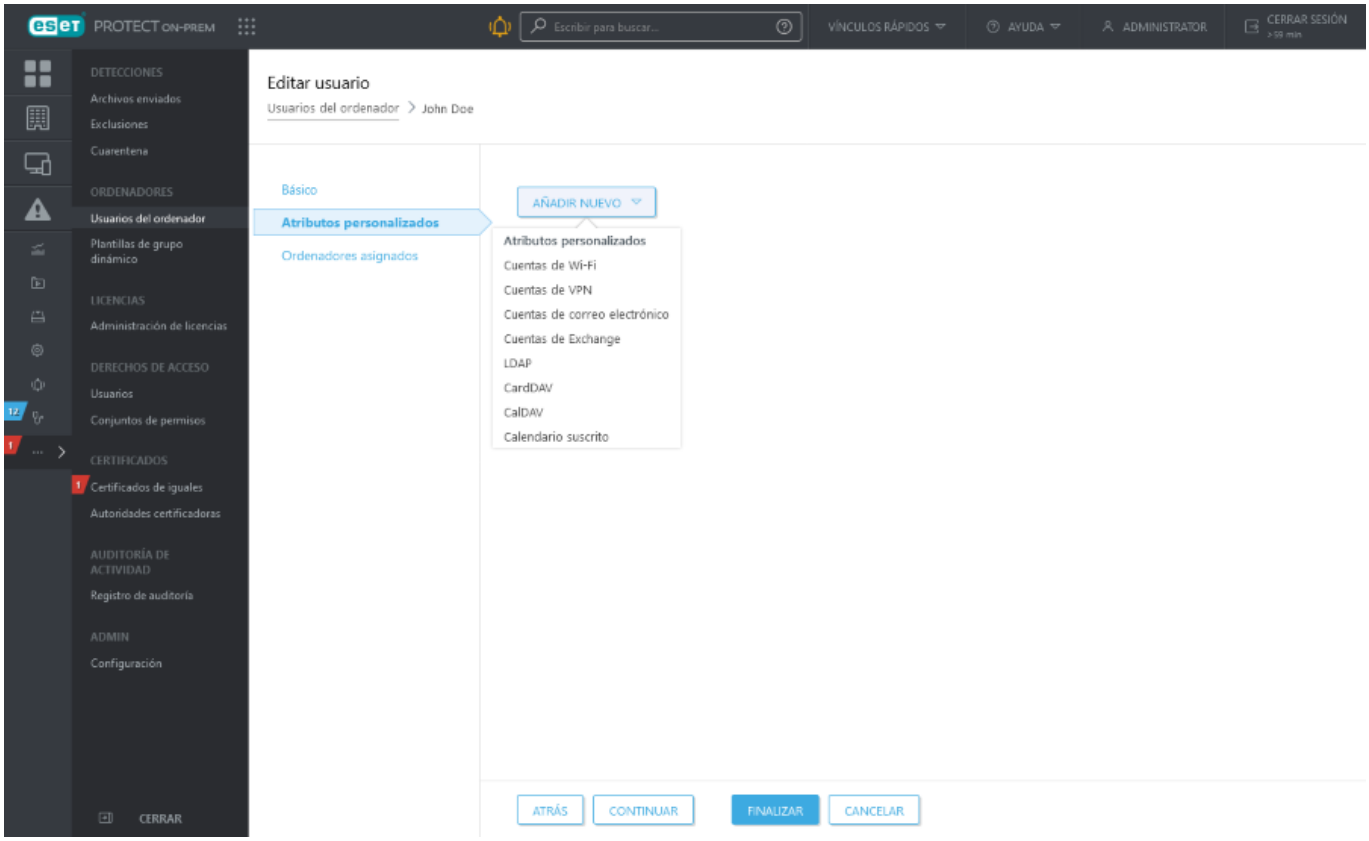
- **LDAP (alias del atributo)**: esta opción resulta especialmente útil si su empresa utiliza LDAP para los contactos. Puede asignar los campos de contacto a los campos de contacto de iOS correspondientes.

- **CalDAV**: contiene la configuración de todo aquel calendario que utiliza las especificaciones CalDAV.

- **CardDAV**: aquí se puede establecer la información de sincronización de todos aquellos contactos que se sincronizan mediante la especificación CardDAV.

- **Calendario suscrito**: si hay calendarios CalDAV configurados, aquí será donde defina el acceso de solo lectura a los calendarios de otros usuarios.

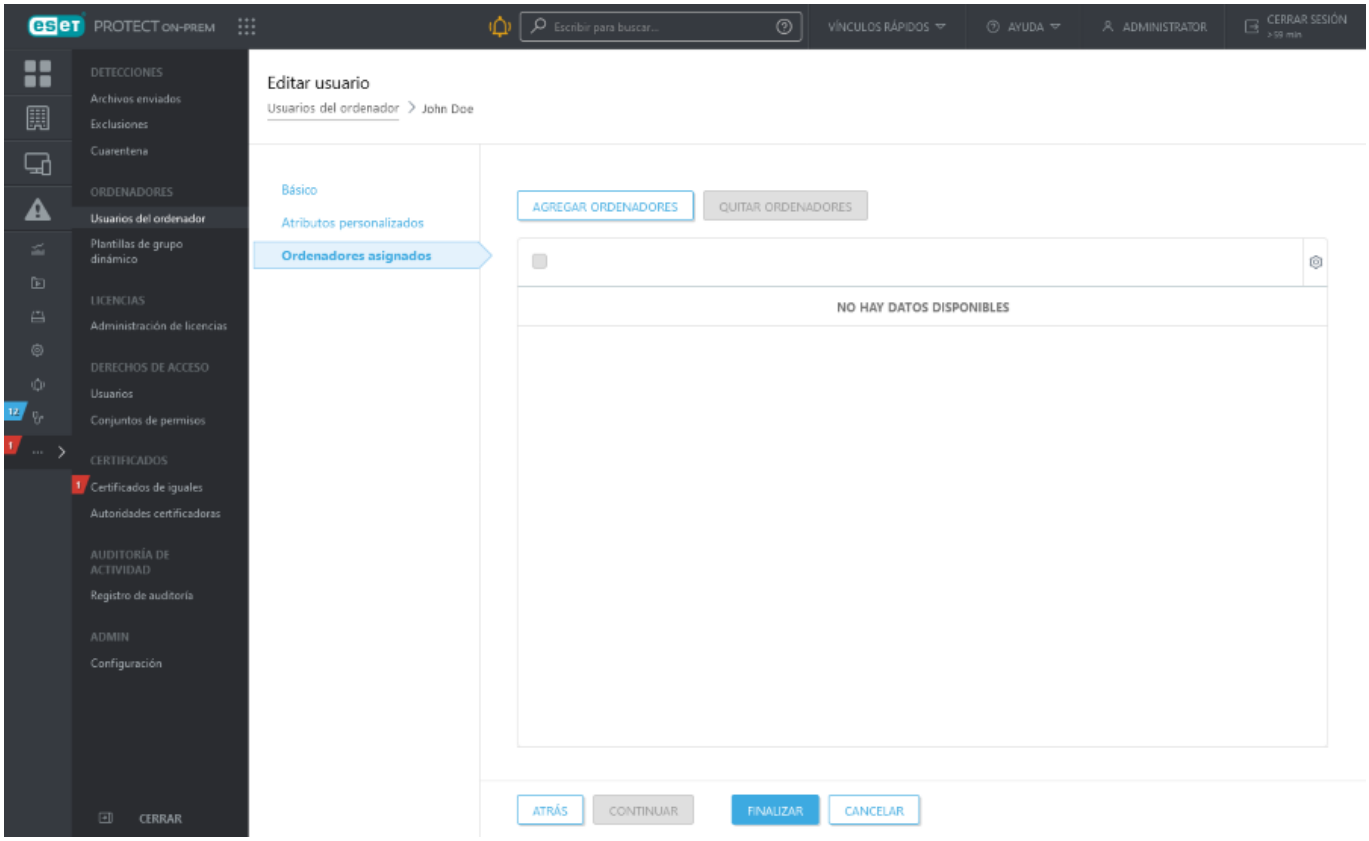
Algunos de los campos se convertirán en un atributo que posteriormente podrá utilizarse al crear una directiva para dispositivo móvil iOS como variable (marcador de posición). Por ejemplo, Iniciar sesión `${exchange_login/exchange}` o Dirección de correo electrónico `${exchange_email/exchange}`.



Ordenadores asignados

Aquí puede seleccionar dispositivos concretos. Para ello, haga clic en **Agregar equipos -** se listarán todos los grupos estáticos y dinámicos con sus miembros. Utilice las casillas de verificación para seleccionar y haga clic en **Aceptar**.

A un usuario solo se le pueden asignar 200 ordenadores como máximo en una operación.

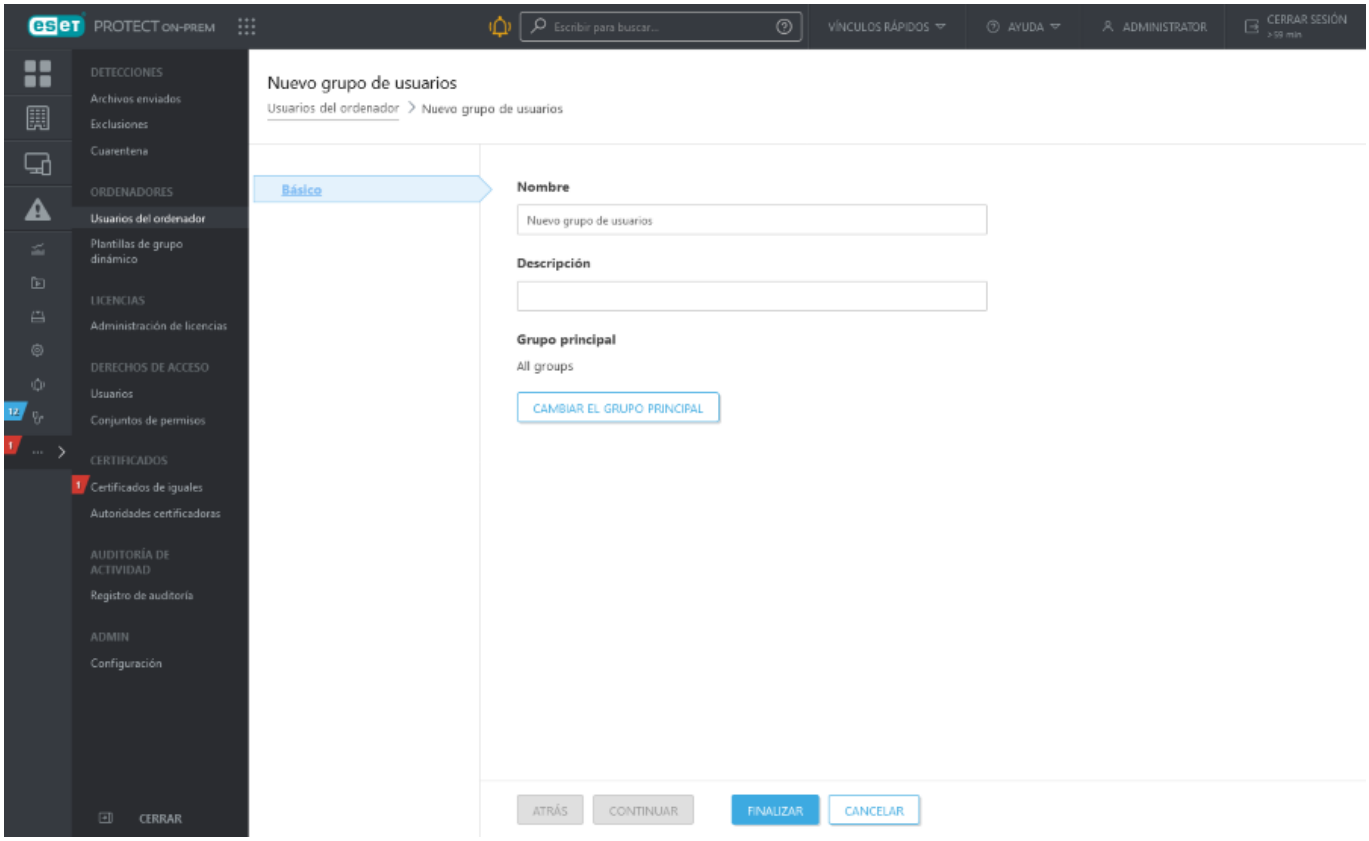


Crear un nuevo grupo de usuarios

Haga clic **Usuarios del ordenador** > ⚙ y seleccione + **Nuevo grupo de usuarios**.

Básico

Introduzca un **nombre y una descripción** (opcional) para el nuevo grupo de usuarios. De 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 el grupo principal** y seleccione un grupo principal en el árbol. Haga clic en **Finalizar** para crear un nuevo grupo de usuarios.



Puede asignar permisos concretos a este grupo de usuarios desde Derechos de acceso utilizando Conjuntos de permisos (consulte la sección **Grupos de usuarios**). De esta forma puede especificar qué usuarios de ESET PROTECT Web Console pueden gestionar qué grupos de usuarios concretos. Si lo desea puede incluso restringir el acceso de dichos usuarios a otras funciones de ESET PROTECT On-Prem mediante políticas. Estos usuarios administrarán exclusivamente los grupos de usuarios.

Plantillas de grupos dinámicos

Las plantillas de grupos dinámicos establecen los criterios que los ordenadores deben cumplir para situarlos en un grupo dinámico. Cuando un cliente cumpla estos criterios, se moverá automáticamente al grupo dinámico correspondiente.

Una plantilla es un objeto estático almacenado en un grupo estático. Los usuarios deben tener los permisos adecuados para poder acceder a las plantillas. Un usuario necesita permisos para poder trabajar con plantillas de grupos dinámicos. Todas las plantillas predefinidas se encuentran en el grupo estático **Todo** y, de manera predeterminada, solo están disponibles para el administrador. Al resto de usuarios se les tendrán que asignar permisos adicionales. Por ello, los usuarios podrían no ver o utilizar las plantillas predeterminadas. Las plantillas pueden moverse a un grupo en el que los usuarios tengan permisos. Para duplicar una plantilla, el usuario debe tener asignados permisos de **Uso** (para plantillas de grupo dinámico) para el grupo en el que está la plantilla de origen y permisos de **Escritura** para el grupo de inicio del usuario (donde se almacenará el duplicado). Consulte el ejemplo de duplicación de objetos.

- Crear nueva plantilla de grupo dinámico
- Reglas de una plantilla de 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 principal.
Mostrar detalles	Muestra el resumen de información sobre la plantilla seleccionada.
Registro de auditoría	Permite ver el Registro de auditoría del elemento seleccionado.
Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Modificar...	Modifique 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 indique, especifique el nombre para su nueva plantilla.
Duplicar	Cree una nueva plantilla de grupo dinámico basada en la plantilla seleccionada. Se necesitará un nombre nuevo para la tarea duplicada. La plantilla duplicada se almacenará en su grupo principal.
Eliminar	Elimine la plantilla de forma permanente.
Importar	Importe plantillas de grupo dinámico desde un archivo. Durante la importación, se verifica la estructura del archivo para garantizar que no esté dañado.
Exportar	Exporte las plantillas de grupos dinámicos seleccionadas a un archivo para realizar copias de seguridad o migraciones. Recomendamos no realizar modificaciones en el archivo, porque podrían provocar que los datos dejaran de ser utilizables.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Nueva plantilla de grupo dinámico

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**.

Básico

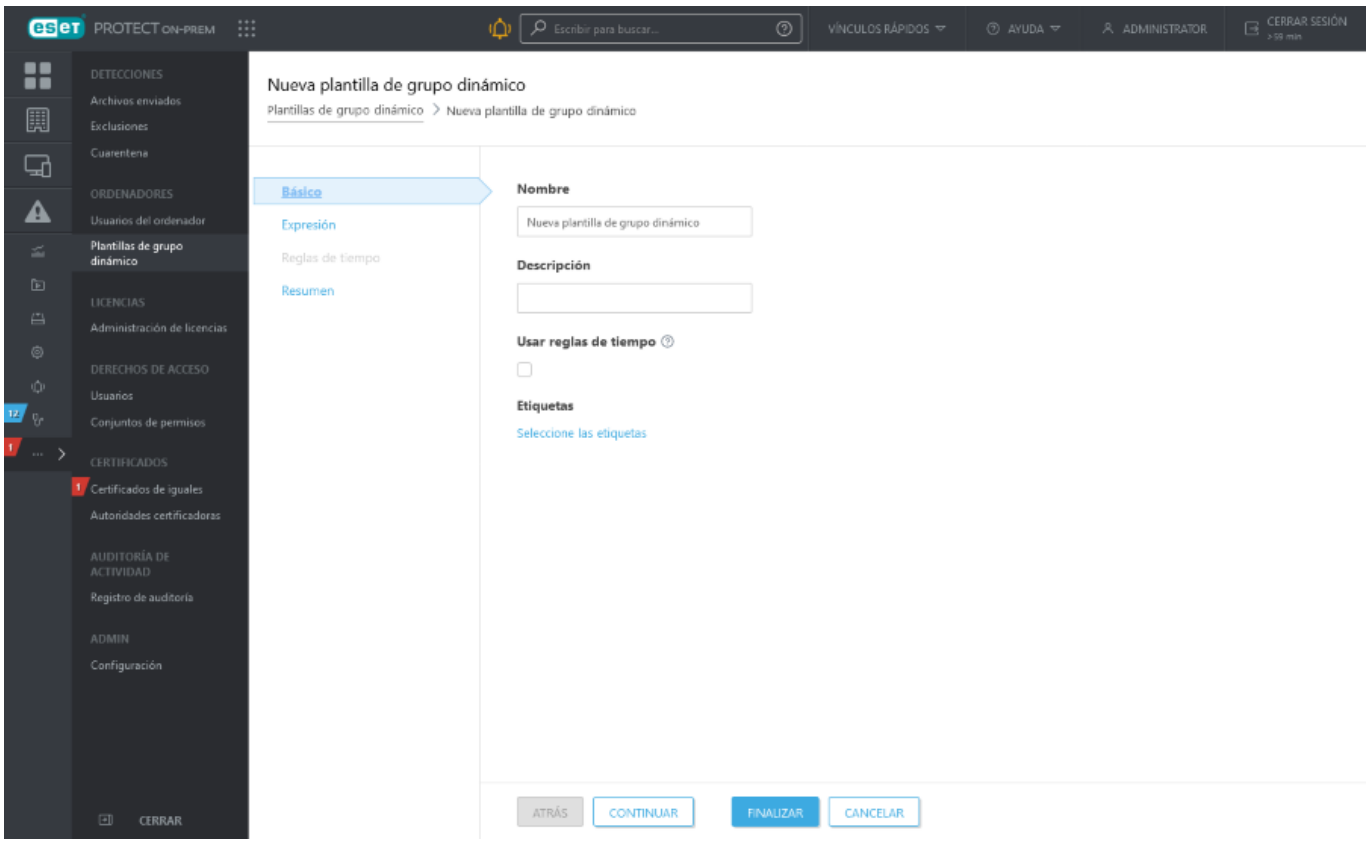
Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

Expresión

Consulte nuestros ejemplos con instrucciones paso a paso ilustradas para ver ejemplos de utilización de los grupos dinámicos en su red.



Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Reglas de una plantilla de grupo dinámico

Cuando establece las reglas de una plantilla de grupo dinámico puede usar distintos operadores para cada condición que desee cumplir en su caso.

En los siguientes capítulos se explican las reglas y operaciones utilizadas en las plantillas de grupos dinámicos:

- Operaciones

- Reglas y conectores lógicos
- Evaluación de las reglas de una plantilla
- Cómo crear automatización en ESET PROTECT On-Prem
- Plantillas de grupos dinámicos
- Casos de uso: crear una plantilla de Grupo dinámico específica

Operaciones

Si especifica varias reglas (condiciones), debe seleccionar qué operación se debe usar para combinar las reglas. En función del resultado, el ordenador cliente se añadirá o no a un grupo dinámico que utiliza esta plantilla.

- La **Operación** seleccionada funciona no solo al combinar más reglas, sino también cuando solo hay una regla.
- No puede combinar operaciones. Solo se usa una operación por plantilla de grupo dinámico, y se aplica a todas sus reglas.

AND (deben darse todas las condiciones).	Comprueba si todas las condiciones obtienen un resultado positivo; el ordenador debe cumplir todos los parámetros necesarios.
OR (debe darse al menos una condición).	Comprueba si al menos una de las condiciones obtiene un resultado positivo, el ordenador debe cumplir al menos uno de los parámetros necesarios.
NAND (al menos una condición no debe darse).	Comprueba si al menos una de las condiciones no puede evaluarse positivamente: el ordenador no debe cumplir al menos un parámetro.
NOR (no debe darse ninguna de las condiciones).	Comprueba si ninguna de las condiciones puede obtener un resultado positivo, el ordenador no cumple ninguno de los parámetros necesarios.

Reglas y conectores lógicos

Una regla está compuesta por un elemento, un conector lógico (operador lógico) y un valor definido.

Al hacer clic en **+ Agregar regla** se abrirá una ventana con una lista de elementos divididos en categorías. Por ejemplo:

Software instalado > **Nombre de la aplicación**

Adaptadores de red > **Dirección MAC**

Edición del SO > **Nombre del sistema operativo**

Puede ver la lista de las reglas disponibles en este artículo de la base de conocimiento de ESET.

Para crear una regla, seleccione un elemento, elija un operador lógico y especifique un valor. La regla se evaluará según el valor que haya especificado y el operador lógico que haya utilizado.

Entre los tipos de valores aceptables se incluyen los números, las cadenas, las enumeraciones, las direcciones IP, las máscaras de productos y los identificadores de ordenadores. Cada valor tiene operadores lógicos distintos asociados y ESET PROTECT Web Console mostrará automáticamente solo aquellos que sean compatibles.

• **"= (es igual que)"**: el valor del símbolo y el valor de la plantilla deben coincidir. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas.

• **"> (es mayor que)"**: el valor del símbolo debe ser mayor que el valor de la plantilla. También se puede usar para crear una comparación de intervalo para los símbolos de la dirección IP.

• **"≥ (es mayor o igual que)"**: el valor del símbolo debe ser mayor o igual que el valor de la plantilla. También se puede usar para crear una comparación de intervalo para los símbolos de la dirección IP.

• **"< (es menor que)"**: el valor del símbolo debe ser menor que el valor de la plantilla. También se puede usar para crear una comparación de intervalo para los símbolos de la dirección IP.

• **"≤ (es menor o igual que)"**: el valor del símbolo debe ser menor o igual que el valor de la plantilla. También se puede usar para crear una comparación de intervalo para los símbolos de la dirección IP.

• **"contiene"**: el valor del símbolo contiene el valor de la plantilla. En el caso de cadenas, esta acción busca una subcadena. La búsqueda se realiza sin distinguir entre mayúsculas y minúsculas.

• **"tiene prefijo"**: el valor del símbolo tiene el mismo prefijo de texto que el valor de la plantilla. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas. Establece los primeros caracteres de la cadena de búsqueda; por ejemplo, en el caso de "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", el prefijo sería "Micros", "Micr", "Microsof", etc.

• **"tiene postfijo"**: el valor del símbolo tiene el mismo postfijo de texto que el valor de la plantilla. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas. Establece los primeros caracteres de la cadena de búsqueda; por ejemplo, en el caso de "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", el postfijo sería "319" o "0.30319", etc.

• **"tiene una máscara"**: el valor del símbolo debe coincidir con la máscara definida en una plantilla. El formato de la máscara permite cualquier carácter, los símbolos especiales "*" (cero, uno o varios caracteres) y "?" (exactamente un carácter); p. ej.: "6.2.*" o "6.2.2033.?".

• **"regex"**: el valor del símbolo debe coincidir con la expresión regular (regex) de una plantilla. La expresión regular debe estar escrita en el formato **Perl**.

i Una expresión regular, *regex* o *regexp* es una secuencia de caracteres que definen 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 coincidir con cualquier valor de la lista de una plantilla. Para agregar un elemento, haga clic en **+ Agregar**. Cada línea es un nuevo elemento de la lista. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas.

• **"es uno de (máscara de cadena)"**: el valor del símbolo debe coincidir con cualquier máscara de la lista de una plantilla. Al comparar las cadenas se tienen en cuenta las mayúsculas y las minúsculas. Ejemplos: *endpoint-pc*, *Endpoint-PC*.

• **"tiene valor"**

i Las reglas de tiempo permiten marcar la casilla **Medir tiempo transcurrido** para crear una plantilla de grupo dinámico en función del tiempo transcurrido desde un evento específico. El ordenador administrado debe ejecutar ESET Management Agent 10.0 o versiones posteriores.

Operadores negados:

> los operadores negados se deben usar con cuidado, ya que en el caso de varias líneas de registro, como el de "Aplicación instalada", con estas condiciones se probarán todas las líneas. Consulte los ejemplos incluidos (Evaluación de las reglas de una plantilla y Plantilla de grupo dinámico - ejemplos para ver cómo se deben usar los operadores negados o las operaciones negadas para obtener los resultados esperados.

- **"≠ (no es igual que)"**: el valor del símbolo y el valor de la plantilla no deben coincidir. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las 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 de texto como valor de la plantilla. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas.
- **"no tiene postfijo"**: el valor del símbolo no tiene el postfijo de texto como valor de la plantilla. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas.
- **"no tiene máscara"**: el valor del símbolo no debe coincidir con la máscara definida en una plantilla.
- **"no es regex"**: el valor del símbolo no debe coincidir con la expresión regular (regex) de una plantilla. La expresión regular debe estar escrita en el formato **Perl**. La operación de negación se proporcionó como elemento de ayuda para negar las expresiones regulares coincidentes sin reescrituras.
- **"no es uno de"**: el valor del símbolo no debe coincidir con ningún valor de la lista de una plantilla. Al comparar las cadenas no se tienen en cuenta las mayúsculas y las minúsculas.
- **"no es uno de (máscara de cadena)"**: el valor del símbolo no debe coincidir con cualquier máscara de la lista de una plantilla.
- **"no tiene valor"**

Evaluación de las reglas de una plantilla

La evaluación de las reglas de una plantilla la gestiona el ESET Management Agent, y no el ESET PROTECT Server (al ESET PROTECT Server solo se envía el resultado). El proceso de evaluación tiene lugar según las reglas configuradas en una plantilla. A continuación se muestran algunos ejemplos del proceso de evaluación de las reglas de una plantilla.

Debe distinguir entre probar en busca de existencia (algo no existe con ese valor) y probar en busca de diferencia (algo existe pero tiene un valor distinto). Algunas reglas básicas para realizar esta distinción:

- Para verificar la existencia: Operación sin negativa (**AND**, **OR**) y operador sin negativa (=, >, <, **contiene**,...).
- Para verificar la existencia de un valor distinto: 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 verificar la presencia de una lista de elementos (por ejemplo, una lista concreta de las aplicaciones instaladas en un ordenador), tendrá que crear una plantilla de Grupo dinámico independiente para cada uno de los elementos de la lista y asignar la plantilla a un Grupo dinámico independiente, un contexto en el que cada Grupo dinámico es un subgrupo de otro. Los ordenadores con la lista de elementos se encuentran en el último subgrupo.

El estado es un conjunto de información diversa. Algunos orígenes facilitan más de un estado de dimensión por equipo (por ejemplo sistema operativo, cantidad de memoria RAM, etc.), otros ofrecen información de estado multidimensional (por ejemplo dirección IP, 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	Hardware - Tamaño de la RAM en MB	Aplicación instalada
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 archivos PDF
124.256.25.25	52-FB-E5-74-35-73				Paquete Office
					Weather Forecast

El estado está compuesto por grupos de información. Un grupo de datos facilita siempre información coherente organizada en filas. El número de filas por grupo podría variar.

Las condiciones se evalúan por grupo y por fila; si hay más condiciones relacionadas con las columnas de un grupo, solo se tienen en cuenta los valores de la misma fila.

Ejemplo 1:

Para este ejemplo, asuma la siguiente condición:

```
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 ordenador, dado que no hay ninguna fila en la que ambas condiciones sean ciertas.

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Hardware - Tamaño de la RAM en MB	Aplicación instalada

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Hardware - Tamaño de la RAM en MB	Aplicación instalada
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 archivos PDF
124.256.25.25	52-FB-E5-74-35-73				Paquete Office
					Weather Forecast

Ejemplo 2:

Para este ejemplo, asuma la siguiente condición:

```
Adaptadores de red.Dirección IP = 192.168.1.2 Y Adaptadores de red.Dirección MAC = 4A-64-3F-10-FC-75
```

En esta ocasión, ambas condiciones coinciden con celdas de la misma fila y, por lo tanto, la regla se evalúa en su totalidad como VERDADERA. Se selecciona el ordenador.

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Hardware - Tamaño de la RAM en MB	Aplicación instalada
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 archivos PDF
124.256.25.25	52-FB-E5-74-35-73				Paquete Office
					Weather Forecast

Ejemplo 3:

En el caso de 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 para dos filas, ya que solo una de las condiciones debe cumplirse. Se selecciona el ordenador.

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Hardware - Tamaño de la RAM en MB	Aplicación instalada
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 archivos PDF

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Hardware - Tamaño de la RAM en MB	Aplicación instalada
124.256.25.25	52-FB-E5-74-35-73				Paquete Office
					Weather Forecast

Plantilla de grupo dinámico - ejemplos

Encontrará útiles plantillas predefinidas de grupos dinámicos en **Más** > **Plantillas de grupos dinámicos**.

Las plantillas de grupo dinámico de ejemplo y los ejemplos de su uso que contiene esta guía muestran algunas de las formas en las que puede usar los grupos dinámicos para administrar su red:

Grupo dinámico que detecta si hay un producto de seguridad instalado
Grupo dinámico que detecta si hay una versión de software concreta instalada
Grupo dinámico que detecta si no hay una versión de software concreta instalada
Grupo dinámico que detecta si no hay una versión de software concreta instalada, pero otra versión sí
Grupo dinámico que detecta si un ordenador está en una subred concreta
Grupo dinámico que detecta versiones instaladas pero no activadas de los productos de seguridad para servidores
Cómo implementar automáticamente productos de ESET en escritorios Windows recién conectados
Aplicar una política basada en la ubicación

Consulte los **artículos de la base de conocimiento**, donde encontrará ejemplos de plantillas de grupo dinámico y su uso:

Ejemplos útiles de plantillas de grupo dinámico en ESET PROTECT On-Prem: ejemplos de cómo puede usar los detalles de Inventario de hardware para crear reglas para un grupo dinámico que contiene los dispositivos que cumplen los criterios de hardware seleccionados.
Configure ESET PROTECT On-Prem para que se implementen automáticamente los productos para equipos de ESET en ordenadores no protegidos
Configure los equipos para que usen ajustes de actualización distintos según la red a la que se conectan mediante ESET PROTECT On-Prem
Cree un certificado nuevo para que las estaciones de trabajo nuevas se unan automáticamente a un grupo dinámico en ESET PROTECT On-Prem

Puede que los artículos de la base de conocimiento no estén disponible en su idioma.

Lógicamente, existen muchos otros objetivos que pueden lograrse con las plantillas de grupos dinámicos mediante la combinación de reglas. Las posibilidades son casi infinitas.

Grupo dinámico - hay un producto de seguridad instalado

Este grupo dinámico se puede usar para ejecutar la tarea inmediatamente después de instalar el producto de seguridad de ESET en una máquina: Activación, Análisis personalizado, etc.

Puede crear una **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos** y crear un nuevo grupo dinámico con plantilla.

Básico

Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (deben darse todas las condiciones).

2.Haga clic en **+ Agregar regla** y seleccione una condición. Seleccione **Ordenador** > **Máscara de productos administrados** > **es uno de** > **Protegido por ESET: Escritorio**. También puede elegir productos de ESET distintos.

Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Grupo dinámico - hay una versión de software concreta instalada

Este grupo dinámico se puede usar para detectar una aplicación de software de seguridad de ESET instalada en una máquina. A continuación podrá ejecutar, por ejemplo, tareas de actualización o ejecutar comandos personalizados en estas máquinas. Se pueden usar distintos operadores, como **"contiene"** o **"tiene prefijo"**.

Puede crear una **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos** y crear un nuevo grupo dinámico con

plantilla.

Básico

Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (deben darse todas las condiciones).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Software instalado** > **Nombre de la aplicación** > **= (es igual que)** > *ESET Endpoint Security*
- **Software instalado** > **Versión de aplicación** > **= (igual)** > *6.2.2033.0*

Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Grupo dinámico - no está instalada una versión concreta de una software

Este grupo dinámico se puede usar para detectar la ausencia de una aplicación de software de seguridad de ESET en una máquina. Los ajustes de este ejemplo incluirán las máquinas que no contengan el software o las máquinas que tengan una versión distinta de la especificada.

Este grupo es útil porque podrá podrá ejecutar la tarea de instalación del software en estos ordenadores con el fin de realizar la instalación o la actualización. Se pueden usar distintos operadores, como **"contiene"** o **"tiene prefijo"**.

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**.

Básico

Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **NAND** (al menos una condición no debe darse).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Software instalado** > **Nombre de la aplicación** > **= (es igual que)** > *ESET Endpoint Security*
- **Software instalado** > **Versión de aplicación** > **= (igual)** > *6.2.2033.0*

Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Grupo dinámico - no está instalada una versión concreta de una software, pero sí otra

Este grupo dinámico se puede usar para detectar una aplicación de software instalada pero con una versión distinta a la que está solicitando. Este grupo es útil, ya que podrá ejecutar tareas de actualización en estas máquinas cuando no cuenten con la versión necesaria. 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**.

Básico

Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (deben darse todas las condiciones).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Software instalado** > **Nombre de la aplicación** > **= (es igual que)** > *ESET Endpoint Security*
- **Software instalado** > **Versión de aplicación** > **≠ (no es igual)** > *"6.2.2033.0"*

Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Grupo dinámico - un ordenador está en una subred concreta

Este grupo dinámico se puede usar para detectar una subred concreta. A continuación se puede usar para aplicar una directiva personalizada para la actualización o el control web. Se pueden especificar varios intervalos.

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**.

Básico

Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (deben darse todas las condiciones).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Direcciones IP de la red** > **Dirección IP del adaptador** > **≥ (mayor o igual que)** > *10.1.100.1*
- **Direcciones IP de la red** > **Dirección IP del adaptador** > **≤ (menor o igual que)** > *10.1.100.254*

• **Direcciones IP de la red** > **Máscara de subred del adaptador** > **= (igual)** > *255.255.255.0*

Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Grupo dinámico - versión instalada pero no activada de producto de seguridad para servidor

Este grupo dinámico se puede usar para detectar productos de servidor inactivos. Una vez detectados estos productos, podrá asignar una tarea del cliente a este grupo con el fin de activar los ordenadores 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**.

Básico

Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

Seleccione **Usar reglas de tiempo** para activar **Reglas de tiempo** y establezca un tiempo específico durante el cual estará activada la coincidencia de grupos dinámicos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (deben darse todas las condiciones).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

• **Ordenador** > **Máscara de productos administrados** > **es uno de** > **Protegido por ESET: Servidor de correo**

• **Problemas funcionales/de protección** > **Fuente** > **= (es igual que)** > **Producto de seguridad**

• **Problemas funcionales/de protección** > **Problema** > = **(es igual que)** > **Producto no activado**

Reglas de tiempo

Establezca un intervalo de tiempo para la nueva plantilla de grupo dinámico. Haga clic en el botón **Agregar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de fin** 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 establecer la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración del tiempo establecido. Puede agregar más intervalos de tiempo.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear la plantilla. Esta plantilla nueva se añadirá a la lista de plantillas y se podrá utilizar más tarde para crear un nuevo grupo dinámico.

Cómo automatizar ESET PROTECT On-Prem

Utilizando técnicas como el ejemplo que se muestra a continuación, puede automatizar distintas acciones, desde actualizaciones del producto y el sistema operativo, análisis y activaciones automáticas de productos recién agregados con licencias preseleccionadas hasta la solución de incidentes complejos.

Cómo implementar automáticamente productos de ESET en escritorios Windows recién conectados

⚠ Este ejemplo solo debe llevarse a cabo en clientes sin software de seguridad de terceros ni software de seguridad de ESET desde el segmento de inicio (por ejemplo, ESET Smart Security). No se recomienda instalar productos de ESET en clientes con software de seguridad de terceros. Puede utilizar ESET AV Remover para quitar otros programas antivirus de su ordenador.

✔ 1. Cree un grupo dinámico llamado *Sin producto de seguridad*.
a.Conviértalo en un grupo secundario del grupo predefinido **Ordenadores Windows** > **Windows (escritorios)**.
b.Haga clic en **Nueva plantilla**.
c.Agregue la siguiente regla: **Ordenador** > **Máscara de productos administrados**.
d.Como operador, seleccione **no igual**.
e.Seleccione la máscara **Protegido por ESET: Escritorio**
f.Haga clic en **Finalizar** para guardar el grupo.
2. Vaya a **Tareas** > **Nuevo** > **Tarea del cliente**.
a.Seleccione **Instalación de software** en el menú desplegable Tarea y escriba el nombre de la tarea en **Nombre**.
b.Elija el paquete en la sección **Configuración** y configure otros parámetros si es necesario.
c.Haga clic en **Finalizar** > **Crear desencadenador**.
d.En la sección **Destino**, 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 los clientes conectados al grupo dinámico desde este momento. Tendrá que ejecutar esta tarea manualmente en los clientes que estuvieran en el grupo dinámico antes de que se creara la tarea.

Aplicar una política basada en la ubicación

1. Cree un grupo dinámico llamado *Subred 120*.
a.Conviértalo en un grupo secundario del grupo **Todo**.
b.Haga clic en **Nueva plantilla**.
c.Agregue la siguiente regla: **Direcciones IP de red** > **Subred IP**.
d.Como operador, seleccione **igual**.
e.Introduzca la subred que quiera filtrar, por ejemplo, 10.1.120.0 (el último número debe ser para filtrar todas las direcciones IP desde la subred 10.1.120.).
f.Haga clic en **Finalizar** para guardar el grupo.
2. Desplácese hasta **Políticas**.
a.Haga clic en **Nueva política** y asigne un **Nombre** a la política.
b.En la sección **Configuración**, seleccione **ESET Management Agent**.
c.Realice el cambio de política; por ejemplo, cambie el **Intervalo de conexión** a 5 minutos.
d.En la sección **Asignar**, haga clic en **Asignar**, marque la casilla situada junto a la *Subred 120* de su grupo y haga clic en **Aceptar** para confirmar.
e.Haga clic en **Finalizar** para guardar la política.
Esta política se aplicará en los clientes conectados al grupo dinámico desde este momento.

Consulte las reglas de eliminación de políticas para comprobar qué le ocurre a la configuración de políticas aplicada cuando la máquina cliente abandona el grupo dinámico (cuando las condiciones que permiten que sea miembro del grupo dinámico dejan de ser válidas).

Consulte otros ejemplos de plantillas de grupos dinámicos.

Administración de licencias

Al comprar licencias para cualquier producto empresarial de ESET, recibirá automáticamente acceso a ESET PROTECT On-Prem. Puede administrar fácilmente sus licencias con ESET PROTECT On-Prem desde el menú principal en **Más** > **Administración de licencias**.Si ya dispone de un nombre de usuario y contraseña que desea convertir a una clave de licencia, consulte Convertir credenciales de licencia heredada. El nombre de usuario y la contraseña se han reemplazado por una clave de licencia/ID pública. La clave de licencia es una cadena única que se utiliza para identificar al propietario de la licencia y la activación propiamente dicha.

Puede activar el producto empresarial de ESET con ESET PROTECT On-Prem.

Consulte también Preguntas frecuentes sobre licencias (usuarios empresariales).

Permisos de administración de licencias

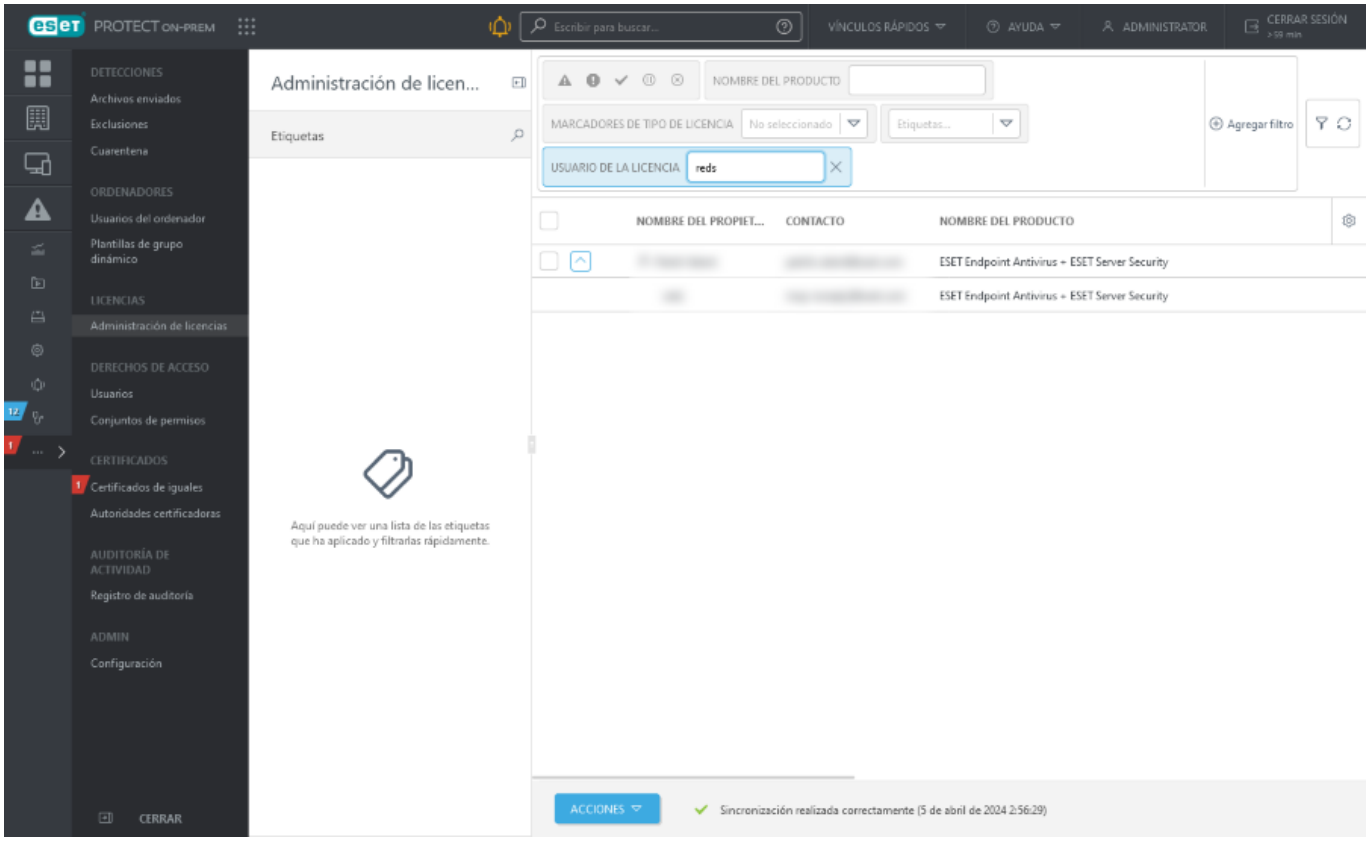
A cada usuario puede asignársele un permiso en Licencias. Los permisos solo son válidos para las licencias contenidas en el grupo estático en el que se ha asignado ese conjunto de permisos. Cada tipo de permiso permite al usuario realizar diferentes acciones.

Solo los administradores cuyo grupo de inicio sea **Todos** y tengan permiso de **Escritura** para las licencias del grupo de inicio pueden agregar o quitar licencias. Cada licencia está identificada por su **ID público** y puede contener una o más unidades. Solo el administrador puede distribuir licencias entre otros usuarios que tengan los permisos suficientes. Las licencias no son reducibles.

Las licencias de ESET MSP Administrator 2 se dividen en un grupo para cada empresa. No puede extraer una

licencia del grupo.

Administración de licencias en Web Console



Las licencias del mismo usuario de ESET Business Account o la misma empresa se agrupan en grupos de licencias. Haga clic en para desplegar el grupo de licencias y ver los detalles de las mismas.

En ESET Business Account y ESET PROTECT On-Prem, cada licencia se identifica con estos elementos:

- **ID público**

- **Tipo de licencia**: **empresarial** (licencia de pago), **prueba** (licencia de prueba), **MSP** (licencia de proveedor de servicios administrados) y **NFR** (licencia no para reventa).

Entre la información adicional sobre la licencia se incluye:

- El **Nombre del propietario** y el **contacto** de la licencia.

- El nombre y el tipo de **Usuario de la licencia**: **Empresa**, **Sitio**, **Cliente MSP**.

- **Nombre del paquete** para el que están pensados los productos de ESET. Obtenga más información sobre los niveles de protección de ESET.

- El **Nombre de producto** de seguridad para el que la licencia está destinada.

- El Estado **de la licencia** (si la licencia está caducada, sobreutilizada o a punto de caducar o estar sobreutilizada, se mostrará un mensaje aquí).

- El número de **Unidades** que se pueden activar con esta licencia y el número de unidades sin conexión. En el caso de los productos de ESET Mail Security, el uso de licencias se calcula en función de las **Unidades**

secundarias que se utilizan para la activación.

• El número de **Unidades secundarias** de los productos para servidor de ESET (protección de buzones, puerta de enlace, conexiones).

• **Validez** representa la fecha de caducidad de la licencia. Es posible que las licencias de suscripción no tengan una fecha de caducidad.

Puede filtrar las licencias por su **Estado**:

Correcto: verde	La licencia está correctamente activada.
Errores: rojo	La licencia no está registrada, ha caducado o está sobreutilizada.
Advertencias: naranja	Su licencia ya está agotada o está a punto de caducar (caducará en 30 días).
Desactivado o suspendido	La licencia está desactivada o se ha suspendido.
Obsoleto	Su licencia ha expirado.

Las licencias caducadas y sobreutilizadas (con estado **Error** u **Obsoleto**) no son visibles en la lista de licencias disponibles en el asistente 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 los grupos de licencias seleccionados:

Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Agregar licencias	Haga clic en **Agregar licencias** y seleccione el método que desea utilizar para agregar las nuevas licencias: 1.**ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**: conecte ESET PROTECT Hub, ESET Business Account o EMA 2 y agregue todas sus licencias a la sección **Administración de licencias**. 2.**Clave de licencia**: introduzca una clave para una licencia válida y haga clic en **Agregar licencias**. La clave de licencia se comprobará con el 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 comprobará con el servidor de activación y se agregará a la lista. Puede ver cómo se ha agregado la licencia según el icono de la columna **Nombre del propietario**: **Archivo de licencia sin conexión**, **Clave de licencia** o **ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**.
Quitar licencias	Quite los grupos de licencias seleccionados. Se le pedirá que confirme esta acción. La eliminación de la licencia no desencadena la desactivación del producto. Su producto de ESET permanecerá activado incluso tras la eliminación de la licencia en **Administración 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 suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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 sobre licencias en ESET PROTECT On-Prem de inmediato. Las licencias se sincronizan automáticamente una vez al día con los servidores de licencias de ESET. Si usa ESET Business Account o ESET MSP Administrator, las licencias también se sincronizan automáticamente una vez al día con estos servicios. Si se produce un error en la sincronización de licencias, asegúrese de que el nombre de host de *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 ha agregado licencias desde ESET Business Account.
Abrir EMA	Abra el portal de ESET MSP Administrator. Esta acción solo está disponible si ha agregado licencias desde ESET MSP Administrator.

Despliegue un grupo de licencias y haga clic en una licencia para realizar las siguientes acciones. El conjunto de acciones depende del tipo de licencia seleccionada:

Usar licencia de activación	Ejecute la tarea Activación del producto con esta licencia.
Etiquetas	Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
Administrar licencia	Si la licencia se sincroniza desde ESET Business Account o ESET MSP Administrator, puede administrar la licencia. Si la licencia está sobreutilizada, puede aumentar la capacidad de la licencia o desactivar algunos de sus dispositivos.
Renovar licencia	Renueve la licencia próxima a caducar, caducada, suspendida o desactivada 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	Permite ver el Registro de auditoría del elemento seleccionado.
Copiar ID público de la licencia	Copie el ID de la licencia pública en el portapapeles.

Licencias de suscripción

ESET PROTECT On-Prem permite administrar licencias de suscripción. Puede agregar dichas licencias mediante ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator o una clave de licencia. Puede comprobar la validez de su suscripción en **Administración de licencias** en la columna **Validez** o en **Ordenadores** > Detalles. No es posible crear un archivo de licencia sin conexión a partir de una licencia de suscripción.

Compatibilidad con ESET Business Account Sites

Ahora puede importar la estructura completa de su ESET Business Account, incluida la distribución de puestos de licencia entre los sitios.

Activación de productos empresariales de ESET

Puede distribuir licencias a los productos de ESET desde ESET PROTECT On-Prem por medio de dos tareas:

- La tarea de instalación de software
- La tarea de activación del producto

Desactivación de productos empresariales de ESET

Puede desactivar los productos empresariales de ESET (es decir, quitar la licencia del producto) de varias maneras desde ESET PROTECT Web Console:

- en **Ordenadores**, seleccione los ordenadores y, a continuación, seleccione **Desactivar productos** - Quita la licencia de todos los dispositivos seleccionados a través del servidor de licencias de ESET. El producto se desactiva aunque no se hubiera activado desde ESET PROTECT On-Prem o la licencia no estuviera administrada por ESET PROTECT On-Prem.

Si selecciona únicamente un ordenador con más productos de ESET instalados (por ejemplo, un producto ESET Endpoint y ESET Inspect Connector), puede optar por desactivar productos individuales.

- Quitar ordenador de administración
- Cree la tarea Eliminar ordenadores que no se conecten con la opción **Desactivar licencia**.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Uso compartido de licencias entre administradores de sucursales

Hay tres usuarios y un administrador; cada usuario tiene su propio grupo de inicio:
• *John*, *San Diego*
• *Larry*, *Sídney*
• *Makio*, *Tokio*
El administrador importa 3 licencias. Estas licencias se encuentran en el grupo estático Todos, y no las pueden utilizar otros usuarios.
Para asignar una licencia a otro usuario, el administrador puede marcar la casilla de verificación que está junto al grupo de licencias que quiere asignar a otro usuario, hacer clic en el botón **Acciones**, hacer clic en **Grupo de acceso** > **Mover** y, a continuación, seleccionar el grupo en el que el usuario tiene permiso.
Para el usuario *John*, seleccione el grupo *San Diego*. *John* debe tener permiso de **Uso** de las **Licencias** del grupo *San Diego* para utilizar la licencia.
Cuando el usuario *John* inicie sesión, podrá ver y utilizar únicamente la licencia movida a su grupo. El administrador debe repetir el proceso para *Larry* y *Makio*; posteriormente los usuarios solo pueden ver su licencia, mientras que el administrador las puede ver todas.

ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator

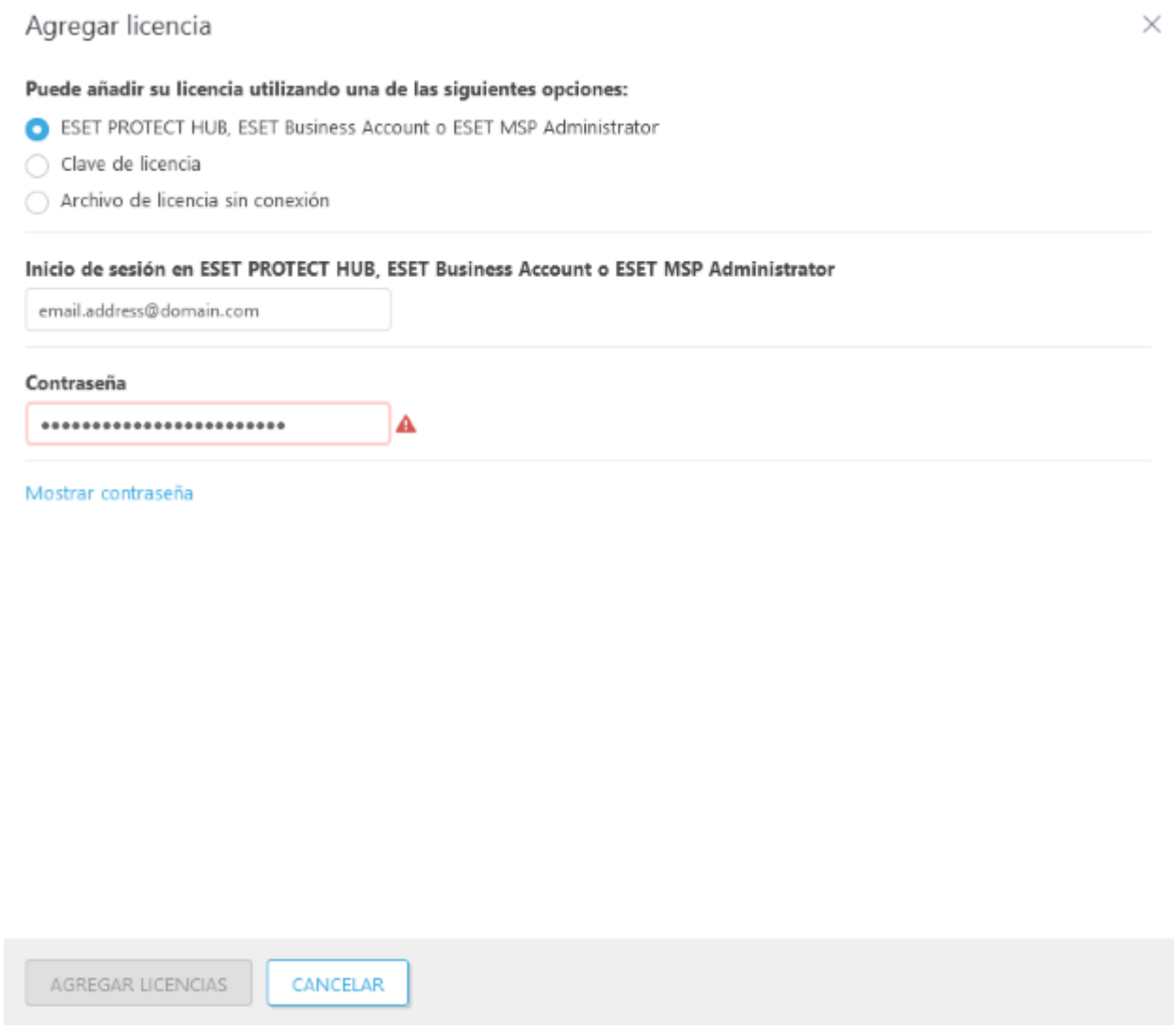
Solo los administradores cuyo grupo de inicio sea **Todos** y tengan permiso de **Escritura** para las licencias del grupo de inicio pueden agregar o quitar licencias. Cada licencia está identificada por su **ID público** y puede contener una o más unidades. Solo el administrador puede distribuir licencias entre otros usuarios que tengan los permisos suficientes. Las licencias no son reducibles.

ESET Business Account o ESET MSP Administrator

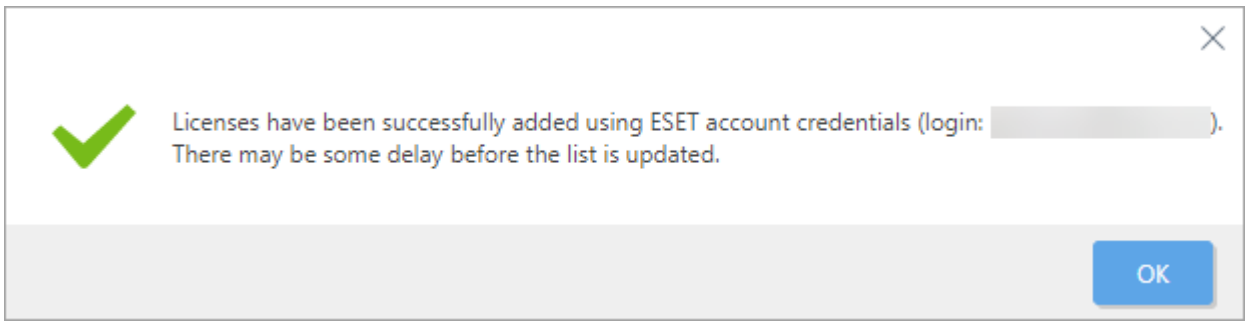
1. Haga clic en**Más** > **Administración de licencias** > **Licencia** > **Agregar licencia**.

2. Seleccione **ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**.

3. Introduzca las credenciales de ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator 2 (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 de ESET Business Account o ESET MSP Administrator con

su árbol de grupos estáticos de **Ordenadores** en Web Console.

Si se produce un error en la sincronización de licencias, asegúrese de que el nombre de host de *edf.eset.com* y sus direcciones IP estén permitidos en la red.

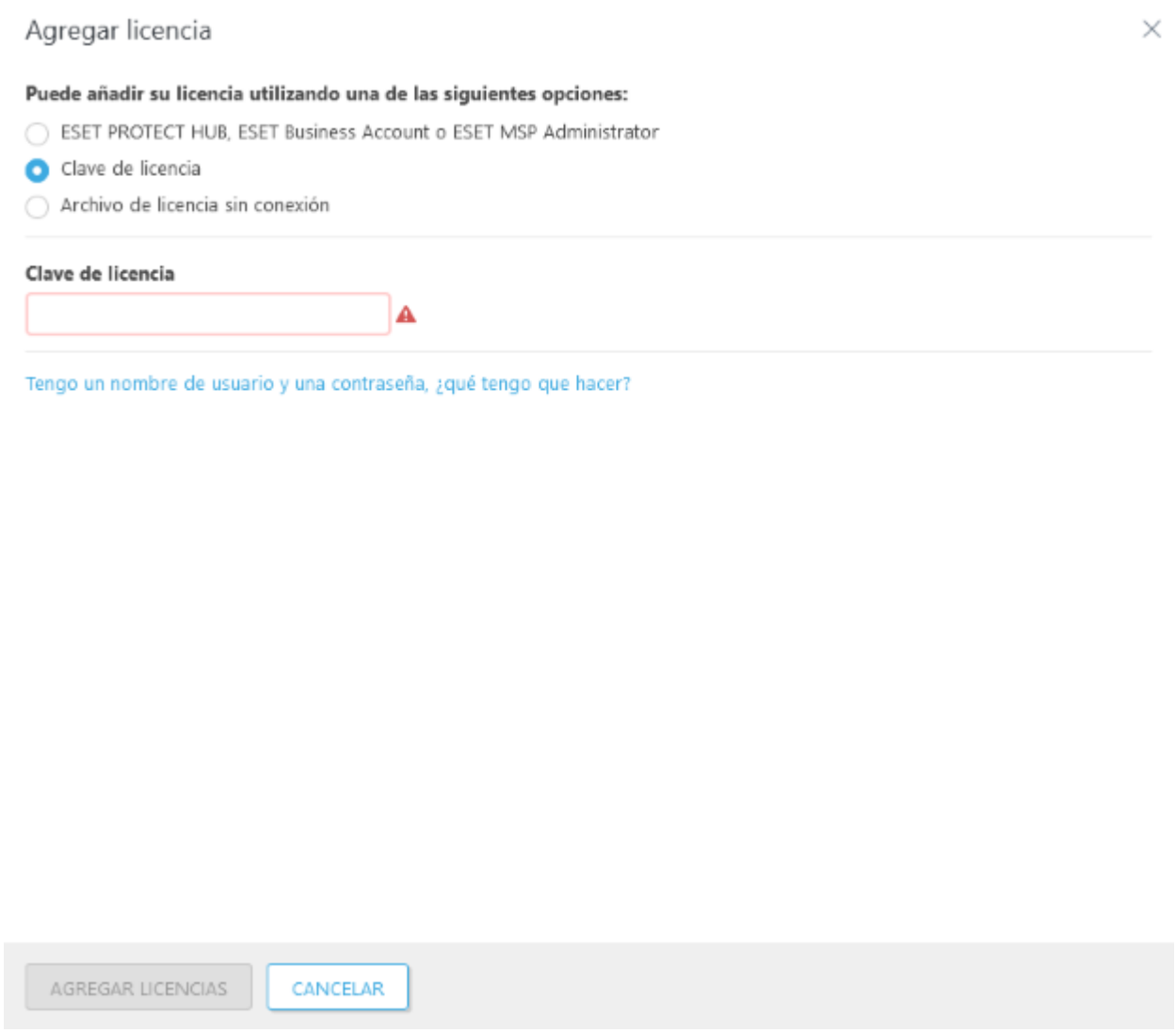
Agregar licencia: clave de licencia

Solo los administradores cuyo grupo de inicio sea **Todos** y tengan permiso de **Escritura** para las licencias del grupo de inicio pueden agregar o quitar licencias. Cada licencia está identificada por su **ID público** y puede contener una o más unidades. Solo el administrador puede distribuir licencias entre otros usuarios que tengan los 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 va a utilizar credenciales de licencias en el formato antiguo (nombre de usuario y contraseña), conviértalas en una clave de licencia. Si la licencia no está registrada, se activará el proceso de registro, que se efectúa en el portal EBA (ESET PROTECT On-Prem facilitará la URL válida para el registro basándose en el origen de la licencia).



Activación sin conexión

Puede utilizar un archivo de licencia del portal de ESET Business Account para activar ESET PROTECT On-Prem y otros productos de seguridad de ESET.

- Cada archivo de licencia sin conexión se genera solo para un producto, por ejemplo, ESET Endpoint Security.

- La licencia sin conexión solo debe utilizarse para clientes que nunca tendrán acceso a los servidores de licencias de ESET (aunque un cliente esté conectado a Internet mediante un proxy con acceso limitado únicamente a los servicios de ESET, no utilice la licencia sin conexión).

- No es posible crear un archivo de licencia sin conexión a partir de una licencia de suscripción.

Para sustituir una licencia sin conexión existente, debe

1. Eliminar la licencia antigua de ESET PROTECT On-Prem y el archivo de licencia de ESET Business Account.

2. Crear una nueva licencia sin conexión en ESET Business Account.
3. Importar la nueva licencia en ESET PROTECT On-Prem

4. Volver a activar los productos con la nueva licencia.

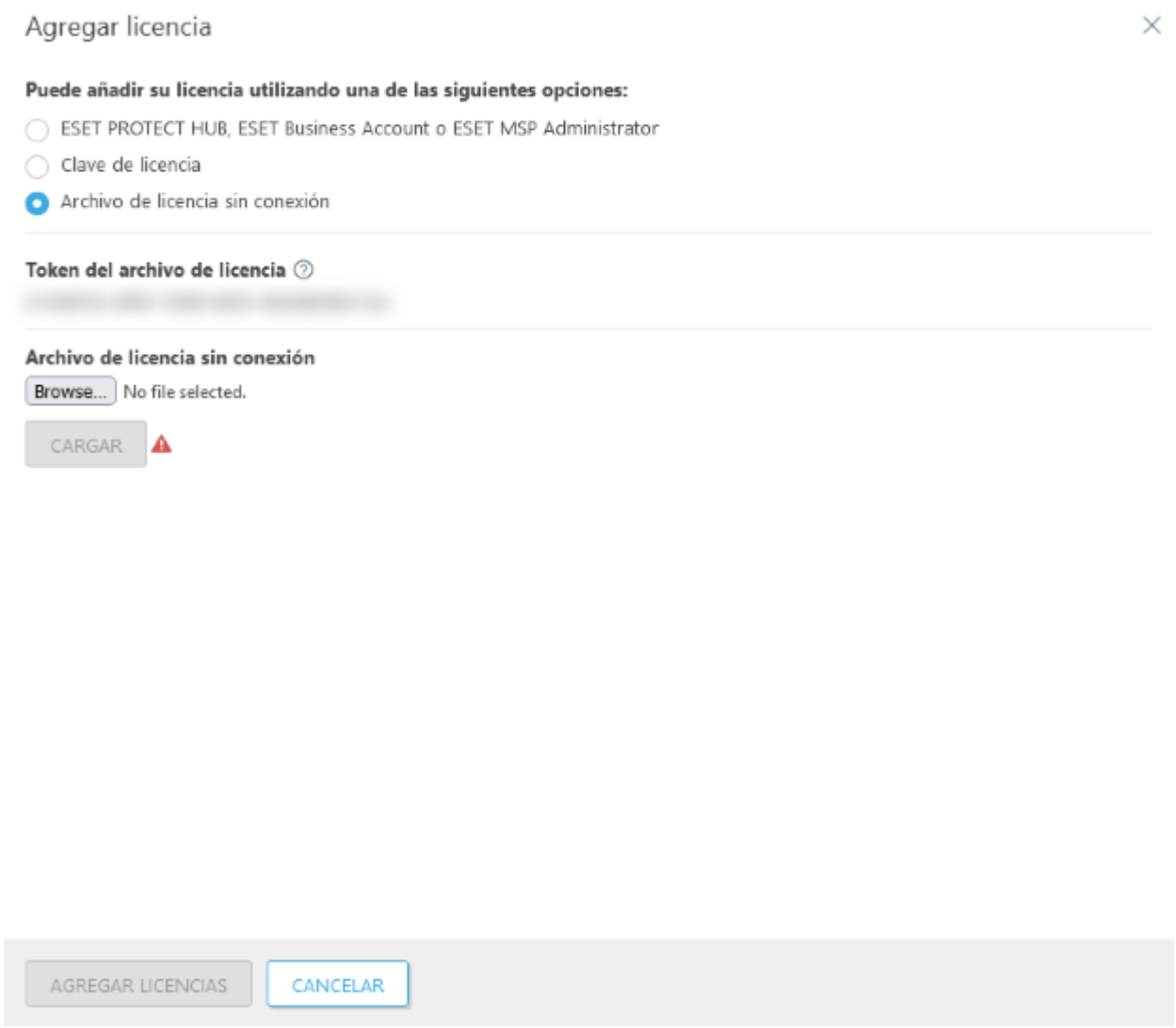
Solo los administradores cuyo grupo de inicio sea **Todos** y tengan permiso de **Escritura** para las licencias del grupo de inicio pueden agregar o quitar licencias. Cada licencia está identificada por su **ID público** y puede contener una o más unidades. Solo el administrador puede distribuir licencias entre otros usuarios que tengan los permisos suficientes. Las licencias no son reducibles.

Archivo de licencia sin conexión

Para crear e importar un archivo de licencia sin conexión, siga este procedimiento:

1. Diríjase a **Administración de licencias** en ESET PROTECT On-Prem y haga clic en **Acciones** > **Agregar licencias**.

2. Seleccione el **Archivo de licencia sin conexión** y copie un **Token del archivo de licencia** específico.

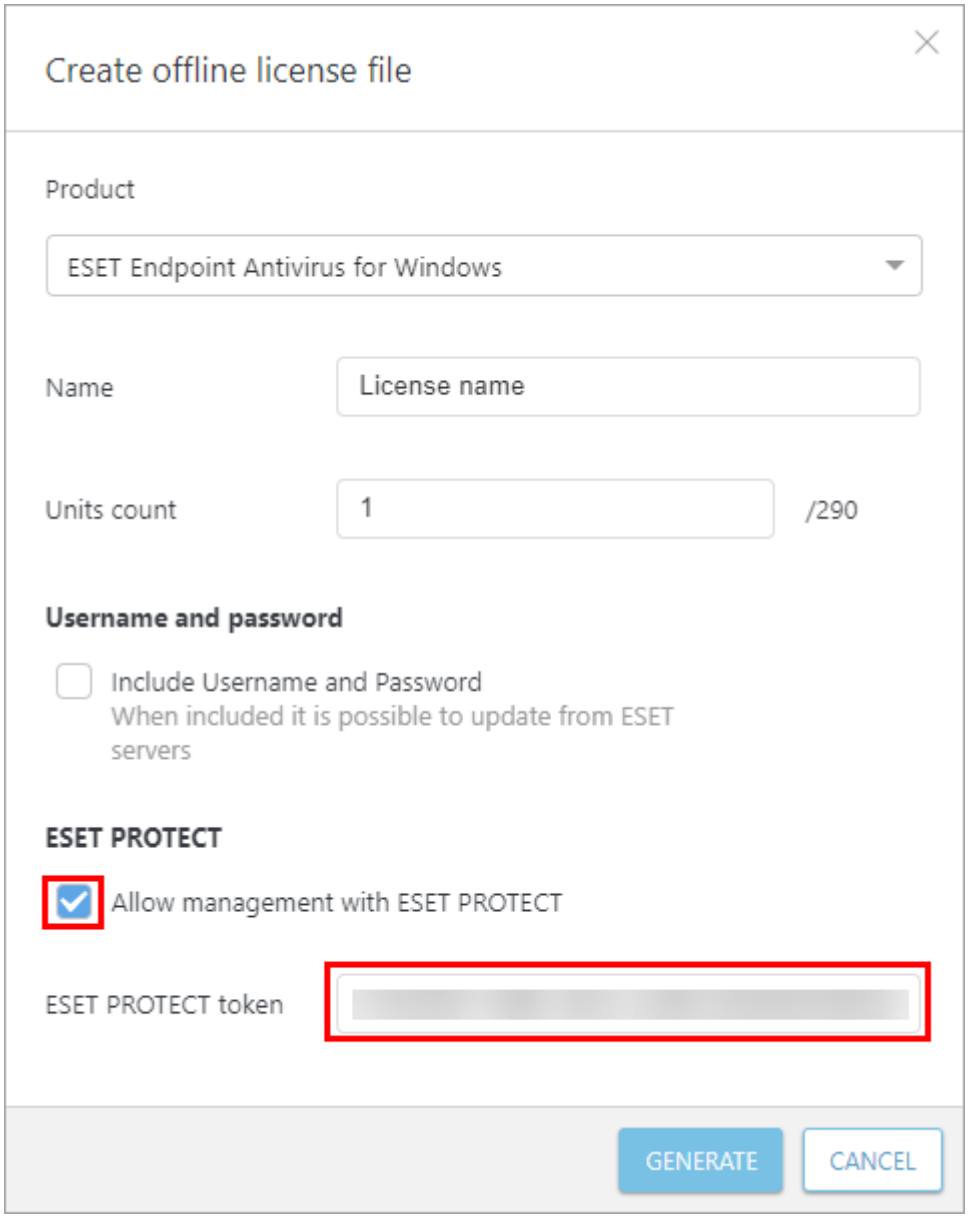


3.Inicie sesión en su ESET Business Account, donde ha importado su licencia.

4.Seleccione la licencia que desee exportar y seleccione **Crear archivos sin conexión**.

5.Seleccione un producto para este archivo de licencia, introduzca el **Nombre** del archivo y su **Número de unidades** (número de puestos exportados al archivo de licencia).

6.Marque la casilla situada junto a **Permitir administración con ESET PROTECT On-Prem** e introduzca el token de **ESET PROTECT On-Prem** (**Token del 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**.

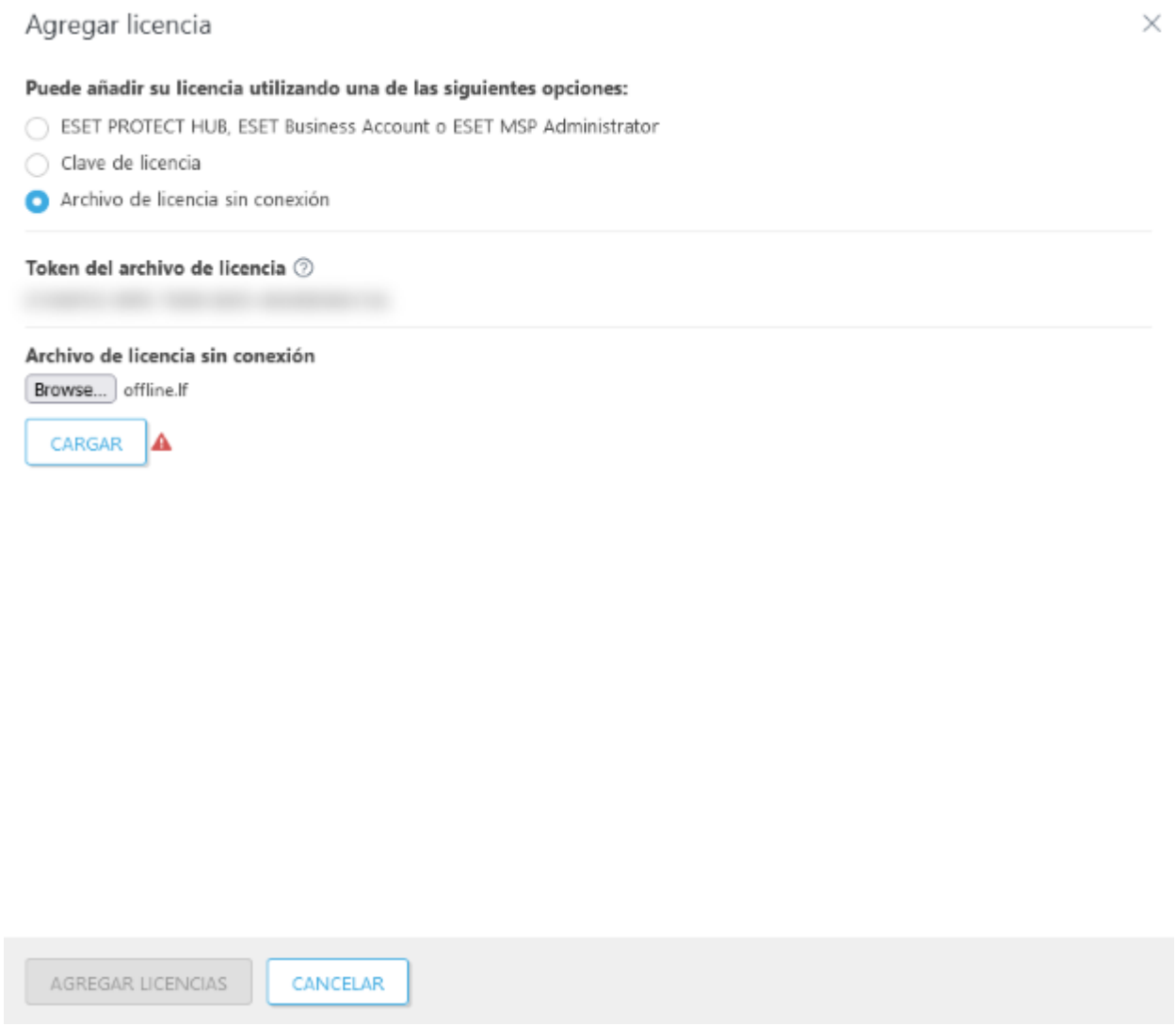
2.Seleccione la ficha **Archivos sin conexión**.

3.Haga clic en el archivo de licencia que ha creado (puede distinguirlo por el nombre) y seleccione **Descargar**.

Vuelva a **Administración de licencias** en 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, a continuación, haga clic en **Agregar licencias**.



Derechos de acceso

Los derechos de acceso le permiten administrar usuarios de ESET PROTECT Web Console y sus permisos.

El modelo de seguridad

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

Término	Explicación
Grupo principal	El grupo principal es el grupo en el que se almacenan automáticamente todos los objetos (dispositivos, tareas, plantillas, etc.) que un usuario crea. Cada usuario solo debe tener un grupo principal.
Objeto	Los objetos se sitúan en **Grupos estáticos**. El acceso a los objetos es a través de grupos, no usuarios (proporcionar acceso por grupo facilita la participación de varios usuarios, por ejemplo, cuando un usuario está de vacaciones). Las excepciones son las tareas del servidor y las notificaciones, que requieren un usuario "ejecutante".
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 cuyo grupo principal sea **Todo** y que tenga un conjunto de permisos completo sobre este grupo es, a efectos prácticos, un administrador.
Derecho de acceso	El derecho para acceder a un objeto o ejecutar una tarea se asigna mediante un conjunto de permisos. Consulte la lista de todos los derechos de acceso y sus funciones para obtener más detalles.
Conjunto de permisos	Un conjunto de permisos representa los permisos de los usuarios que acceden a ESET PROTECT Web Console. Estos permisos definen lo que pueden hacer o ver los usuarios en ESET PROTECT Web Console. A un usuario pueden asignársele varios conjuntos de permisos. Los conjuntos de permisos solo se aplican a objetos de grupos definidos. Estos **Grupos estáticos** se configuran en la sección **Grupos estáticos** al crear o modificar un conjunto de permisos.
Funcionalidad	Una funcionalidad es un tipo de objeto o acción. Normalmente, las funcionalidades reciben estos valores: **Lectura**, **Escritura**, **Uso**. La combinación de funcionalidades aplicadas a un Grupo de acceso recibe el nombre de Conjunto de permisos.

Lista de ejemplos relacionados con los derechos de acceso

Hay distintos ejemplos en la guía de administración sobre derechos de acceso. Esta es la lista de dichos ejemplos:

- Cómo duplicar las políticas

- Diferencia entre Uso y Escritura
- Cómo crear una solución para administradores de sucursales
- Cómo compartir objetos mediante la duplicación
- Cómo dividir el acceso a certificados y autoridades
- Cómo permitir que los usuarios creen instaladores
- Cómo quitar las notificaciones
- Cómo crear directivas
- Permitir que los usuarios vean todas las políticas
- Compartir licencias entre administradores de sucursales

Usuarios

La administración de los usuarios es parte de la sección **Más** de ESET PROTECT Web Console.

- Crear un usuario nativo
- Acciones y detalles del usuario
- Cambiar la contraseña del usuario
- Usuarios asignados
- Asignar un conjunto de permisos a un usuario

Hay dos tipos de usuario:

- Usuarios nativos: cuentas de usuario creadas y administradas desde ESET PROTECT Web Console.
- Grupos de seguridad de dominio asignados: cuentas de usuario administradas y autenticadas por Active Directory.

Cuando se configura ESET PROTECT On-Prem por primera vez, el único usuario es el **Administrador** (usuario nativo con el grupo de inicio **Todo** y acceso a todo).
• No se recomienda utilizar esta cuenta de usuario regularmente. Se recomienda encarecidamente crear otra cuenta de "administración" o utilizar administradores de grupos de seguridad de dominio con el conjunto de permisos del administrador asignado. Utilice la cuenta de administrador predeterminada únicamente como una opción de respaldo.
• También puede crear cuentas de usuario adicionales con menos derechos de acceso según las competencias deseadas de la cuenta.
• Opcionalmente, puede configurar Autenticación de doble factor para usuarios nativos y grupos de seguridad de dominio asignados. Esto aumentará la seguridad al iniciar sesión y acceder a ESET PROTECT Web Console.

Solución para administradores de sucursales

Si una empresa tiene dos oficinas, cada una con administradores locales, deben asignárseles más conjuntos de permisos para grupos diferentes.
Supongamos que *John* es el administrador de *San Diego* y *Larry* es el administrador de *Sídney*. Ambos deben ocuparse únicamente de sus ordenadores locales y utilizar **Paneles, Políticas, Informes** y **Plantillas de grupos dinámicos** con sus equipos. El *administrador* principal debe seguir estos pasos:
1.Crear grupos estáticos nuevos: *Oficina de San Diego*, *Oficina de Sídney.*
2.Crear nuevos conjuntos de permisos:
a)**Conjunto de permisos** llamado *Conjunto de permisos de Sídney*, con el grupo estático *Oficina de Sídney*, y con permisos de acceso totales (excepto **Configuración del servidor**).
b)**Conjunto de permisos** llamado *Conjunto de permisos de San Diego*, con el grupo estático *Oficina de San Diego*, y con permisos de acceso totales (excepto **Configuración del servidor**).
c)**Conjunto de permisos** llamado *Todos los grupos/paneles*, con el grupo estático *Todo*, y con los siguientes permisos:

- **Lectura** en **Tareas del cliente**
- **Uso** en **Plantillas de grupos dinámicos**
- **Uso** en **Informes y paneles**
- **Uso** en **Políticas**
- **Uso** en **Enviar correo electrónico**
- **Uso** en **Enviar captura de SNMP**
- **Uso** en **Exportar informe a un archivo**
- **Uso** en **Licencias**
- **Escritura** en **Notificaciones**

3.Crear el nuevo usuario *John*, con grupo de inicio *Oficina de San Diego*, y asignarle los conjuntos de permisos *Conjunto de permisos de San Diego* y *Todos los grupos/paneles*.
4.Crear el nuevo usuario *Larry*, con grupo principal *Oficina de Sídney,* y asignarle los conjuntos de permisos *Conjunto de permisos de Sídney* y *Todos los grupos/paneles*.
Si se configuran así los permisos, *John* y *Larry* podrán utilizar los mismos informes, tareas, políticas y paneles y utilizar plantillas de grupos dinámicos sin restricciones; no obstante, solo podrán utilizar las plantillas de los ordenadores de sus grupos principales.

Uso compartido de objetos

Si un administrador quiere compartir objetos, como plantillas de grupos dinámicos, plantillas de informes o políticas, tiene a su disposición las siguientes opciones:

- Mover esos objetos a grupos compartidos

- Crear objetos duplicados y moverlos a grupos estáticos accesibles a otros usuarios (ver ejemplo a continuación)

Para duplicar un objeto, el usuario debe tener permiso de **Lectura** del objeto original y permiso de **Escritura** en su **Grupo principal** para este tipo de acción.

El *administrador*, cuyo grupo principal es *Todo,* quiere compartir *Plantilla especial* con el usuario *John*. La plantilla la creó el *administrador*, por lo que está en el grupo *Todo*. El *administrador* debe seguir estos pasos:

1.Desplácese hasta **Más** > **Plantillas de grupos dinámicos**.

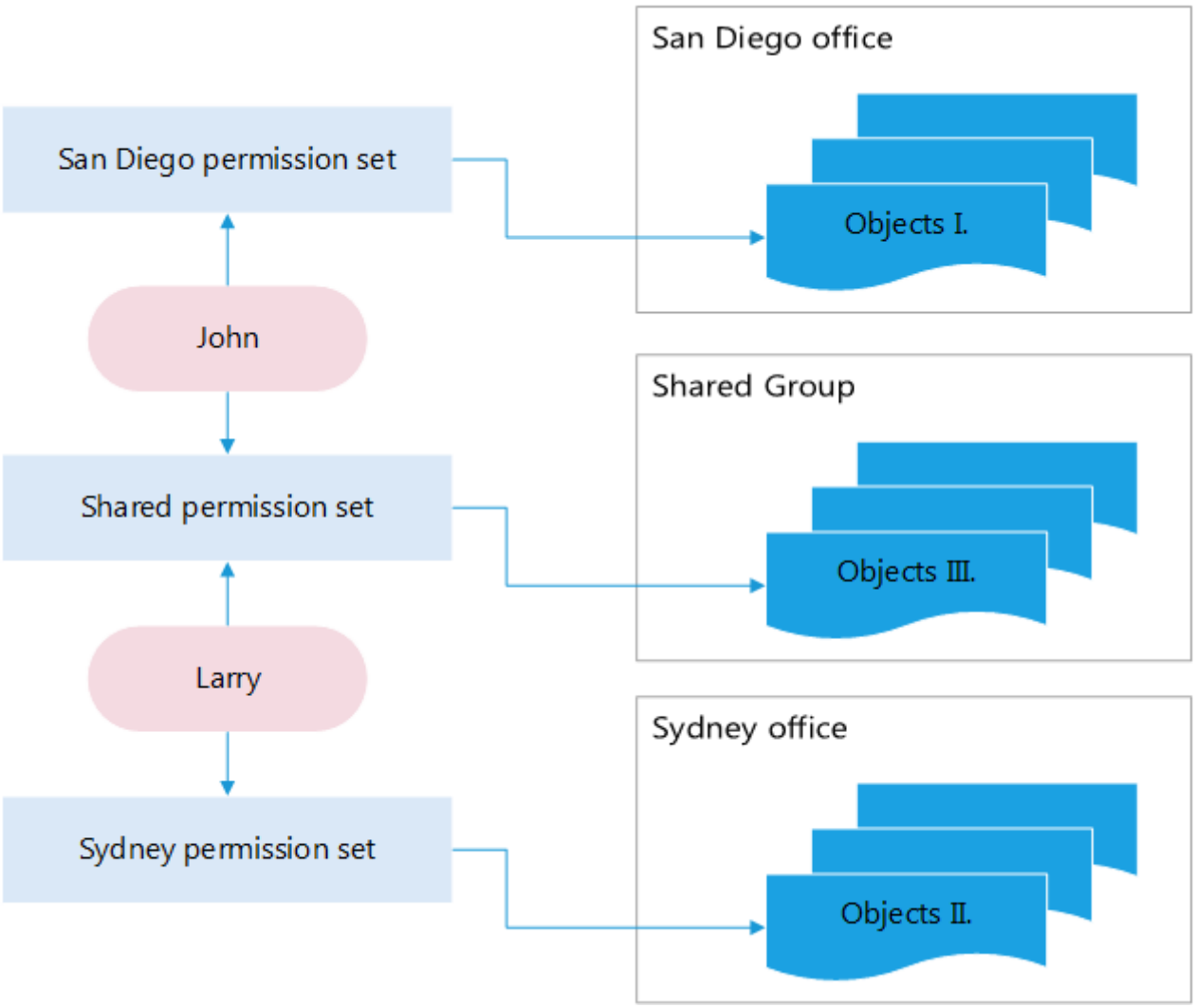
2.Seleccione *Plantilla especial* y haga clic en **Duplicar**; si es necesario, configure el nombre y la descripción y haga clic en **Finalizar**.

3.La plantilla duplicada estará en el grupo principal del *administrador*, el grupo *Todo*.

4.Desplácese hasta **Más** > **Plantillas de grupos dinámicos** y seleccione la plantilla duplicada; haga clic en **Grupo de acceso** > **Mover** y seleccione el grupo estático de destino (en el que *John* tiene los permisos correspondientes). Haga clic en **Aceptar**.

Cómo compartir objetos entre más usuarios mediante un grupo compartido

Para comprender mejor cómo funciona el nuevo modelo de seguridad, consulte el siguiente esquema. Existe una situación en la que hay dos usuarios creados por el administrador. Cada usuario tiene su propio grupo principal con los objetos que ha creado. El *Conjunto de permisos de San Diego* otorga a *John* el derecho de manipular los *objetos* de su grupo principal. La situación es similar para *Larry*. Si estos usuarios tienen que compartir objetos (por ejemplo, ordenadores), estos objetos deben moverse a *Grupo compartido* (un grupo estático). Debe asignarse a ambos usuarios el *Conjunto de permisos compartido* con *Grupo compartido* en la sección **Grupos estáticos**.



Filtros y personalización del diseño

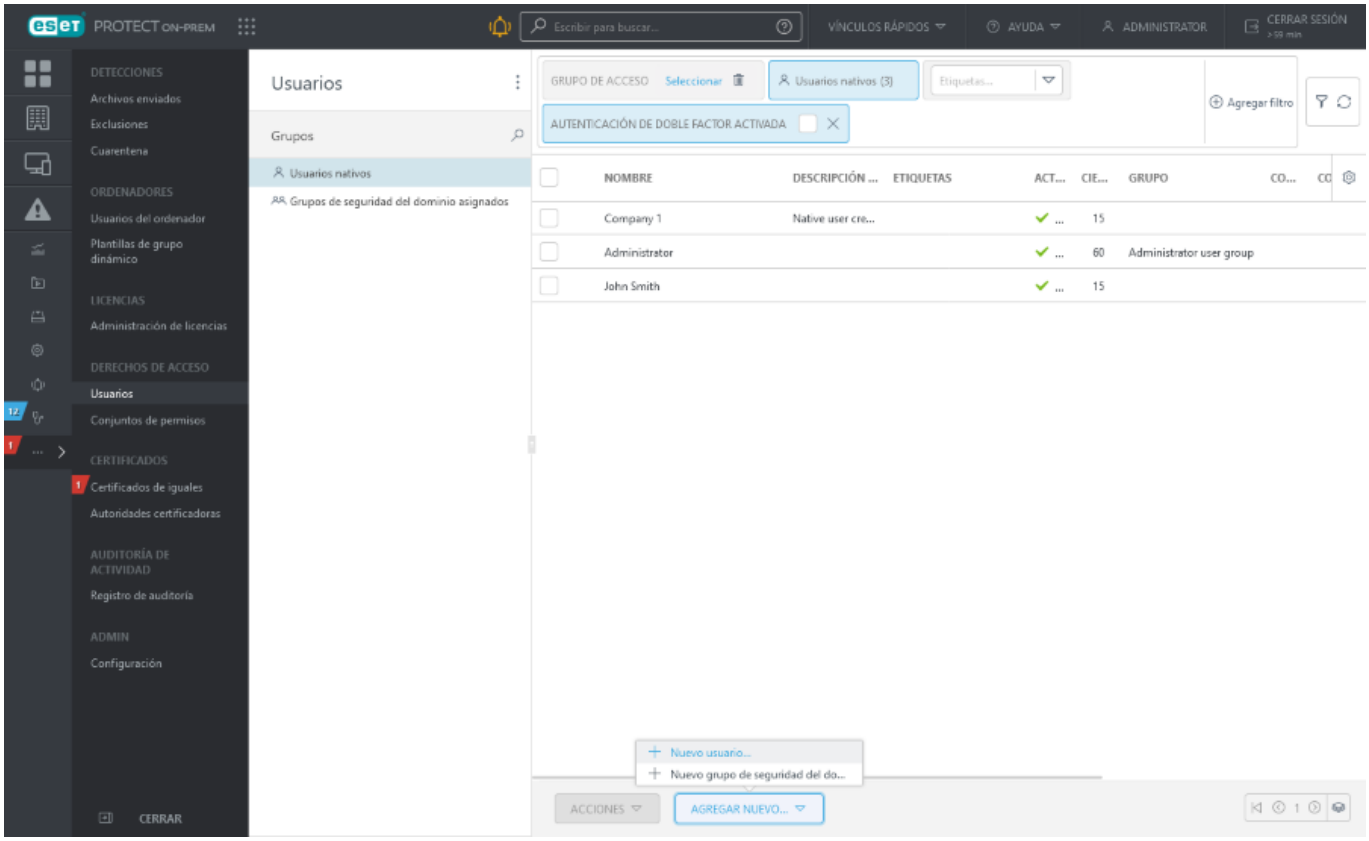
Puede personalizar la vista de pantalla actual de Web Console:

- Agregar filtros y preajustes de filtros.
- 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 correctamente el usuario, se recomienda seguir estos pasos:
> 1.Decida qué grupo estático será el grupo principal del usuario. Si es necesario, cree el grupo.
> 2.Decida qué conjunto de permisos es el más conveniente para el usuario. Si es necesario, cree un nuevo conjunto de permisos.
> 3.Siga las instrucciones de este capítulo y cree el usuario.



Básico

Introduzca un nombre de **usuario** y una **descripción** opcional para el nuevo usuario.

Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

Seleccione **Grupo principal**. Este es el grupo estático donde se guardarán automáticamente todos los objetos creados por este usuario.

Grupo de inicio – El grupo de inicio 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 derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "Department_1" como **grupo de inicio** de la tarea del cliente.

Si el grupo de inicio preseleccionado no cumple sus expectativas, puede seleccionar uno manualmente.

Establecer contraseña

La contraseña del usuario debe tener al menos 8 caracteres. La contraseña no debe contener el nombre de usuario.

Cuenta

Activado: seleccione esta opción si no desea que la cuenta esté desactivada (si tiene pensado utilizarla más

tarde).

Es necesario cambiar la contraseña: seleccione esta opción para obligar al usuario a cambiar la contraseña la primera vez que inicia sesión en ESET PROTECT Web Console.

Caducidad de la contraseña (días): esta opción define el número de días que es válida la contraseña (debe cambiar la contraseña una vez que caduque).

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 seleccionar una competencia predefinida (indicada a continuación) o puede utilizar un conjunto de permisos personalizado.

- **Conjunto de permisos del revisor** (derechos de solo lectura para el grupo **Todo**).
- **Conjunto de permisos del administrador** (acceso completo para el grupo **Todo**)
- **Conjunto de permisos de instalación asistida por el servidor** (derechos de acceso mínimos necesarios para la instalación asistida por el servidor)
- **Conjunto de permisos del revisor de ESET Inspect**: derechos mínimos de acceso de solo lectura (para el grupo **Todo**) que necesita un usuario de ESET Inspect On-Prem.
- **Conjunto de permisos del servidor de ESET Inspect**: derechos de acceso (para el grupo **Todo**) que se necesitan para el proceso de instalación de ESET Inspect On-Prem y la posterior 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**) que necesita un usuario de ESET Inspect On-Prem.

Cada conjunto de permisos contiene permisos que solo se refieren a los objetos de los **Grupos estáticos** seleccionados en dicho conjunto de permisos.

Los usuarios sin ningún conjunto de permisos no podrán iniciar sesión en Web Console.

⚠ Todos los conjuntos de permisos predefinidos tienen el grupo **Todo** en la sección **Grupos estáticos**. Tenga esto en cuenta al asignárselos a un usuario. Los usuarios tendrán estos permisos en todos los objetos de ESET PROTECT On-Prem.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear el usuario.

Acciones y detalles del usuario

Para administrar un usuario, seleccione el usuario en cuestión y seleccione una de las acciones disponibles:

Acciones

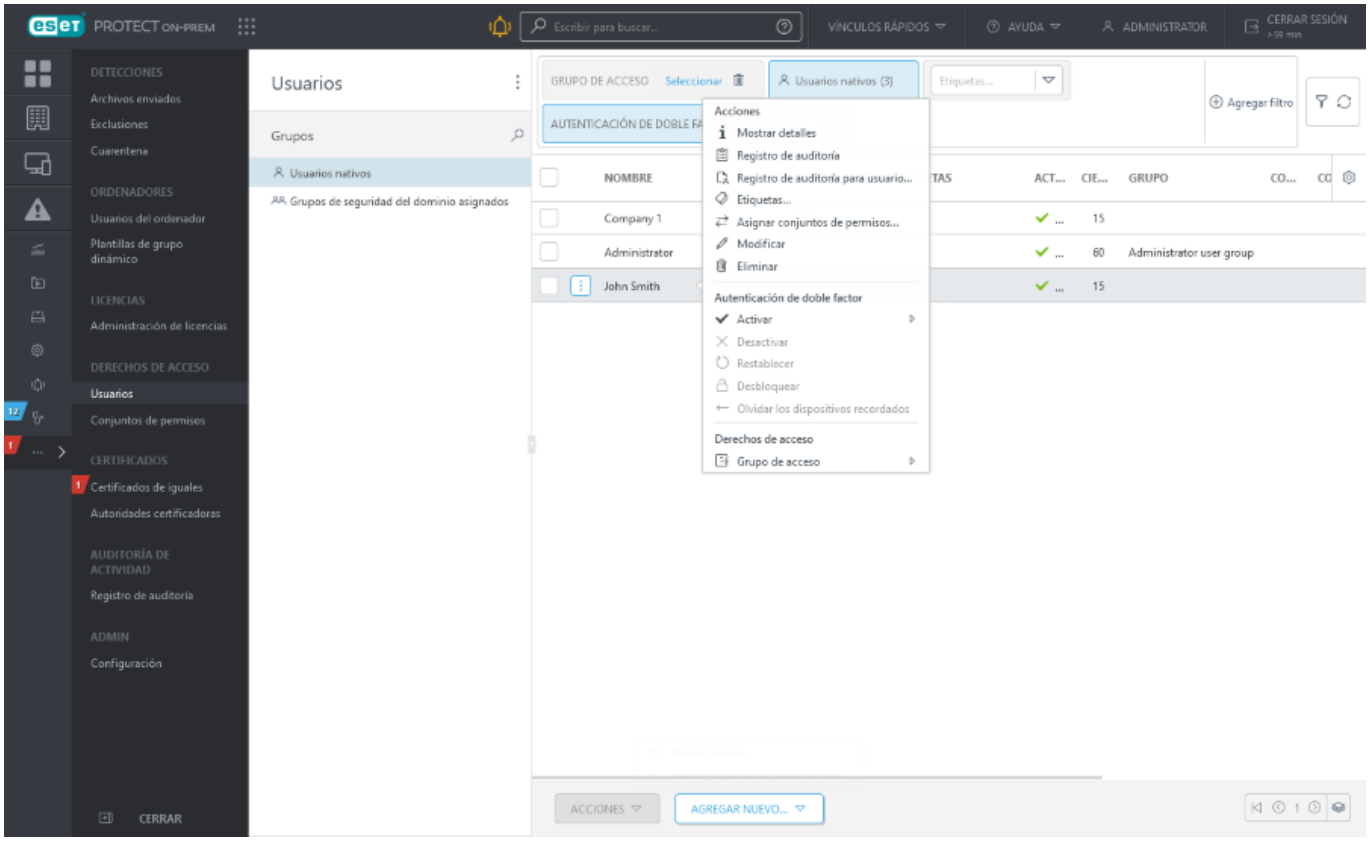
- **Mostrar detalles**: permite ver los detalles del usuario.
- **Registro de auditoría**: muestra el Registro de auditoría de todos los usuarios.
- **Registro de auditoría para usuario seleccionado**: permite ver el Registro de auditoría del usuario seleccionado.
- **Etiquetas** - Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
- **Asignar conjuntos de permisos**: asigne un conjunto de permisos al usuario.
- **Editar**: edite la configuración del usuario.
- **Eliminar**: permite eliminar el usuario.

Autenticación de doble factor

- **Activar**: active la autenticación de doble factor para el usuario.
- **Desactivar**: desactive la autenticación de doble factor existente para el usuario.
- **Restablecer**: restablezca la configuración de autenticación de doble factor del usuario.
- **Desbloquear**: si el usuario se ha bloqueado, puede desbloquearlo con este ajuste.
- **Olvidar los dispositivos memorizados**: requiera autenticación de doble factor del usuario en los dispositivos recordados.

Derechos de acceso

- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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

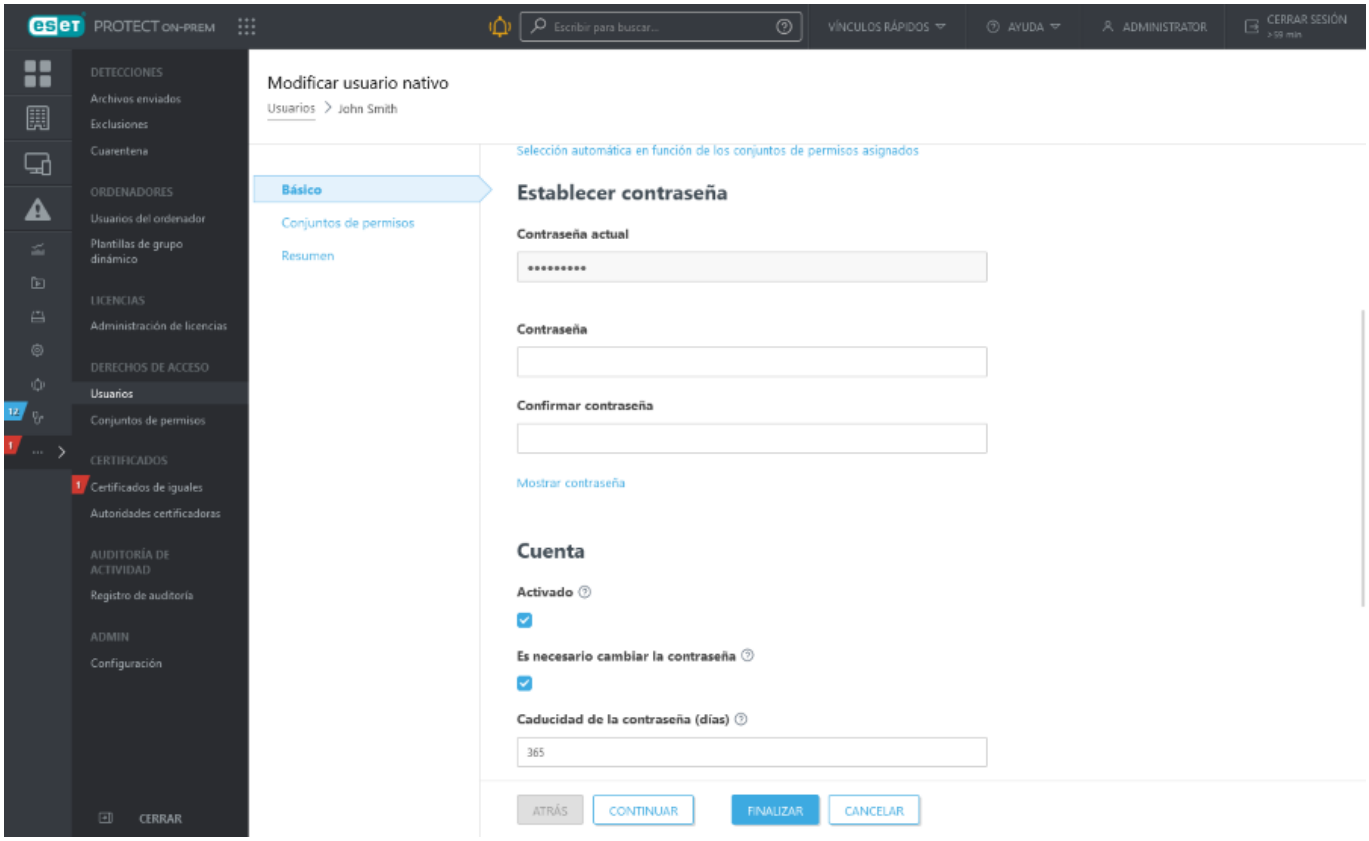
Hay dos secciones en los detalles del usuario:

- **Visión general**: información básica sobre el usuario. Puede administrar el usuario con los botones **Acciones** y **Autenticación de doble factor** situados en la parte inferior.
- **Conjuntos de permisos**: la lista de conjuntos de permisos asignados al usuario. Haga clic en un conjunto de permisos para administrarlo.

Cambiar la contraseña del usuario

Puede cambiar la contraseña de cualquier usuario para el que tenga derechos de acceso. Debe tener permisos de escritura en el grupo estático en el que está almacenado el usuario. El usuario está almacenado en el grupo de inicio del usuario principal.

1. Haga clic en **Más** > **Usuarios**.
2. Seleccione el usuario y haga clic en **Modificar**.
3. En la sección **Básico**, desplácese hasta **Establecer contraseña**.
4. Si está modificando el usuario que ha iniciado sesión, debe introducir la **Contraseña actual**. Cuando se editan otros usuarios, el campo de **Contraseña actual** se rellena previamente.
5. Introduzca la nueva contraseña en los campos **Contraseña** y **Confirmar contraseña**.
6. Haga clic en **Finalizar**.

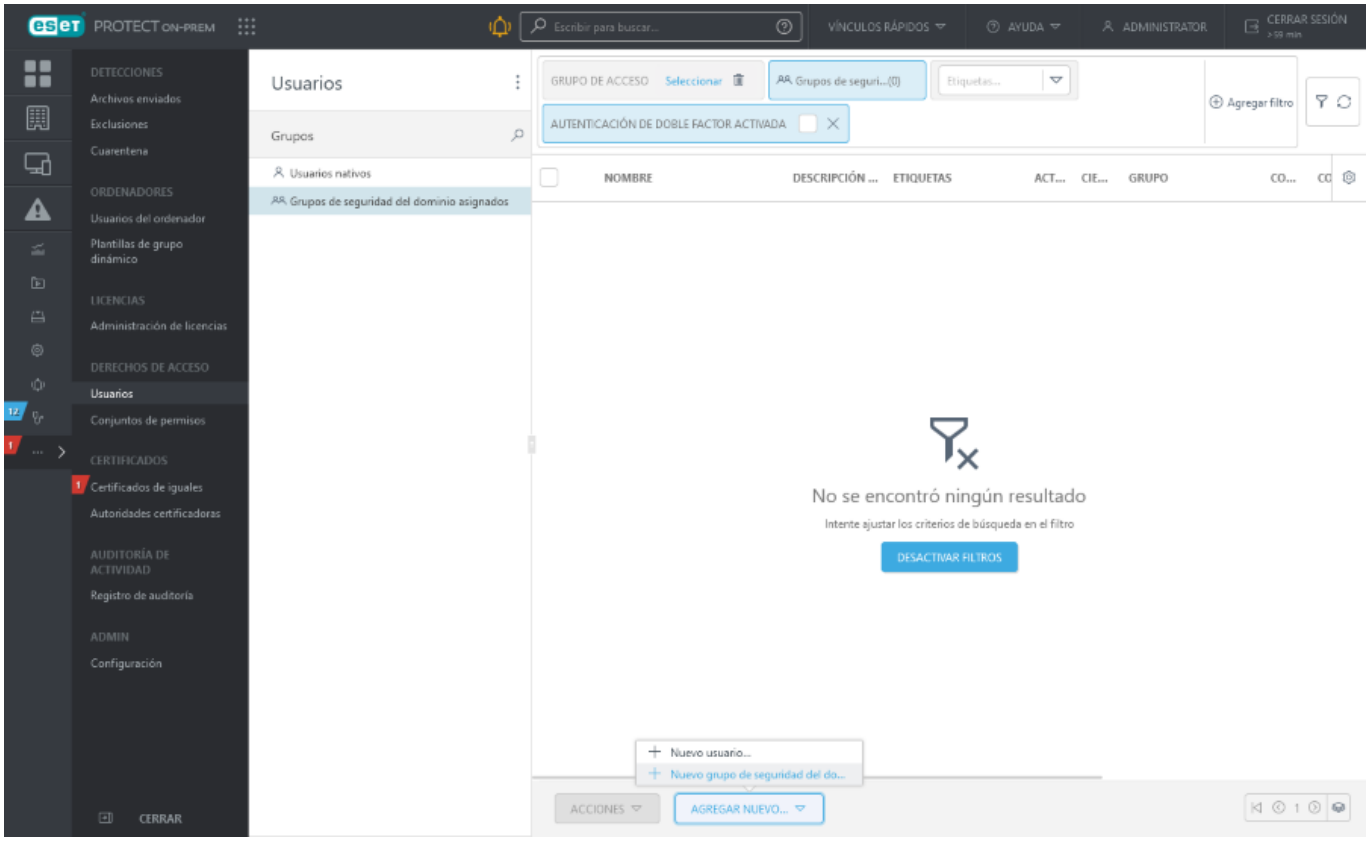


Asignar usuarios del Grupo de seguridad del dominio

Puede asignar un grupo de seguridad de dominio al ESET PROTECT Server y permitir que los usuarios existentes (miembros de estos grupos de seguridad de dominio) se conviertan en usuarios de ESET PROTECT Web Console.

Esta función solo está disponible para sistemas con Active Directory.

Para acceder al **Asistente para grupo de seguridad del dominio asignado**, diríjase a **Más** > **Usuarios** > **Agregar nuevo** > **Nuevo grupo de seguridad del dominio asignado**.



Básico

Grupo de dominio

Escriba el **Nombre** de este grupo. También puede escribir una **Descripción** del grupo.

Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

Seleccione **Grupo principal**. Este es el grupo estático donde se guardarán automáticamente todos los objetos creados por los usuarios de este grupo de dominio.

Grupo de inicio – El grupo de inicio 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 derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "Department_1" como **grupo de inicio** de la tarea del cliente.

Si el grupo de inicio preseleccionado no cumple sus expectativas, puede seleccionar uno manualmente.

Este grupo de dominio estará definido por un **SID de grupo** (identificador de seguridad). Haga clic en **Seleccionar** para elegir un grupo de la lista y, a continuación, en **Aceptar** para confirmar. Su instancia de ESET PROTECT Server debe unirse al dominio o de lo contrario no habrá grupos en la lista si está utilizando el dispositivo virtual, consulte el capítulo relacionado.

- Si LDAPS no está disponible, puede asignar el grupo de seguridad del dominio:
  - mediante la desactivación temporal de la configuración de Active Directory en **Más** > Configuración > **Configuración avanzada** > **Active Directory**.
  - escribiendo el SID de grupo manualmente.
- Si sigue recibiendo un mensaje de error tras hacer clic en Seleccionar y tiene AD correctamente configurado, puede que se haya agotado el tiempo de espera del proceso en segundo plano. Puede intentar las siguientes medidas:
  - Introducir el SID de forma manual para evitar el error.
  - Introducir sus credenciales de AD en **Más** > Configuración > **Configuración avanzada** > **Active Directory**. En este caso, ESET PROTECT On-Prem utilizará una forma distinta y más rápida de recuperar la lista de SID.

Cuenta

Activado: seleccione esta opción si no desea que la cuenta esté desactivada (si tiene pensado utilizarla más tarde).

Cierre de sesión automático (min): esta opción define el periodo de inactividad (en minutos) tras el cual se cierra la sesión del usuario en Web Console.

Contacto por correo y **Contacto** por teléfono se pueden definir para ayudar a identificar al grupo.

Conjuntos de permisos

Asigne competencias (derechos) a los usuarios de este grupo.

Los conjuntos de permisos se establecen para el grupo de seguridad del dominio de Active Directory (en lugar de para usuarios concretos, como ocurre en el caso de **Usuario nativo**).

Puede asignar varios conjuntos de permisos a un grupo de seguridad del dominio.

Puede seleccionar una competencia predefinida (indicada a continuación) o puede utilizar un conjunto de permisos personalizado.

- **Conjunto de permisos del revisor** (derechos de solo lectura para el grupo **Todo**).
- **Conjunto de permisos del administrador** (acceso completo para el grupo **Todo**)
- **Conjunto de permisos de instalación asistida por el servidor** (derechos de acceso mínimos necesarios para la instalación asistida por el servidor)
- **Conjunto de permisos del revisor de ESET Inspect**: derechos mínimos de acceso de solo lectura (para el grupo **Todo**) que necesita un usuario de ESET Inspect On-Prem.
- **Conjunto de permisos del servidor de ESET Inspect**: derechos de acceso (para el grupo **Todo**) que se necesitan para el proceso de instalación de ESET Inspect On-Prem y la posterior 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**) que necesita un usuario de ESET Inspect On-Prem.

Cada conjunto de permisos contiene permisos que solo se refieren a los objetos de los **Grupos estáticos** seleccionados en dicho conjunto de permisos.

Los usuarios sin ningún conjunto de permisos no podrán iniciar sesión en Web Console.

> ⚠ Todos los conjuntos de permisos predefinidos tienen el grupo **Todo** en la sección **Grupos estáticos**. Tenga esto en cuenta al asignárselos a un usuario. Los usuarios tendrán estos permisos en todos los objetos de ESET PROTECT On-Prem.

Resumen

Revise las opciones configuradas para este usuario y haga clic en **Finalizar** para crear el grupo.

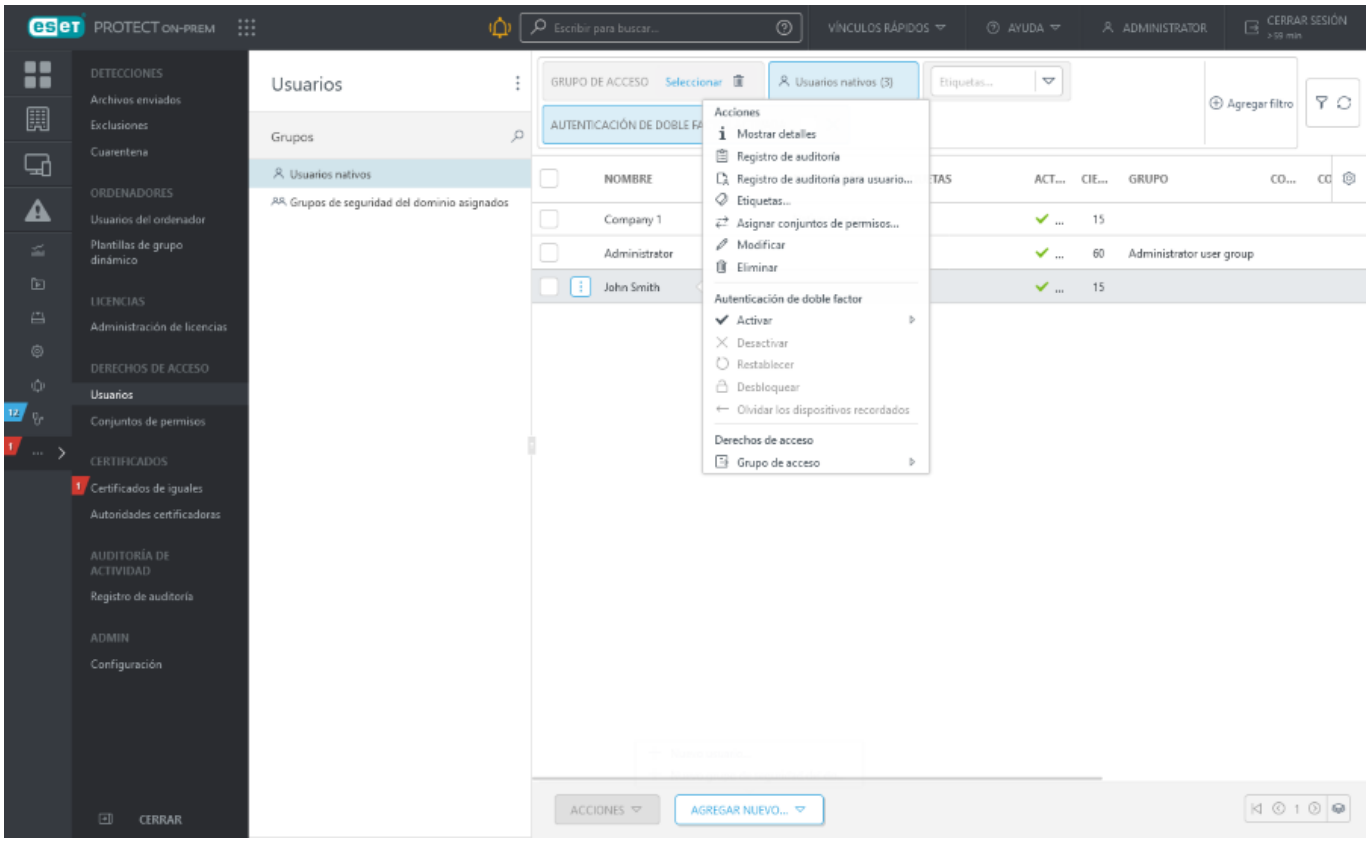
Los usuarios aparecerán en los **Grupos de seguridad del dominio asignados** después de iniciar sesión por primera vez.

Asignar un conjunto de permisos a un usuario

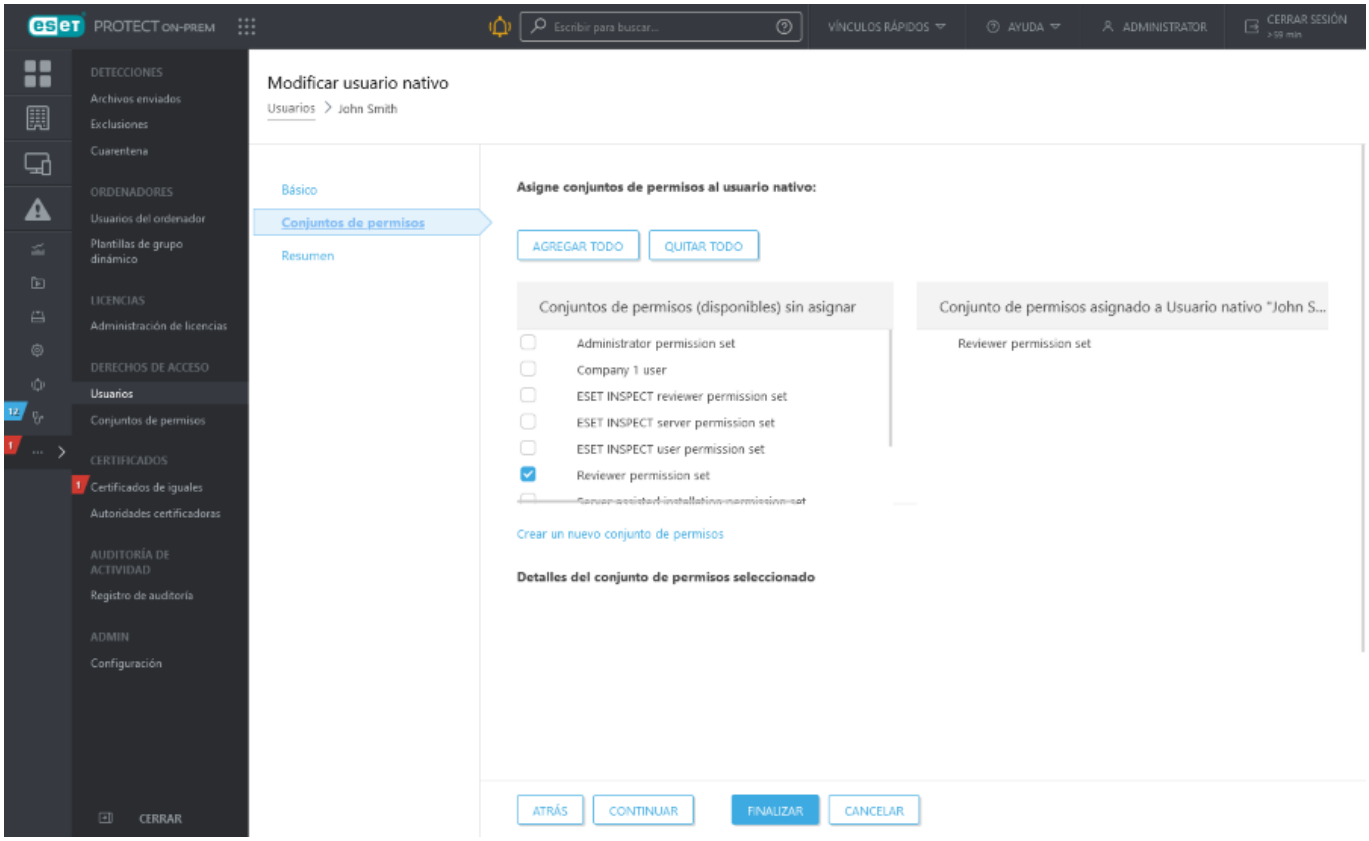
1. Hay dos formas de asignar un conjunto de permisos a un usuario:

   a)Haga clic en **Más** > **Usuarios** > haga clic en un usuario y seleccione **Asignar conjuntos de permisos** para asignar conjuntos de permisos específicos al usuario.

   b)En la sección **Usuarios**, haga clic en **Editar**para modificar un usuario específico.



2. Marque la casilla situada junto a un Conjunto de permisos en la sección **Conjuntos de permisos (disponibles) sin asignar**. Consulte Administrar conjuntos de permisos si desea más información.



Autenticación de doble factor

La autenticación de doble factor (2FA) ofrece una alternativa más segura de inicio de sesión y acceso a ESET PROTECT Web Console. 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 en el número de usuarios que pueden iniciar sesión en ESET PROTECT On-Prem mediante la autenticación de doble factor.
- La configuración de **Proxy HTTP** no se aplica para la comunicación con autenticación de doble factor (2FA).
- Puede activar la autenticación de doble factor también para la cuenta de Administrador.

Requisitos previos

- Para activar la autenticación de doble factor para otro usuario, el usuario actual necesita el permiso de **Escritura** sobre ese usuario. Cuando se activa este método, el usuario debe configurar la autenticación de doble factor antes de iniciar sesión. Cada usuario recibirá un enlace a través de un mensaje de texto (SMS) que puede abrir en el navegador web de su teléfono para consultar las instrucciones de configuración de la autenticación de doble factor.
- La autenticación de doble factor no funciona sin acceso de red directo a los servidores de autenticación de doble factor de ESET. Es necesario permitir como mínimo acceso a los servidores de autenticación de doble factor dentro del cortafuegos. Si el proxy está configurado en **Más** > **Configuración** > **Configuración avanzada** > **Proxy HTTP**, no se aplica a la autenticación de doble factor.

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

Activa la autenticación de doble factor para un usuario de la Consola web

1. Cree un nuevo usuario o utilice 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 doble factor** > **Activar**. A continuación, seleccione la opción que prefiera usar:

   • **ESET Secure Authentication**: ESET proporciona la autenticación de doble factor mediante su 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 ESET PROTECT On-Prem 9.1 y versiones posteriores, puede utilizar un cliente de autenticación de terceros que admita el protocolo TOTP necesario. Hemos probado las siguientes aplicaciones: Google Authenticator, Microsoft Authenticator y Authy.

4. La próxima vez que el usuario inicie sesión, escriba su número de teléfono cuando se le indique.

5. Instale la aplicación para dispositivos móviles ESET Secure Authentication o una aplicación de autenticación de terceros en el teléfono móvil del usuario utilizando el vínculo del código QR o el SMS.

6. Una vez que instale la aplicación utilizando el token, su instancia de ESET PROTECT On-Prem se agrega a la aplicación.

7. Inicie sesión e introduzca la contraseña de un solo uso de la aplicación para dispositivo móviles en la Consola web cuando se le indique. Se genera una nueva contraseña de un solo uso cada 30 segundos.

8. También puede marcar la casilla **Recordar este dispositivo** si desea autorizar que su dispositivo no solicite autenticación de doble factor en cada inicio de sesión.

Puede olvidar los dispositivos recordados del usuario activo en la configuración del usuario.

9. Haga clic en **Enviar**.

Resolución de problemas

El usuario se bloqueará si escribe mal la contraseña de un solo uso diez veces. El administrador puede desbloquear el usuario en **Más** > **Usuarios** > haciendo clic en el usuario y seleccionando **Desbloquear**.

Si un usuario de Web Console no puede iniciar sesión en Web Console con autenticación de doble factor, siga estos pasos:

1. Haga una copia de seguridad de la ESET PROTECT base de datos.

2. Seleccione la opción correspondiente:

   • Puede acceder al número de teléfono configurado para autenticación de doble factor:

   a)Durante el inicio de sesión en Web Console, haga clic en **Restablecer token** en la ventana de autenticación de doble factor.

b)Se envía un SMS de verificación al número de teléfono configurado para autenticación de doble factor.

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 que se indican a continuación.

• No se puede acceder al número de teléfono configurado para autenticación de doble factor (el teléfono se ha perdido, está dañado, etc.).

a)Restablezca la contraseña de Web Console para desactivar la utenticación de doble factor en la cuenta de Administrador.

El estado de la utenticación de doble factor de otras cuentas de usuario de ESET PROTECT On-Prem no se verá afectado.

b)El usuario puede iniciar sesión en Web Console sin la utenticación de doble factor y, a continuación, volver a activarla tras iniciar sesión.

Conjuntos de permisos

Un conjunto de permisos representa los permisos de los usuarios que acceden a ESET PROTECT Web Console. Estos permisos definen lo que pueden hacer o ver los usuarios en Web Console. Los usuarios nativos tienen sus propios permisos, mientras que los usuarios de dominio tienen los permisos de su grupo de seguridad asignado. Cada conjunto de permisos tiene su dominio de aplicación (grupos estáticos). Los permisos seleccionados en la sección **Funcionalidad** se aplicarán a los objetos de los grupos configurados en la sección **Grupos estáticos** para cada usuario que tenga asignado dicho conjunto de permisos. Tener acceso a un grupo estático determinado significa tener acceso a todos sus subgrupos. Configurando adecuadamente los grupos estáticos es posible crear sucursales independientes para los administradores locales (ver el ejemplo).

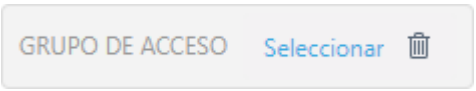
Un usuario puede tener un conjunto de permisos asignado aunque no pueda verlo. Un conjunto de permisos también es un objeto que se almacena automáticamente en el grupo principal del usuario que lo creó. Cuando se crea una cuenta de usuario, el usuario se almacena como objeto en el grupo principal del usuario que la creó. Normalmente es el administrador el que crea usuarios, por lo que se almacenan en el grupo *Todo*.

Los conjuntos de permisos se suman. Si asigna más conjuntos de permisos a un mismo usuario, el acceso resultante del usuario será la suma de todos los conjuntos de permisos.

Combinación de más conjuntos de permisos

El acceso definitivo que un usuario tiene para un objeto es el resultado de la combinación de todos los conjuntos de permisos que el usuario tiene asignados. Por ejemplo, un usuario cuenta con dos conjuntos de permisos: uno para el grupo doméstico con todos los permisos, y otro para un grupo con ordenadores solo con los permisos Lectura, Usar para ordenador y grupos. Este usuario puede ejecutar todas las tareas desde el grupo doméstico en ordenadores del otro grupo.

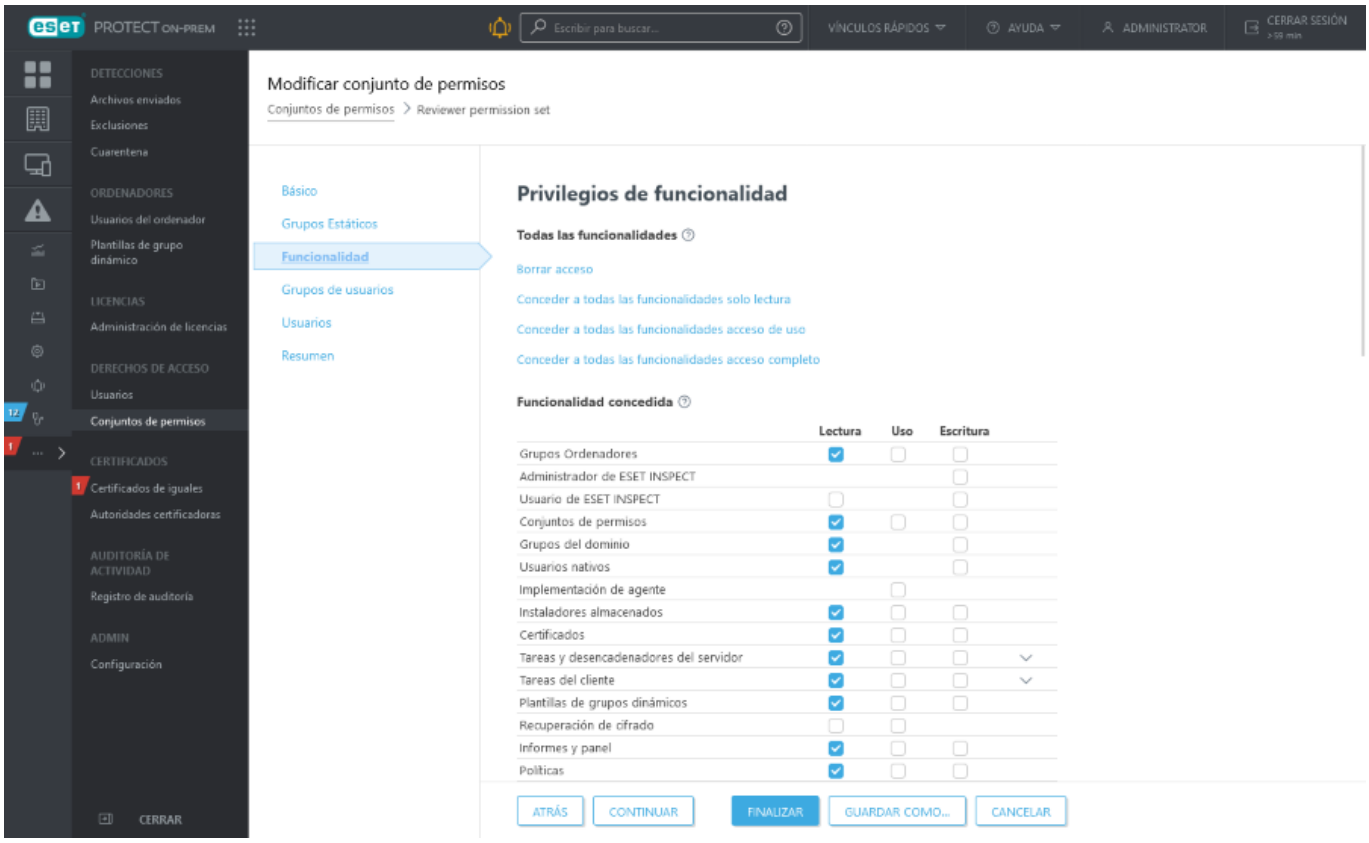
En términos generales, un usuario puede ejecutar objetos de un grupo estático sobre objetos de otro grupo estático, siempre que el usuario tenga permisos para un tipo de objeto determinado del grupo en cuestión.



El botón de filtrado de **Grupo de acceso** permite a los usuarios

seleccionar un grupo estático y filtrar los objetos vistos según el grupo en el que se encuentran.

Puede usar etiquetas para filtrar los elementos mostrados.



Práctica recomendada para trabajar con permisos:
• No otorgar acceso a la ESET PROTECT configuración del servidor a usuarios sin experiencia: solo el administrador debe tener este acceso.
• Debe estudiarse la restricción del acceso a **Tareas del cliente** > **Ejecutar comando**: es una tarea muy potente que puede utilizarse mal.
• Los usuarios que no sean administradores no deben tener permisos en **Conjuntos de permisos**, **Usuarios nativos** y **Configuración del servidor**.
• Si es necesario un modelo de permisos más complicado, no dude en crear más conjuntos de permisos y asignarlos como corresponda.

Con el permiso Registro de auditoría, el usuario puede ver las acciones registradas del resto de usuarios y dominios, incluso las relacionadas con los activos que el usuario no tiene permisos suficientes para ver.

Además de los permisos relativos a las funciones de ESET PROTECT On-Prem, también puede asignar acceso de **Lectura**, **Uso** y **Escritura** a Grupos de usuarios.

Duplicación

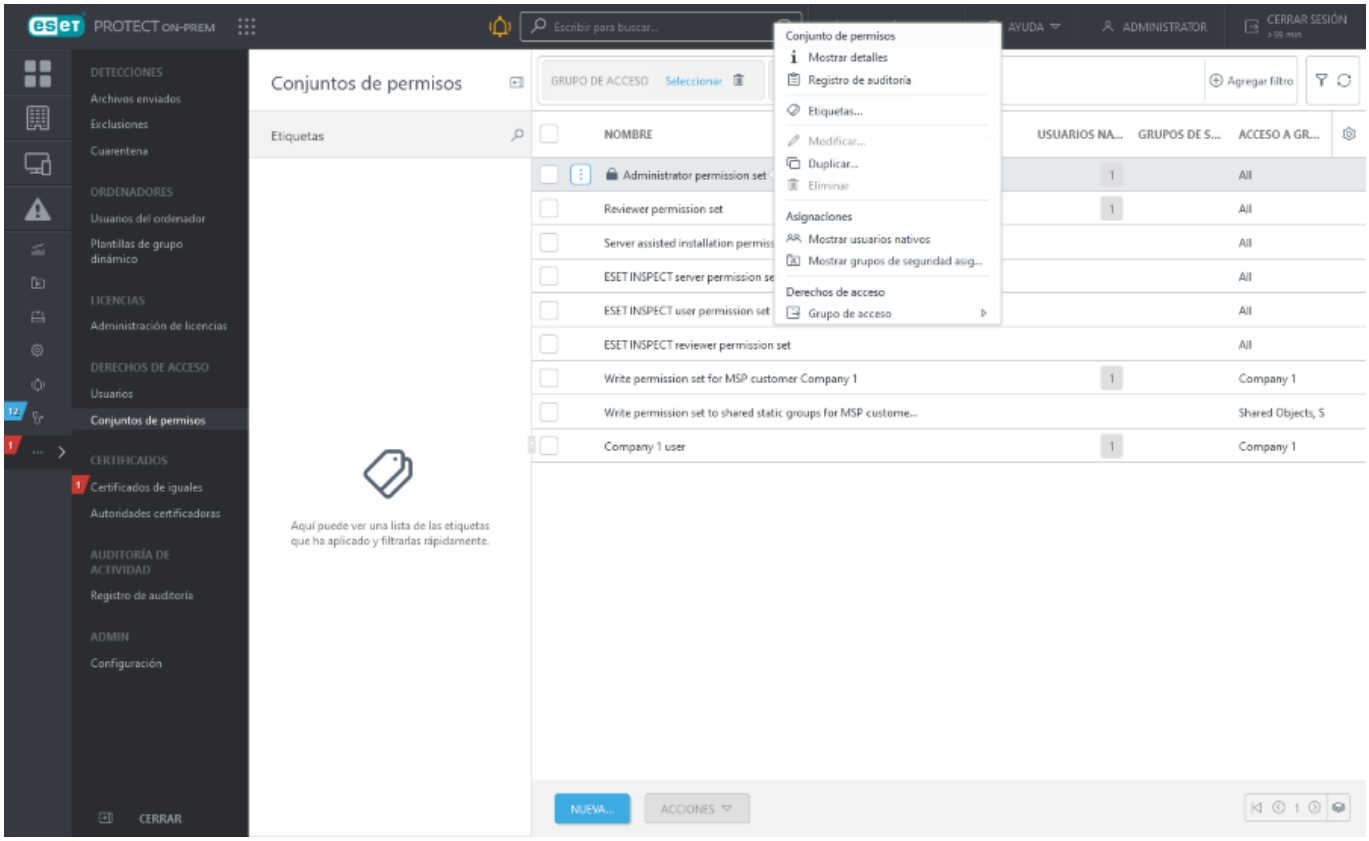
Para duplicar un objeto, el usuario debe tener permiso de **Lectura** del objeto original y permiso de **Escritura** en su **Grupo principal** para este tipo de acción.
John, cuyo grupo principal es *Grupo de John,* quiere duplicar *Política 1* creada por *Larry*; por lo tanto, la política está en el grupo principal de Larry, *Grupo de Larry*.
1.Cree un grupo estático nuevo. Llámelo, por ejemplo, *Políticas compartidas*.
2.Asigne a *John* y a *Larry* permisos de **Lectura** de las **Políticas** del grupo *Políticas compartidas*.
3.*Larry* mueve *Política 1* al grupo *Políticas compartidas*.
4.Asigne a *John* permisos de **Escritura** en **Políticas** en su grupo principal.
5.*John* ya puede **Duplicar** la *Política 1:* el duplicado aparecerá en su grupo principal.

Diferencia entre Uso y Escritura

Si el *administrador* no quiere permitir que el usuario *John* modifique políticas en el grupo *Políticas compartidas*, debe crear el siguiente conjunto de permisos:
- Funcionalidad **Políticas**: permisos de **Lectura** y **Uso** seleccionados
- **Grupos estáticos**: Políticas compartidas

Si se asignan estos permisos a *John*, *John* podrá ejecutar esas políticas, pero no podrá modificarlas o eliminarlas, ni crear nuevas políticas. Si un administrador añade el permiso de **Escritura**, John podrá crear nuevas políticas, modificarlas y eliminarlas 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 los detalles del conjunto de permisos.

- **Registro de auditoría** - Permite ver el Registro de auditoría del elemento seleccionado.
- **Etiquetas** - Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
- **Editar**: permite editar el conjunto de permisos.
- **Duplicar**: permite crear un conjunto de permisos duplicado que puede modificar y asignar a un usuario específico. El duplicado se almacenará en el grupo principal del usuario que lo duplicó.
- **Eliminar**: elimina el conjunto de permisos.

Asignaciones

- **Mostrar usuarios nativos**: muestra la lista de usuarios nativos asignados.
- **Mostrar grupos de seguridad asignados**: muestra la lista de grupos de seguridad del dominio asignados.

Derechos de acceso

- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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 conjuntos de permisos predefinidos tienen el grupo **Todo** en la sección **Grupos estáticos**. Tenga esto en cuenta al asignárselos a un usuario. Los usuarios tendrán estos permisos en todos los objetos de 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**.

Básico

Escriba el **Nombre** del conjunto (ajuste obligatorio). También puede especificar una **Descripción** y **Etiquetas**.

Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

Grupos estáticos

Puede **Seleccionar** un grupo estático (o varios grupos estáticos) o **Crear nuevo grupo** para que asuma esta competencia. Los permisos marcados en la sección **Funcionalidad** se aplicarán a los objetos contenidos en los grupos seleccionados en esta sección.

Funcionalidad

Seleccione los módulos individuales a los que desea conceder acceso. El usuario con esta competencia tendrá acceso a estas tareas específicas. También es posible configurar diferentes permisos para cada tipo de tarea del servidor y tarea del cliente. Hay cuatro conjuntos de funcionalidad predeterminados. Seleccione uno de estos cuatro o elija las casillas de verificación de la funcionalidad manualmente.

Al otorgar permiso de **Escritura** se otorgan automáticamente derechos de **Uso** y **Lectura**; al otorgar derechos de **Uso** se otorgan automáticamente derechos de **Lectura**.

Grupos de usuarios

Puede agregar un Grupo de usuarios (o varios grupos de usuarios) cuyos parámetros de usuarios se puedan utilizar en una política (por ejemplo, Administración de dispositivos móviles de ESET para iOS o Modo de anulación).

Usuarios

Elija un usuario para asignarle este conjunto de permisos. Todos los usuarios disponibles se muestran a la izquierda. Seleccione usuarios específicos o todos los usuarios con el botón **Agregar todo**. Los usuarios asignados se muestran a la derecha. No es obligatorio asignar permisos a un usuario, puede hacerlo más tarde.

Resumen

Revise las opciones configuradas para esta competencia y haga clic en **Finalizar**. El conjunto de permisos se almacena en el grupo principal del usuario que lo creó.

Haga clic en **Guardar como** para crear un nuevo conjunto de permisos basado en el conjunto de permisos que está editando. Se solicitará introducir un nombre para el nuevo conjunto de permisos.

Lista de permisos

Tipos de permisos

Cuando cree o modifique un conjunto de permisos, en **Más** > **Conjuntos de permisos** > **Nuevo/Modificar** > **Funcionalidad** encontrará una lista de todos los permisos disponibles. Los permisos de ESET PROTECT Web Console están divididos en categorías; por ejemplo, **Grupos y ordenadores**, **Políticas**, **Tareas del cliente**, **Informes**, **Notificaciones**, etc. Un conjunto de permisos determinado puede otorgar acceso de **Lectura**, **Uso** o **Escritura**. En general:

- Los permisos de **Lectura** son adecuados para los usuarios que realizan auditorías. Pueden ver datos, pero no efectuar cambios.
- Los permisos de **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 o duplicarlos.

Algunos tipos de permisos (indicados a continuación) controlan un proceso, no un objeto. El motivo es que actúan

a nivel global, por lo que no importa a qué grupo estático está aplicado el permiso, ya que funcionará de todas formas. Si un usuario tiene el proceso autorizado, solo podrá utilizarlo con objetos para los que tenga permisos suficientes. El permiso **Exportar informe a un archivo**, por ejemplo, permite la funcionalidad de exportación, pero los datos que contiene el informe los determina otro permiso.

Lea el artículo de la base de conocimiento con conjuntos de permisos y tareas de ejemplo que necesita el usuario para realizar las tareas correctamente.

Las funcionalidades a las que el usuario actual no tiene derechos de acceso no están disponibles (atenuadas).

Se pueden asignar permisos a los usuarios para los siguientes procesos:

- **Implementación de agente**
- **Informes y consola** (solo estará disponible la funcionalidad de la consola, pero las plantillas de informe utilizables dependen de los grupos estáticos accesibles)
- **Enviar correo electrónico**
- **Exportar informe a un archivo**
- **Enviar captura de SNMP**
- **Configuración del servidor**
- **ESET Inspect Administrador**
- **ESET Inspect Usuario**
- **Informes completos**

Tipos de funcionalidades:

Grupos y ordenadores

Lectura: ver listas de los ordenadores, los grupos y los ordenadores de un grupo.

Uso: utilizar un ordenador o grupo como destino de una política o tarea.

Escritura: crear, modificar y quitar ordenadores. Esto también incluye cambiar el nombre de un ordenador o grupo.

ESET Inspect Administrador

Escritura: desempeñar funciones administrativas en ESET Inspect On-Prem.

ESET Inspect Usuario

Lectura: acceso de solo lectura a ESET Inspect On-Prem. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de 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 las correspondientes listas de derechos de acceso.

Uso: asignar conjuntos de permisos existentes a los usuarios y quitárselos.

Escritura: crear, modificar y quitar conjuntos de permisos.

Al asignar (o desasignar) un conjunto de permisos a un usuario, se requiere permiso de **Escritura** para los **Grupos del dominio** y los **Usuarios nativos**.

Grupos de dominio

Lectura: ver grupos de dominio.

Escritura: permite otorgar y revocar conjuntos de permisos. Crear, modificar y quitar grupos de dominio.

Usuarios nativos

Lectura: ver los usuarios nativos.

Escritura: permite otorgar y revocar conjuntos de permisos. Crear, modificar y quitar usuarios nativos.

Implementación de agente

Uso: permitir acceso para la implementación del agente mediante **vínculos rápidos** o la adición manual de ordenadores cliente desde ESET PROTECT Web Console.

Instaladores almacenados

Lectura: ver los instaladores almacenados.

Uso: exportar los instaladores almacenados.

Escritura: crear, modificar y quitar los instaladores almacenados.

Certificados

Lectura: leer la lista de certificados de igual y autoridades certificadoras.

Uso: exportar certificados de igual y autoridades certificadoras, y utilizarlos en instaladores o tareas.

Escritura: crear nuevos certificados de igual o autoridades certificadoras, y revocarlos.

Tareas y desencadenadores de servidor

Lectura: leer la lista de tareas y su configuración (excepto campos confidenciales como las contraseñas).

Uso: ejecutar una tarea existente con Ejecutar ahora (como usuario que ha iniciado sesión en Web Console).

Escritura: crear, modificar y quitar tareas del servidor.

Para expandir las categorías, se puede hacer clic en el signo y se pueden seleccionar tareas únicas o múltiples del servidor.

Tareas del cliente

Lectura: leer la lista de tareas y su configuración (excepto campos confidenciales como las contraseñas).

Uso: planificar la ejecución de tareas del cliente existentes o cancelar su ejecución. Tenga en cuenta que para asignar tareas (o cancelar la asignación) a destinos (ordenadores o grupos), se requiere también el acceso de Uso a dichos destinos.

Escritura: crear, modificar y quitar tareas del cliente existentes. Tenga en cuenta que para asignar tareas (o cancelar la asignación) a destinos (ordenadores o grupos), se requiere también el acceso de **Uso** a dichos objetos de destino.

Las categorías pueden desplegarse haciendo clic en el signo , y pueden seleccionarse uno o más tipos de tareas del cliente.

Plantillas de grupos dinámicos

Lectura: leer la lista de plantillas de grupos dinámicos.

Uso: utilizar las plantillas existentes con grupos dinámicos.

Escritura: crear, modificar y quitar plantillas de grupos dinámicos.

Recuperación de cifrado

Lectura

Uso: gestionar el proceso de Recuperación de cifrado.

Informes y consola

Lectura: ver plantillas de informes y sus categorías. Generar informes basados en plantillas de informes. Leer paneles propios basados en paneles predeterminados.

Uso: modificar paneles propios con las plantillas de informes disponibles.

Escritura: crear, modificar y quitar las plantillas de informes existentes y sus categorías. Modificar los paneles predeterminados.

Políticas

Lectura: leer la lista de políticas y su configuración.

Uso: asignar las políticas existentes a destinos (o cancelar su asignación). Tenga en cuenta que también es necesario el acceso de **Uso** a los destinos.

Escritura: crear, modificar y quitar políticas.

Enviar correo electrónico

Uso: enviar mensajes de correo electrónico. (Útil para las tareas del servidor Notificaciones y Generar informe).

Enviar captura de SNMP

Uso: permite enviar una captura de SNMP (útil para Notificaciones).

Exportar informe a un archivo

Uso: le permite almacenar informes en el sistema de archivos del ordenador ESET PROTECT Server. Útil con la tarea del servidor Generar informe.

Licencias

Lectura: leer la lista de licencias y sus estadísticas de uso.

Uso: utilizar la licencia para activarla.

Escritura: agregar y quitar licencias. (El grupo principal del usuario debe ser Todo. De manera predeterminada, solo puede hacerlo el administrador).

Notificaciones

Lectura: leer la lista de notificaciones y su configuración.

Uso: asignar etiquetas.

Escritura: crear, modificar y quitar notificaciones. Para una buena gestión de las notificaciones, pueden ser necesarios también derechos de acceso de **Uso** en **Enviar captura de SNMP** o **Enviar correo electrónico**, dependiendo de la configuración de las notificaciones.

Configuración del servidor

Lectura: leer la ESET PROTECT configuración del servidor.

Escritura: modificar la ESET PROTECT configuración del servidor.

Registro de auditoría

Lectura: ver el Registro de auditoría y leer el informe del Registro de auditoría.

Informes completos

Usar: genere la plantilla de informe de MDR.

Funcionalidad de ESET Inspect concedida

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 Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para **Usuario de ESET Inspect**.

Certificados

Los certificados son una parte importante de ESET PROTECT On-Prem: 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 ESET PROTECT Web Console.

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 en ESET PROTECT On-Prem en nuestro artículo de la base de conocimiento.

En lo referente a certificados, tiene varias opciones:

- Puede utilizar certificados creados automáticamente durante la instalación de ESET PROTECT On-Prem.
- Puede crear una nueva autoridad certificadora (CA) o importar la clave pública que utilizará para firmar el certificado de igual para cada uno de los componentes (ESET Management Agent, ESET PROTECT Server, ERA ESET PROTECT MDM).
- Puede utilizar su propia autoridad certificadora y certificados personalizados.

> Si tiene previsto migrar de un ESET PROTECT Server a un nuevo equipo servidor, debe exportar/realizar una copia de seguridad de todas las autoridades certificadoras que utilice, así como del certificado de ESET PROTECT Server. De lo contrario, ningún componente de ESET PROTECT podrá comunicarse con su nuevo ESET PROTECT Server.

Puede crear una nueva **autoridad certificadora** y **certificados de iguales** en ESET PROTECT Web Console; siga las instrucciones de esta guía para:

- Crear una nueva autoridad certificadora
  - Importar una clave pública
  - Exportar una clave pública
  - Exportar una clave pública en formato BASE64
- Crear un nuevo certificado de igual
  - Crear un certificado
  - Exportar un certificado
  - Crear un certificado de APN/ABM
  - Revocar un certificado
  - Uso de certificado
  - Configurar un nuevo certificado de ESET PROTECT Server
  - Certificados personalizados con ESET PROTECT On-Prem
  - Certificado con caducidad próxima: informe y sustitución

> 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.

El valor Válido desde de todos los certificados y las autoridades certificadoras creadas durante la instalación de los componentes de ESET PROTECT se establece en 2 días antes de la creación del certificado.
El valor Válido desde de todos los certificados y las autoridades de certificación creados en ESET PROTECT Web Console se establece en 1 día antes de la creación del certificado. La finalidad de esta medida es cubrir todas las discrepancias de tiempo posibles entre los sistemas afectados.
Por ejemplo, una autoridad certificadora y un certificado creados el 12 de enero de 2017 durante la instalación, tendrán un valor Válido desde predefinido del 10 de enero de 2017 a las 10 00:00:00, mientras que una autoridad certificadora y un certificado creados el 12 de enero de 2017 en ESET PROTECT Web Console tendrán un valor Válido desde predefinido del 11 de enero de 2017 a las 00:00:00.

Certificados de iguales

Si en el sistema hay presente una autoridad certificadora debe crear un certificado de iguales para cada uno de los componentes de ESET PROTECT. Cada componente (ESET Management Agent y ESET PROTECT Server) requiere un certificado concreto.

Nuevo

Esta opción se utiliza para crear un nuevo certificado. Estos certificados son utilizados por ESET Management Agent y ESET PROTECT Server.

Certificado de APN/ABM

Esta opción se utiliza para crear un nuevo certificado de APN/ABM. MDM utiliza este certificado. Esta acción requiere una licencia válida.

Uso de certificado

También puede consultar qué clientes están usando este certificado de ESET PROTECT.

Etiquetas

Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).

Modificar...

Seleccione esta opción para editar la **descripción** de un certificado existente en la lista.

Registro de auditoría

Permite ver el Registro de auditoría del elemento seleccionado.

Exportar o **Exportar Base64...**

Exporte un certificado como archivo *.pfx* o archivo *.txt* (Base64). Este archivo es necesario si instala ESET Management Agent localmente en un ordenador o al instalar MDM.

Revocar

Si ya no desea utilizar el certificado, seleccione **Revocar**. Esta opción anula el certificado permanentemente y lo añade de forma efectiva a la lista negra. Esta información se envía a las instancias de ESET Management Agent durante la próxima conexión. ESET PROTECT On-Prem No aceptará certificados revocados.

Asegúrese de que no haya agentes ESET Management (u otros componentes) que usen este certificado antes de revocarlo. Una vez revocado el certificado, los componentes no podrán conectarse a ESET PROTECT Server. Reinstale los componentes con un certificado válido para restaurar la funcionalidad.

Grupo de acceso

Un certificado o autoridad certificado pueden moverse a otro grupo. Así quedarán a disposición de los usuarios que tengan suficientes derechos para dicho grupo. Para encontrar fácilmente el grupo principal de un certificado, seleccione el certificado y haga clic en **Grupo de acceso** en el menú desplegable. El grupo principal del certificado aparecerá en la primera línea del menú desplegable (por ejemplo, /Todo/San Diego. Consulte nuestro caso de ejemplo para obtener más información sobre el uso compartido de certificados).

Solo verá los certificados que se encuentren en su grupo de inicio (siempre que tenga permiso de **lectura** sobre los certificados). Los certificados creados durante la instalación de ESET PROTECT On-Prem se encuentran en el grupo **Todo**, y solo los administradores tienen acceso a ellos.

Haga clic en el botón **Mostrar elementos revocados** para ver todos los certificados revocados.

Certificado de agente para instalación asistida por el servidor: este certificado se genera durante la instalación del servidor, siempre que seleccione la opción **Generar certificados**.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Crear un nuevo certificado

Como parte del proceso de instalación, ESET PROTECT On-Prem requiere que cree certificado de iguales para los agentes. Estos certificados se utilizan para autenticar la comunicación entre el agente del dispositivo cliente y ESET PROTECT Server.

solo hay una excepción, un **Certificado de agente para instalación asistida por el servidor** no se puede crear manualmente. Este certificado se genera durante la instalación del servidor, siempre que se haya seleccionado la opción **Generar certificados**.

Para crear un nuevo certificado en **ESET PROTECT Web Console**, diríjase a **Más** > **Certificados de iguales** y haga clic en **Acciones** > **Nuevo**.

Básico

Descripción: escriba la descripción del certificado.

Haga clic en **Seleccione las etiquetas** para asignar etiquetas.

Producto: seleccione el tipo de certificado que desee crear en el menú desplegable.

Host: deje el **valor predeterminado (un asterisco) en el campo Host** para permitir la distribución de este certificado sin asociación a un nombre DNS o dirección IP específicos.

Al crear el certificado de MDM, rellene la dirección IP o el nombre de host del dispositivo host de MDM. El valor predeterminado (un asterisco) no es válido para este tipo de certificado.

Frase de contraseña: le recomendamos que deje este campo en blanco, pero puede configurar una contraseña para el certificado que se requerirá cuando los clientes intenten realizar la activación.

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

Atributos (asunto)

Estos campos no son obligatorios, pero puede utilizarlos para incluir información más detallada sobre este certificado.

Nombre común: este valor debe contener la cadena "Agente", o "Servidor" de acuerdo con el **Producto** seleccionado. Si lo desea, puede introducir información descriptiva acerca del certificado. Introduzca los valores **Válido desde** y **Válida hasta** para asegurarse de que el certificado es válido.

El valor Válido desde de todos los certificados y las autoridades certificadoras creadas durante la instalación de los componentes de ESET PROTECT se establece en 2 días antes de la creación del certificado.
El valor Válido desde de todos los certificados y las autoridades de certificación creados en ESET PROTECT Web Console se establece en 1 día antes de la creación del certificado. La finalidad de esta medida es cubrir todas las discrepancias de tiempo posibles entre los sistemas afectados.
Por ejemplo, una autoridad certificadora y un certificado creados el 12 de enero de 2017 durante la instalación, tendrán un valor Válido desde predefinido del 10 de enero de 2017 a las 10 00:00:00, mientras que una autoridad certificadora y un certificado creados el 12 de enero de 2017 en ESET PROTECT Web Console tendrán un valor Válido desde predefinido del 11 de enero de 2017 a las 00:00:00.

Firmar

Seleccione uno de estos dos métodos de firma:

- **Autoridad certificadora**: si desea firmar utilizando la **Autoridad certificadora de ESET PROTECT** (autoridad certificadora creada automáticamente durante la instalación de ESET PROTECT On-Prem).
  - Seleccione la **Autoridad certificadora de ESET PROTECT** en la lista de autoridades certificadoras.
  - Crear una nueva autoridad certificadora
- **Archivo pfx personalizado**: para usar un archivo *.pfx* personalizado, haga clic en **Examinar**, navegue hasta el archivo *.pfx* personalizado y haga clic en **Aceptar**. Seleccione **Cargar** para cargar este certificado en el servidor. No puede utilizar el certificado personalizado.

Si quiere firmar un nuevo certificado con la autoridad certificadora de ESET PROTECT On-Prem (creada durante la instalación de ESET PROTECT On-Prem) en el dispositivo virtual de ESET PROTECT, es necesario cumplimentar el campo **Frase de contraseña de la autoridad certificadora. Esta es** la contraseña que especificó durante la configuración del dispositivo virtual de ESET PROTECT.

Resumen

Revise la información del certificado que ha introducido y haga clic en **Finalizar**. El certificado ahora se habrá creado correctamente y estará disponible en la lista **Certificados** para usar cuando se instale el agente. El certificado se creará en su grupo principal.

Estas son las alternativas que tiene a la creación de un nuevo certificado:Importar una clave pública, Exportar una clave pública o Exportar un certificado de igual.

Exportar certificado de igual

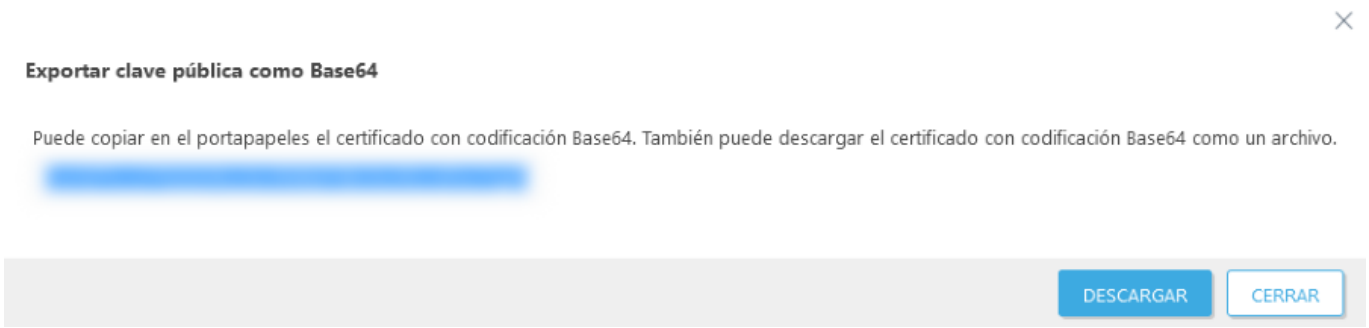
Exportar certificados de igual

1.Seleccione en la lista los **certificados de igual** que desee usar, y active la casilla de verificación situada junto a ellos.

2.Seleccione **Exportar** en el menú contextual. El certificado se exportará (incluida la clave privada) como archivo *.pfx*. Escriba el nombre del certificado y haga clic en **Guardar**.

Exportar como Base64 desde certificados de igual

Los certificados de los componentes de ESET PROTECT están disponibles en Web Console. Para copiar los contenidos en un certificado con formato Base64, haga clic en **Más** > **Certificados de iguales**, seleccione un certificado y, a continuación, seleccione **Exportar como Base64**. Puede descargar también el certificado con codificación Base64 como un archivo. Repita este paso con los certificados de otros componentes, y con su autoridad certificadora.



Para exportar un certificado, un usuario debe tener derechos de **Uso** de **Certificados**. Consulte la lista completa de derechos de acceso para obtener más información.

Certificado de APN/ABM

ESET PROTECT MDM utiliza un certificado de APN (Notificación push de Apple)/ABM (Apple Business Manager) para la inscripción de dispositivos iOS. Tendrá que crear un **Certificado push proporcionado por Apple** y conseguir que Apple lo firme para poder inscribir dispositivos iOS en ESET PROTECT On-Prem. Asegúrese también de tener una licencia válida para ESET PROTECT On-Prem.

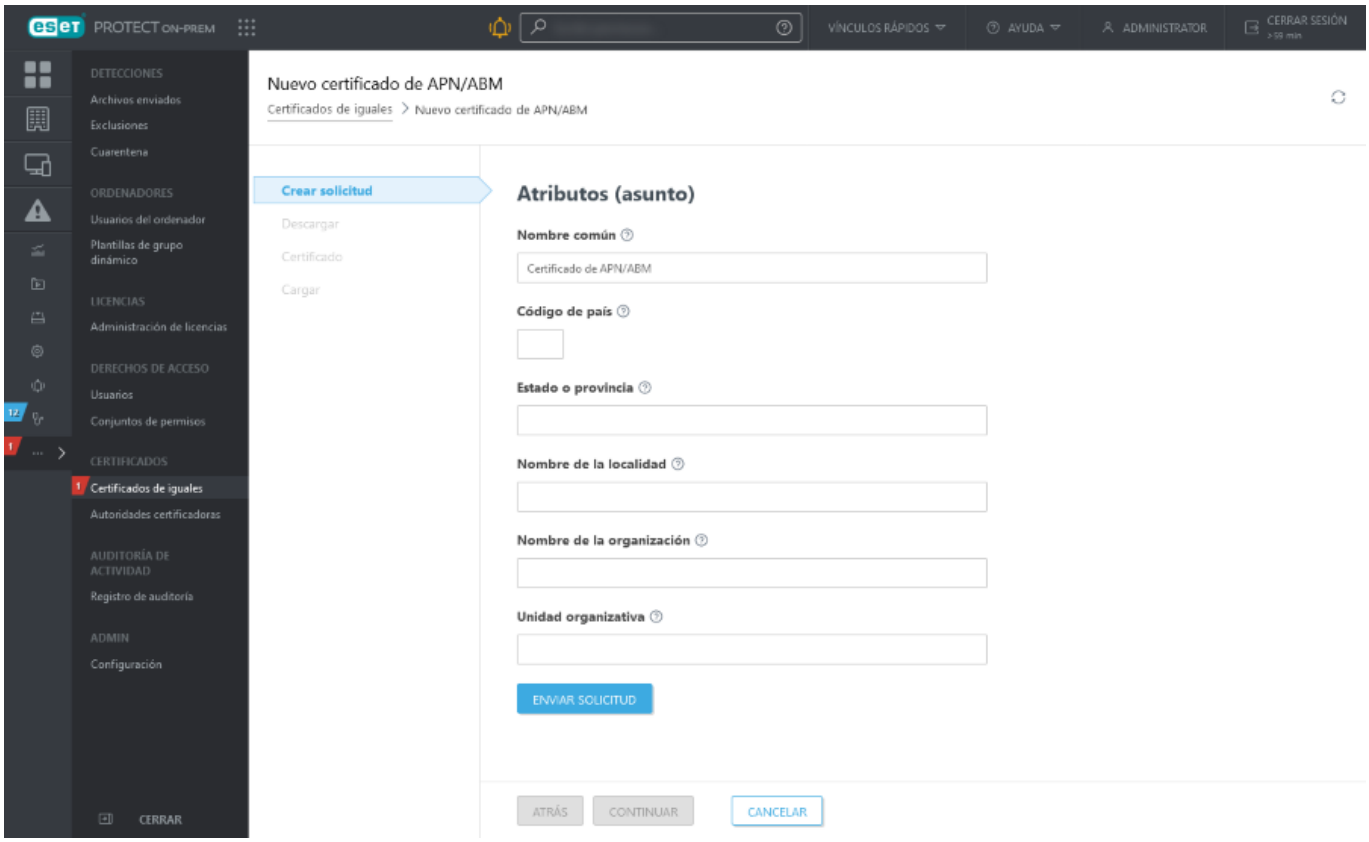
Haga clic en la pestaña **Más** > **Certificados de iguales**, haga clic en **Nuevo y, a continuación,** seleccione

Certificado de APN/ABM.

> Para adquirir un certificado de APN necesitará un Apple ID. Apple requiere este ID para firmar el certificado.
> El certificado de APN tiene una validez de un año. Si su certificado está cerca de caducar, siga los pasos indicados a continuación y, en el paso 2 de la parte del certificado, seleccione **Renovar**.
> Para adquirir un token de inscripción de ABM, necesitará una Cuenta de Apple ABM.

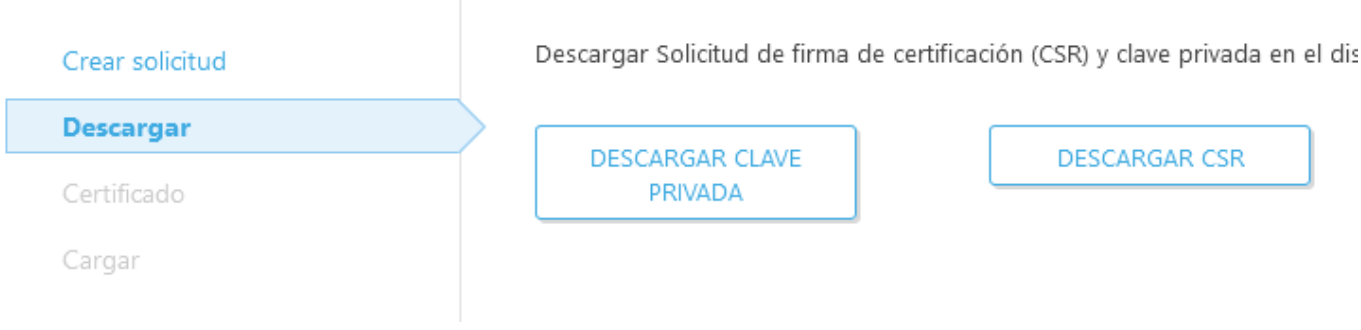
Crear solicitud

Especifique los atributos del certificado (Código del país, Nombre de la organización, etc.) y haga clic en **Enviar solicitud**.



Descargar

Descargue su **CSR** (Solicitud de firma de certificación) y una **Clave privada**.



Certificado

1.Abra el Portal de certificados push de Apple e inicie sesión con su Apple ID.

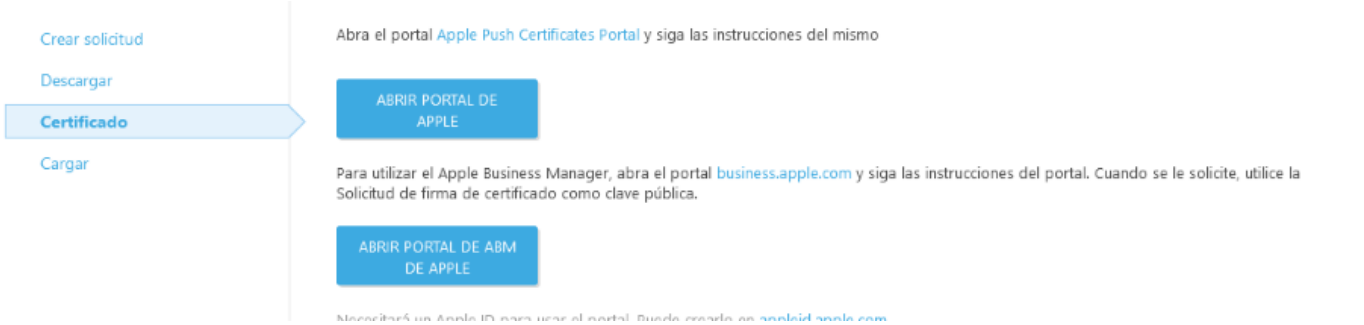
2.Haga clic en **Crear un certificado**.

3.Rellene la nota (opcional). Haga clic en **Elegir archivo**, cargue el archivo CSR que descargó en el paso anterior y haga clic en **Cargar**.

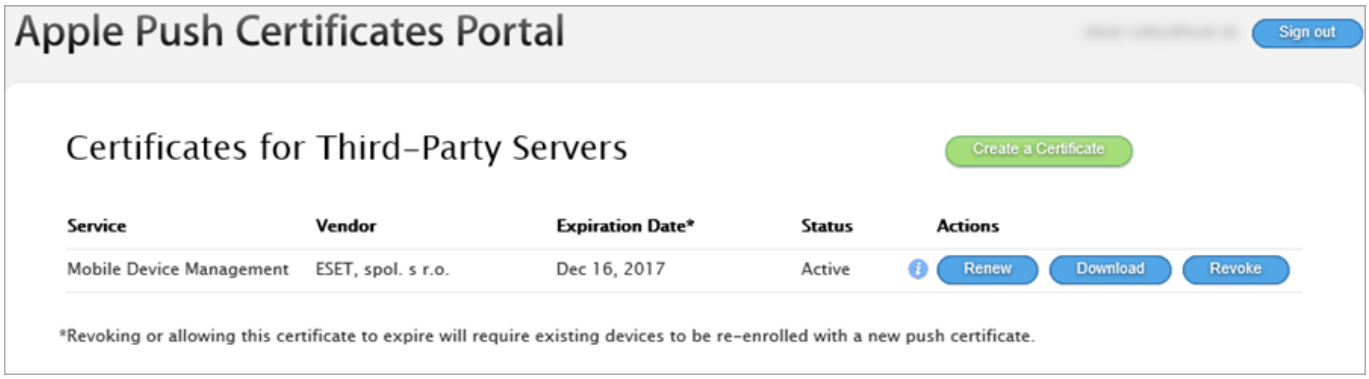
4.Después de algún tiempo verá una nueva pantalla de confirmación con la notificación de que su certificado APNS para el servidor de administración de dispositivos móviles de ESET se creó correctamente.

5.Haga clic en **Descargar** y guarde el archivo *.pem* en su ordenador.

6.Cierre el Portal de certificados push de Apple y vaya a la sección Cargar que aparece a continuación.



El certificado de APNS es necesario para las políticas de MDC ABM y no ABM. Siga estas instrucciones para crear un certificado de inscripción de ABM.



Cargar

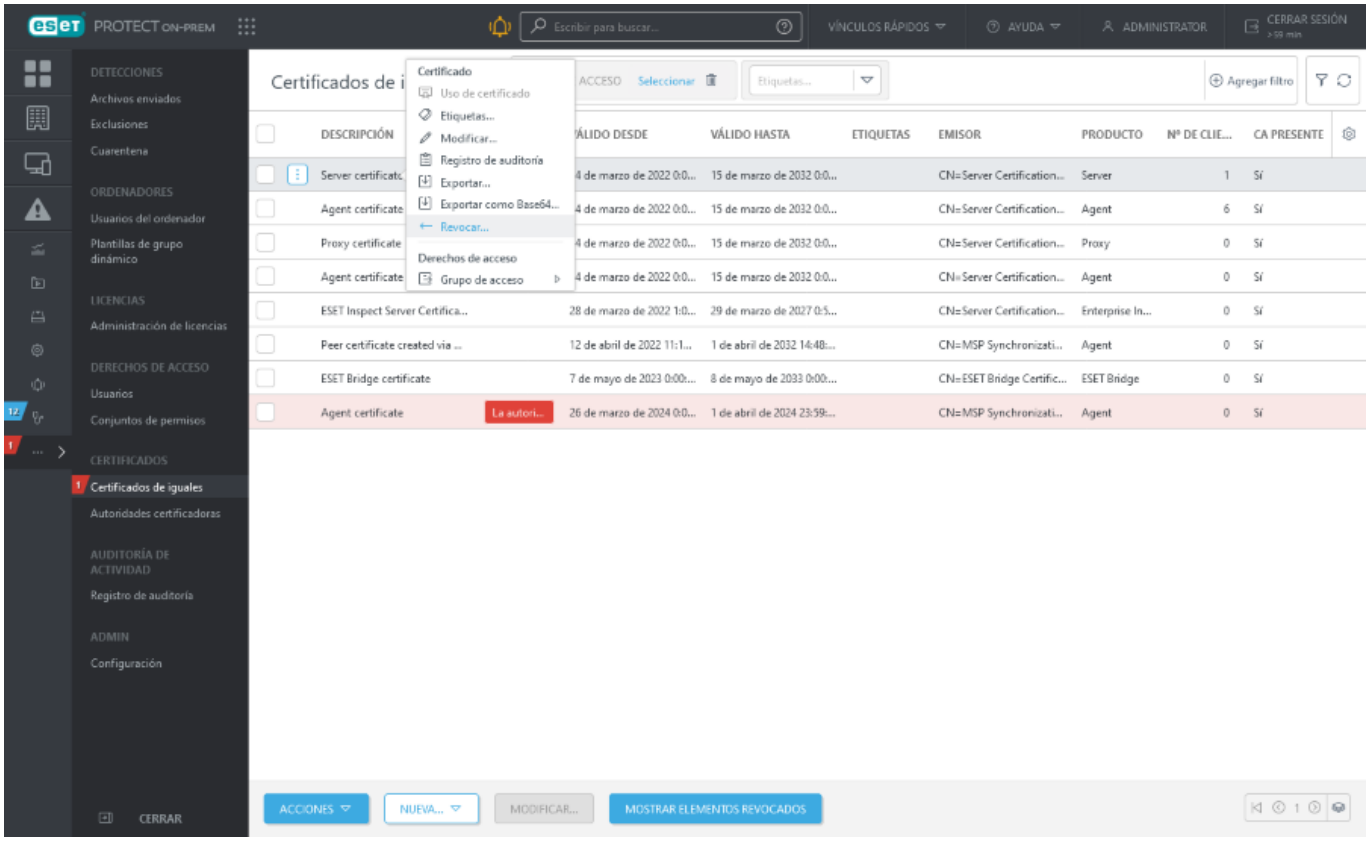
Una vez haya completado los pasos anteriormente indicados, puede crear una Política para que MDC active APNS para la inscripción de iOS. A continuación puede Inscribir cualquier dispositivo iOS; para ello visite *https://<mdmcore>:<enrollmentport>/unique_enrollment_token* desde el navegador del dispositivo.

Mostrar elementos revocados

En esta lista se muestran todos los certificados que se han creado y se han anulado a través de ESET PROTECT Server. Los certificados revocados se eliminarán automáticamente de la pantalla **Certificado de igual** principal. Haga clic en **Mostrar elementos revocados** para ver los certificados que se han revocado desde la ventana principal.

Para revocar un certificado, siga los pasos indicados a continuación:

1. Diríjase a **Más** > **Certificados de iguales** > seleccione un certificado y haga clic en **Revocar**.



2. Especifique el **Motivo** de la revocación y haga clic en **Revocar**.

3. Haga clic en **Aceptar**. El certificado desaparecerá de la lista de Certificados de iguales. Para ver los certificados anteriormente revocados, haga clic en el botón **Mostrar elementos revocados**.

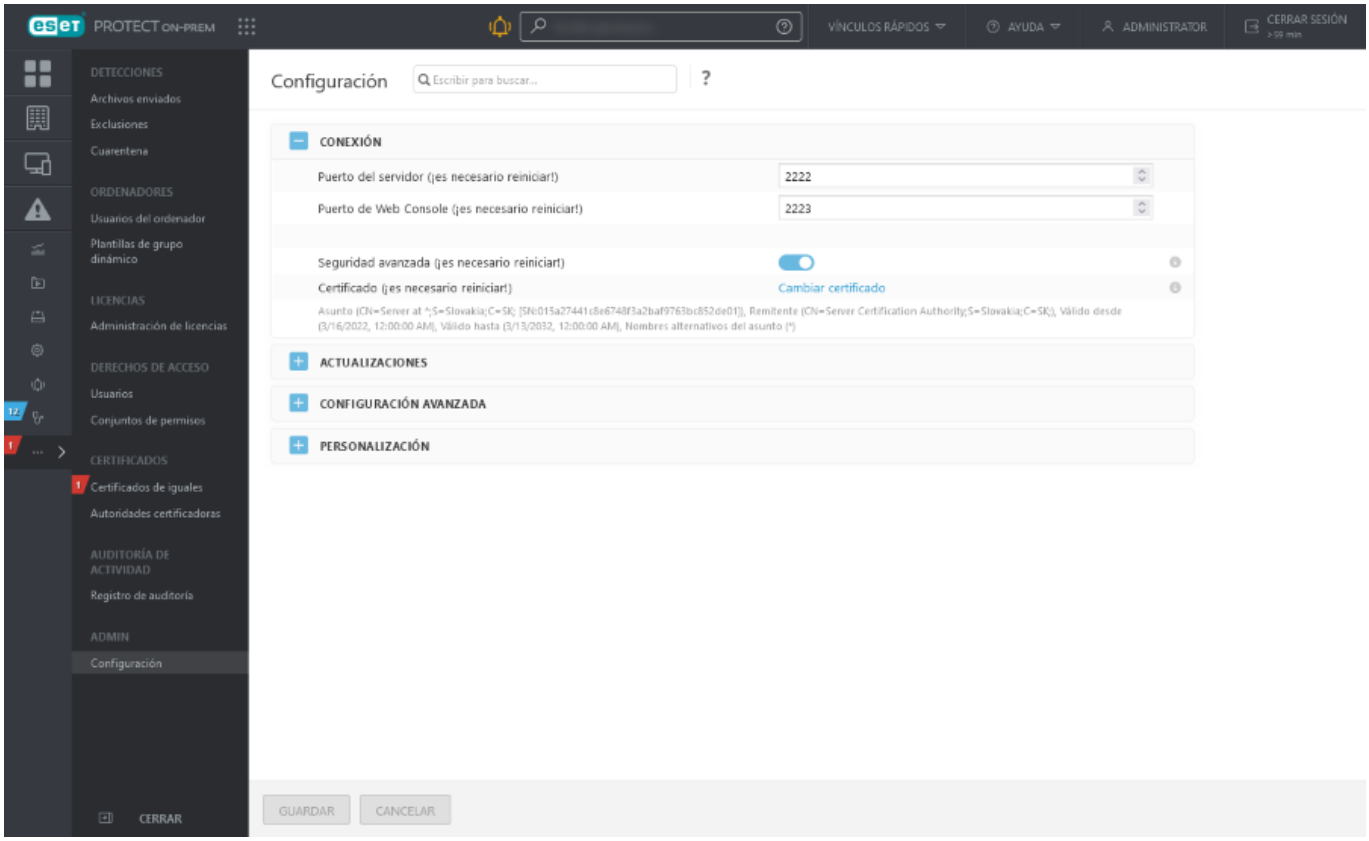
Configurar un nuevo certificado de ESET PROTECT Server

El certificado del ESET PROTECT Server se crea durante la instalación, y se distribuye a los ESET Management Agent y a otros componentes para permitir la comunicación con el ESET PROTECT Server.

- En caso de ser necesario, puede configurar ESET PROTECT Server para que use un certificado de igual distinto. Puede usar el certificado de ESET PROTECT Server (generado automáticamente durante la instalación) o un **Certificado personalizado**.

• El certificado de ESET PROTECT Server es necesario para una conexión y autenticación TLS seguras. 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.

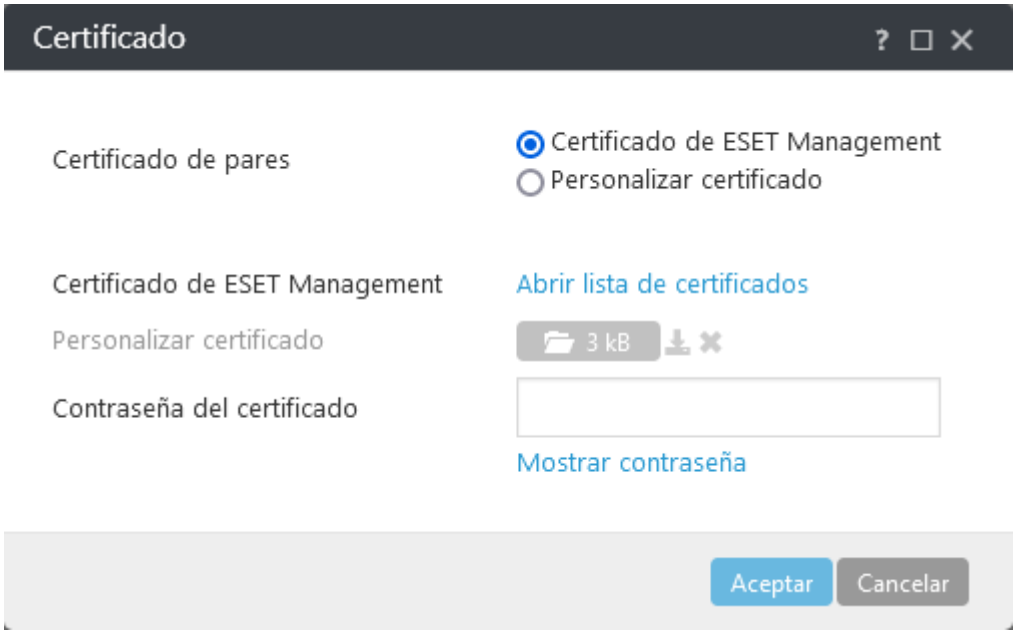
1. Haga clic en **Más** > **Configuración** > despliegue la sección **Conexión**, seleccione **Cambiar certificado**.



2. Elija entre los dos tipos de certificado de igual:

• **Certificado de ESET Management**: haga clic en **Abrir lista de certificados** y seleccione el certificado que desea utilizar.

• **Certificado personalizado**: desplácese hasta su certificado personalizado y, a continuación, haga clic en **Aceptar** y **Guardar**. Si está realizando una migración, seleccione el archivo *.pfx* del certificado de ESET PROTECT Server que exportó de su antiguo ESET PROTECT Server.



3. Utilice la opción **Reiniciar** en ESET PROTECT Server, consulte nuestro artículo de la Base de conocimiento.

Certificados personalizados con ESET PROTECT On-Prem

Si tiene su propia PKI (infraestructura de clave pública) y desea que ESET PROTECT On-Prem utilice sus certificados personalizados para establecer comunicación entre sus componentes, vea el siguiente ejemplo. Este ejemplo se realiza en Windows Server 2012 R2. Las capturas de pantalla pueden ser distintas de otras versiones de Windows, pero el procedimiento general no varía.

- No utilice certificados con una validez breve (por ejemplo, Let's Encrypt con una validez de 90 días) para evitar el complejo procedimiento de sustituirlos con frecuencia.
- Si administra dispositivos móviles, no se recomienda el uso de certificados autofirmados (incluidos los certificados firmados por la autoridad certificadora de 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 externa.

Puede utilizar OpenSSL para crear nuevos certificados autofirmados. Para obtener más información, lea el artículo de nuestra Base de conocimiento.

Funciones de servidor necesarias:

- Servicios de dominio de Active Directory.
- Servicios de certificados de Active Directory con la autoridad certificadora raíz independiente instalada.

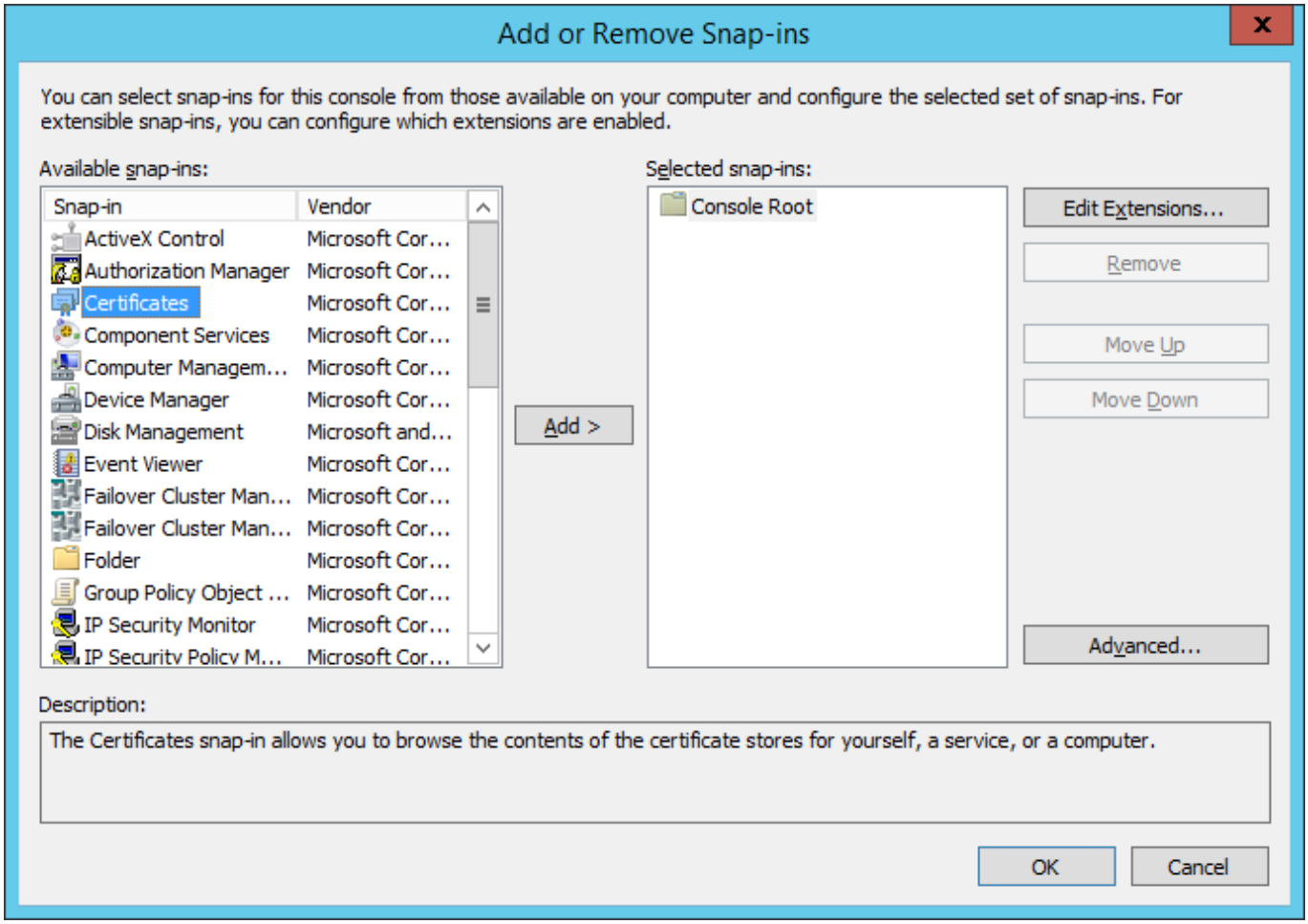
1. Abra **Consola de administración** y añada complementos de **Certificados**:

   a)Inicie sesión en el servidor como miembro del grupo de administradores 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 de equipo** y haga clic en **Siguiente**.

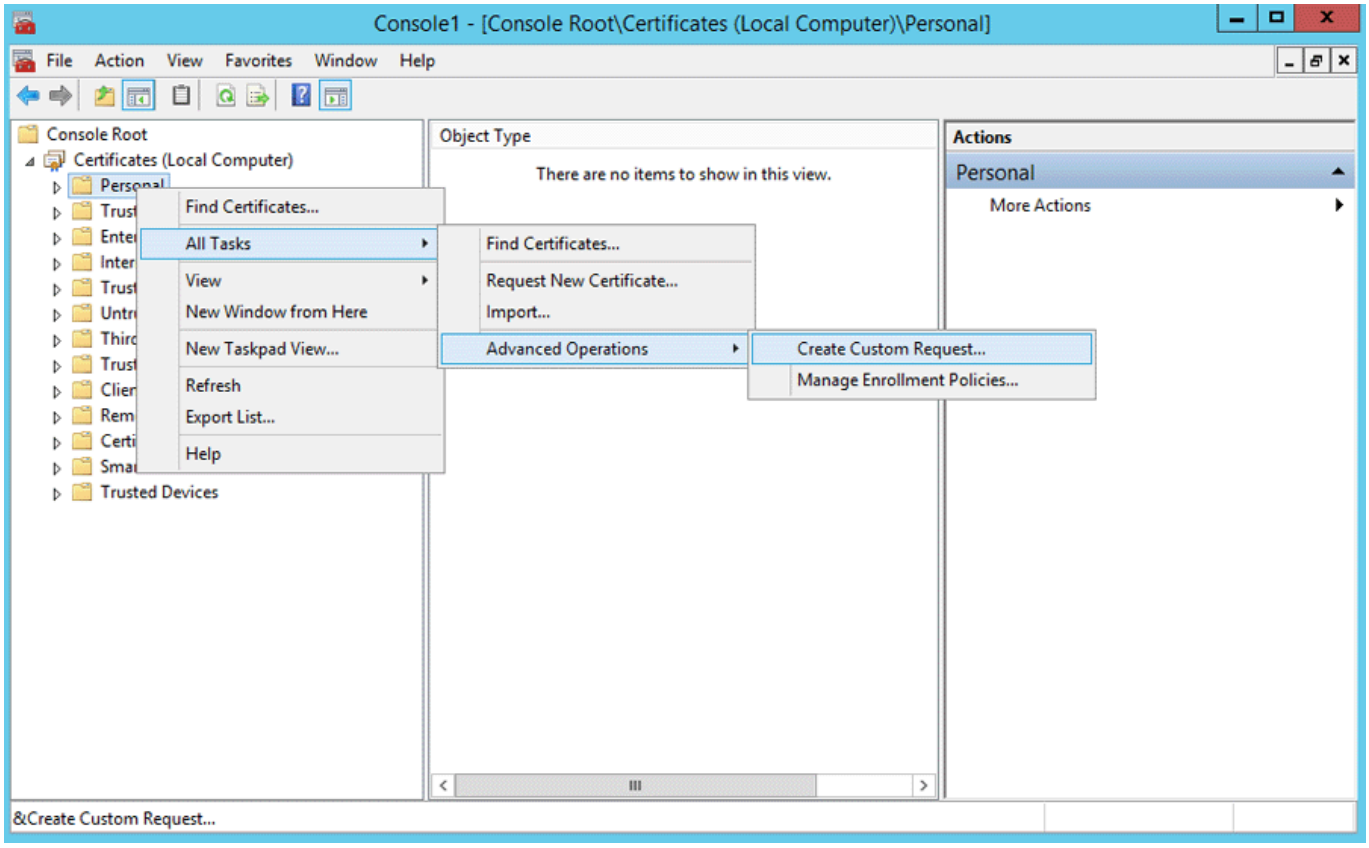
f)Asegúrese de seleccionar **Equipo local** (predeterminado) y haga clic en **Finalizar**.

g)Haga clic en **Aceptar**.

2. Cree una **Solicitud de certificado personalizado**:

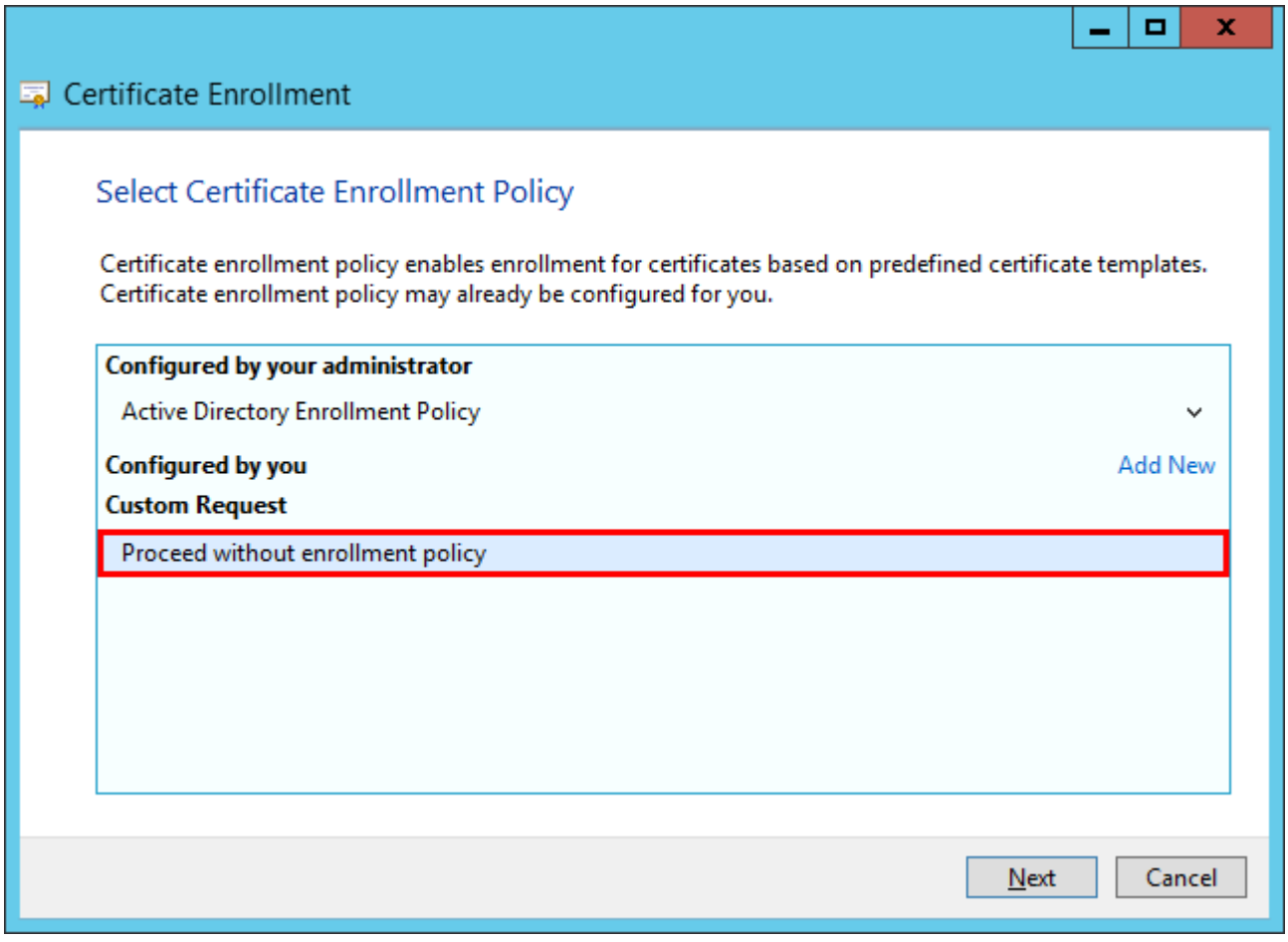
a)Haga doble clic en **Certificados (equipo local)** para desplegar esta opción.

b)Haga doble clic en Personal para desplegar esta opción. Haga clic con el botón derecho del ratón en Certificados y seleccione Todas las tareas > Operaciones avanzadas y elija Crear solicitud personalizada.

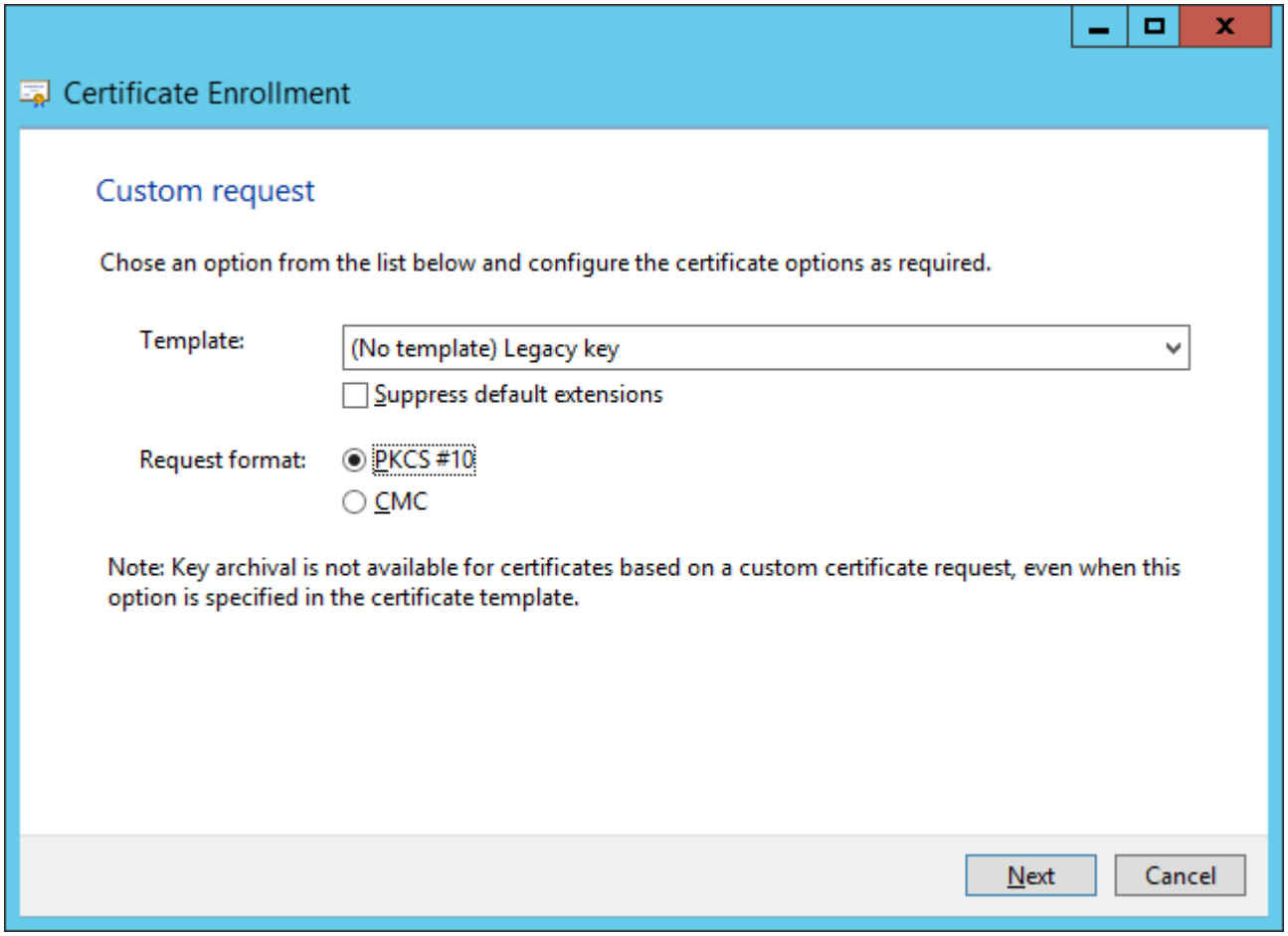


c)Se abrirá la ventana del asistente de Inscripción de certificados: haga clic en **Siguiente**.

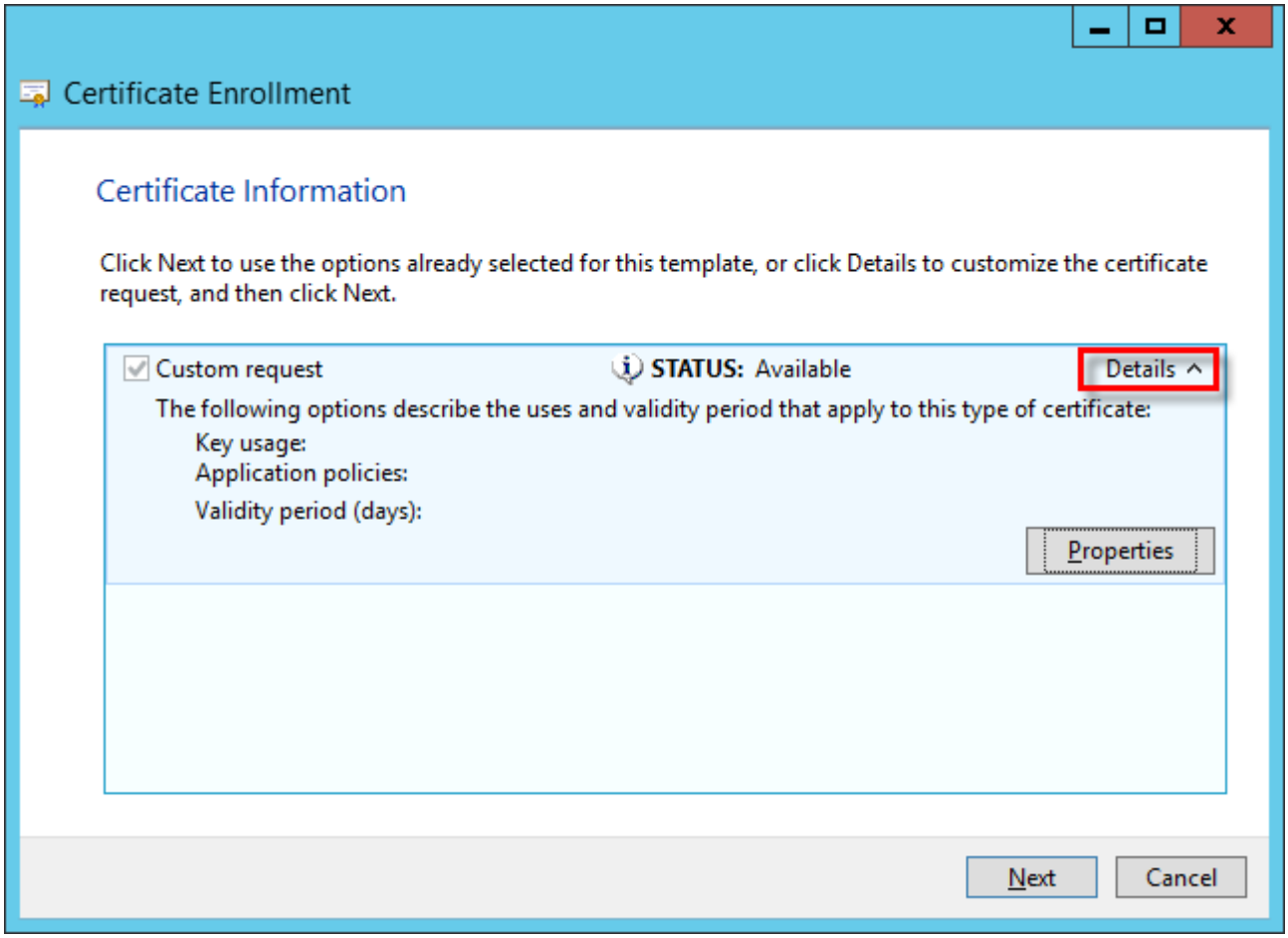
d)Seleccione **Continuar sin política de inscripción** y haga clic en **Siguiente** para continuar.



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 desplegar la sección **Detalles** y, a continuación, haga clic en **Propiedades**.



g)En la ficha **General**, escriba el **Nombre descriptivo** de su certificado; también puede introducir la descripción (opcional).

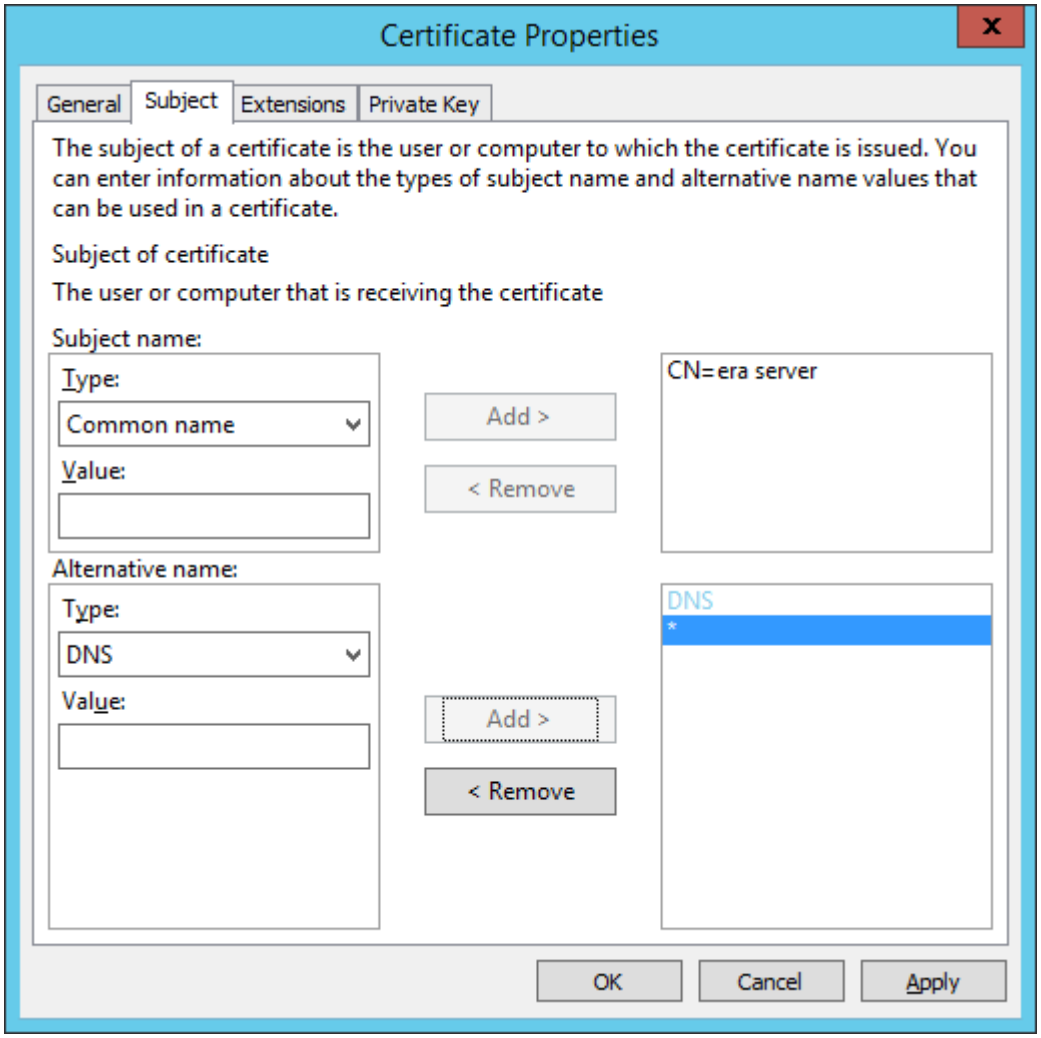
h)En la ficha **Sujeto**, haga lo siguiente:

En la sección **Nombre de sujeto**, seleccione **Nombre común** en la lista desplegable de **Tipo** e introduzca `era server` en el campo **Valor**; a continuación, haga clic en **Agregar**. **CN=era server** aparecerá en el cuadro de información de la derecha. Si está creando una solicitud de certificado para ESET Management Agent, escriba `era agent` en el campo del valor Nombre común.

El nombre común debe contener la cadena: "**servidor**" o "**proxy**", en función de la solicitud de certificado que desee crear.

i)En la sección **Nombre alternativo**, elija **DNS** en la lista desplegable de **Tipo** e introduzca * (asterisco) en el campo **Valor**; a continuación, haga clic en el botón **Agregar**.

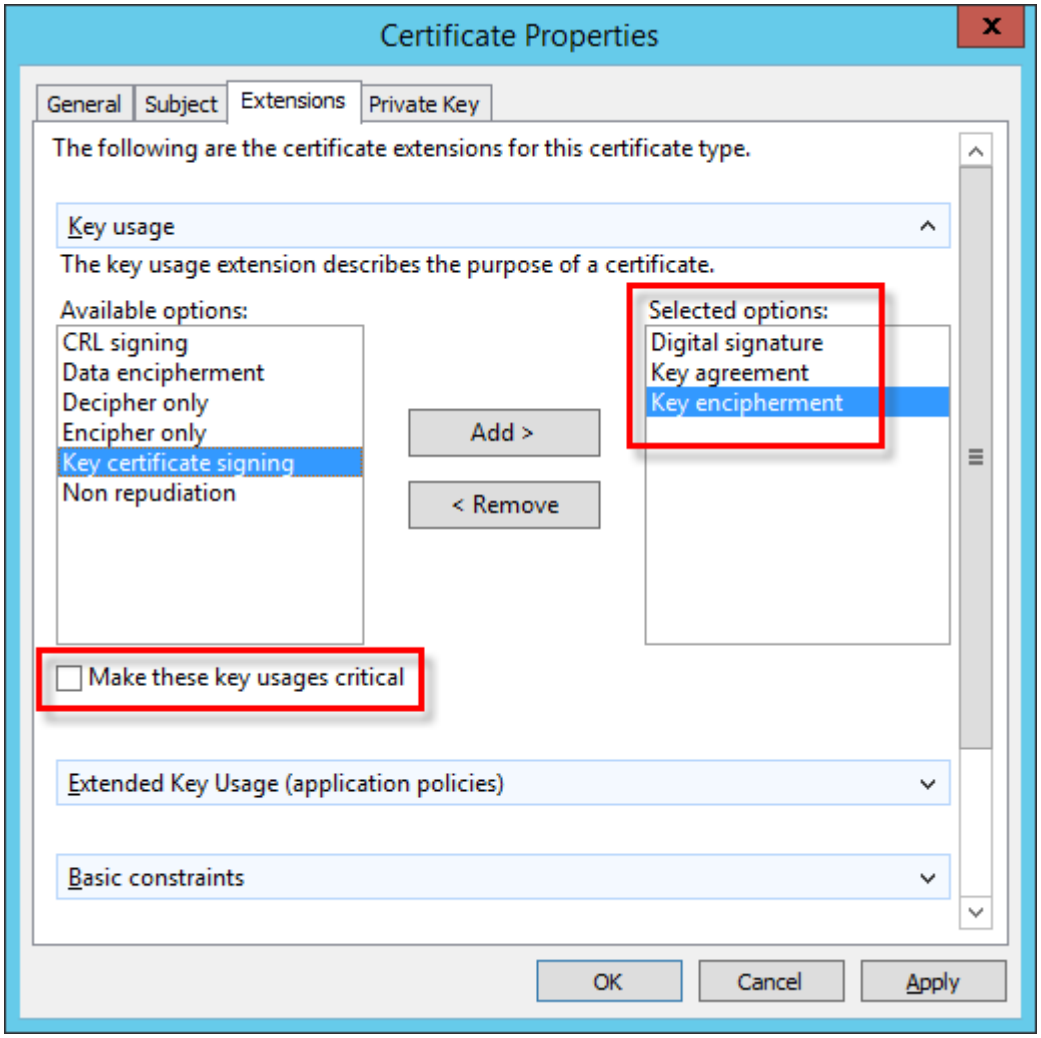
El nombre alternativo del sujeto (SAN) debe definirse como "DNS:*" para ESET PROTECT Server y para todos los agentes.



j)En la ficha **Extensiones**, despliegue la sección **Uso de la clave** haciendo clic en la flecha. Añada lo siguiente de las opciones disponibles: **Firma digital**, **Acuerdo de claves**, **Cifrado de clave**. Cancele la sección de la opción **Hacer que estos usos de clave sean críticos**.

Asegúrese de seleccionar estas 3 opciones en **Uso de claves** > **Firma de certificados clave**:

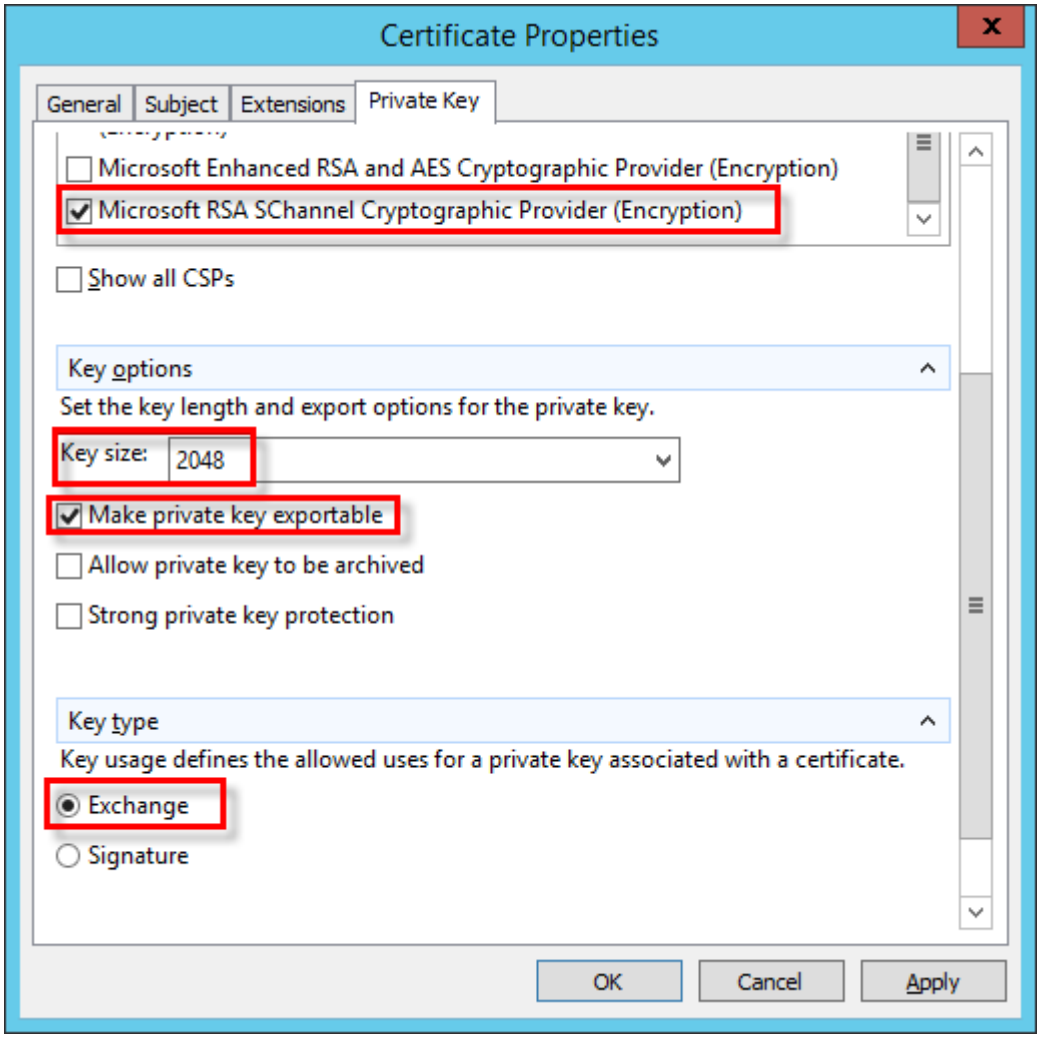
- **Firma digital**
- **Acuerdo de claves**
- **Cifrado de clave**



k)En la ficha **Clave privada**, haga lo siguiente:

i.Despliegue la sección **Proveedor de servicios de cifrado** haciendo clic en la flecha. Se mostrará una lista con todos los proveedores de servicios de cifrado (CSP). Asegúrese de seleccionar solo **Proveedor criptográfico de canales S de Microsoft RSA (Cifrado)**.

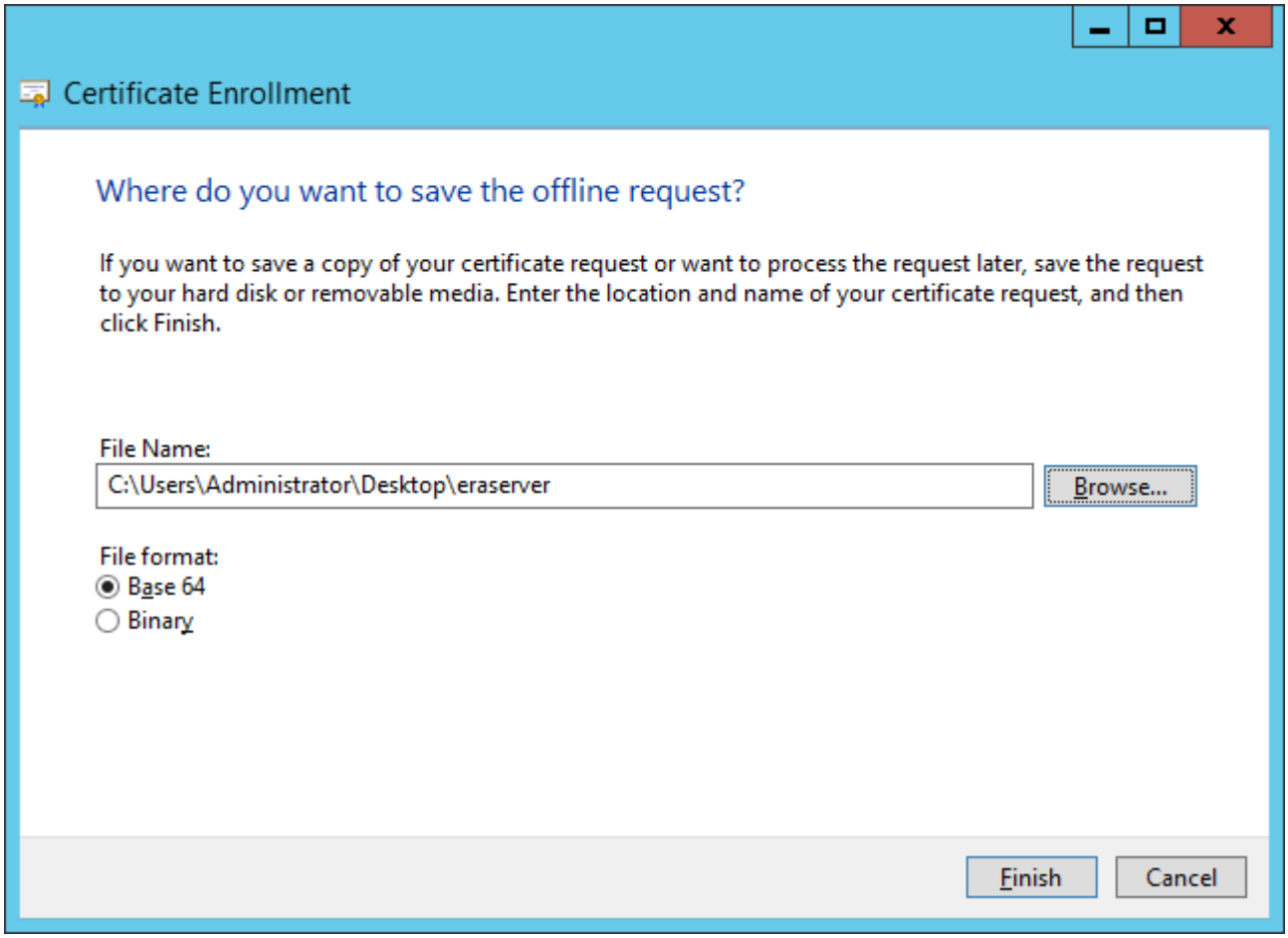
Cancele la selección de los CSP que no sean **Proveedor de cifrado Microsoft RSA SChannel (cifrado)**.



i.Despliegue la sección **Opciones de clave**. En el menú **Tamaño de la clave**, ajuste un valor mínimo de **2048**. Seleccione **Hacer exportable la clave privada**.

ii.Despliegue la sección **Tipo de clave** y seleccione **Intercambiar**. Haga clic en **Aplicar** y compruebe sus ajustes.

l)Haga clic en **Aceptar**. Aparecerá la información del certificado. Haga clic en el botón **Siguiente** para continuar. Haga clic en **Examinar** para seleccionar la ubicación en la que se guardará la solicitud de firma del certificado (CSR). Escriba el nombre del archivo y asegúrese de que esté seleccionada **Base 64**.

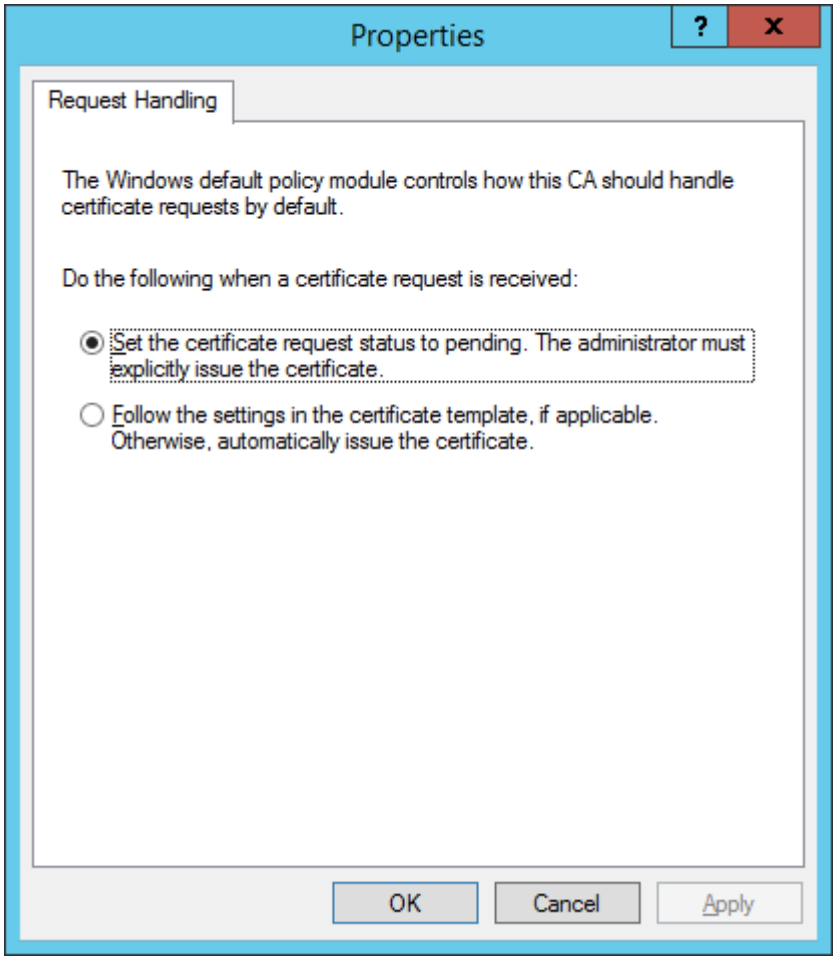


m)Haga clic en **Finalizar** para generar la CSR.

3. Siga los pasos indicados a continuación para importar su solicitud de certificado personalizado:

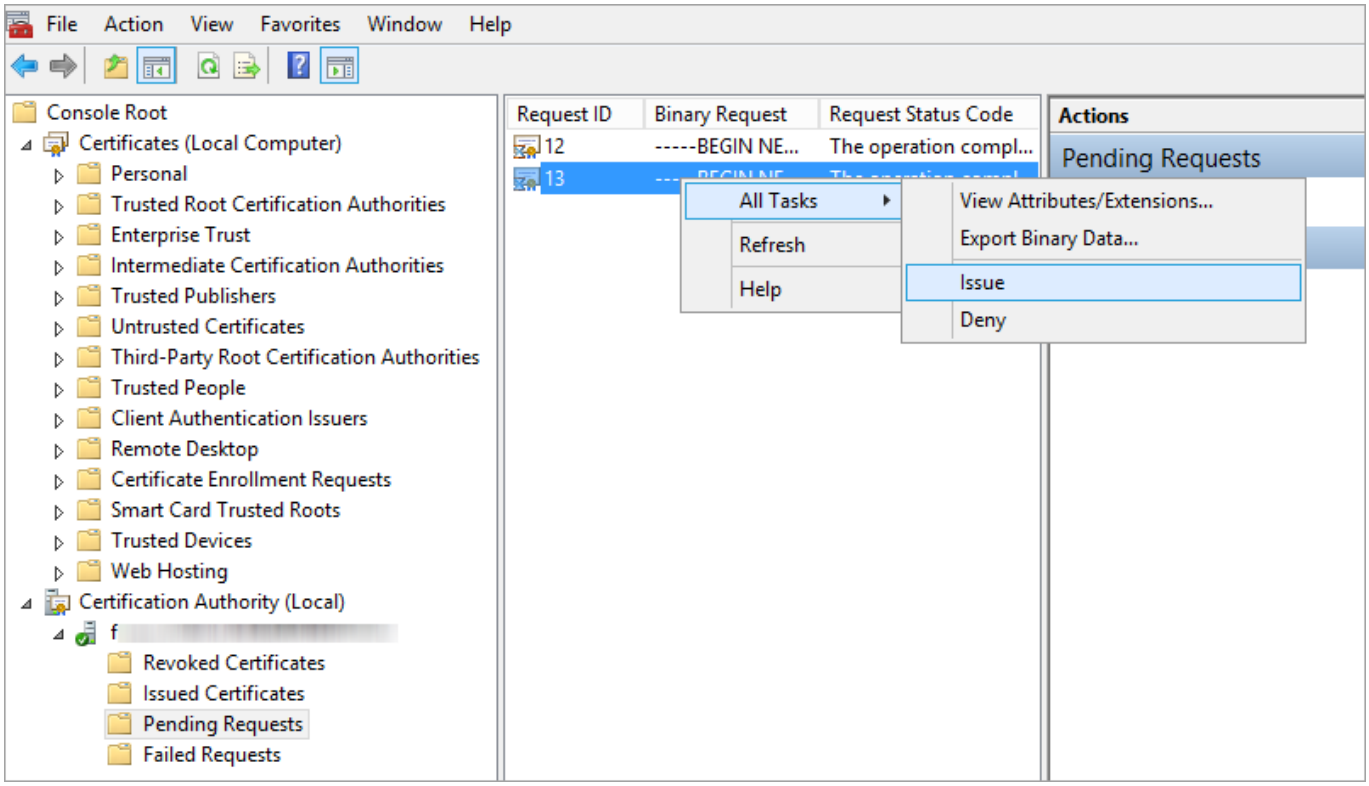
a)Abra Administrador de servidores y haga clic en **Herramientas** > **Autoridad certificadora**.

b)En el árbol **Autoridad certificadora (local)**, seleccione la ficha **Su servidor** (normalmente FQDN) > **Propiedades** y, a continuación, seleccione la ficha **Módulo de políticas**. Haga clic en **Propiedades** y seleccione **Establecer el estado de la solicitud de certificado como pendiente. El administrador debe emitir explícitamente el certificado**. De lo contrario, no funcionará correctamente. Si desea cambiar este ajuste, tendrá que reiniciar los servicios de certificados de Active Directory.



c)En el árbol **Autoridad certificadora (local)**, seleccione **Su servidor (normalmente FQDN)** > **Todas las tareas** > **Enviar nueva solicitud...** y vaya al archivo **CSR** generado anteriormente en el paso 2.

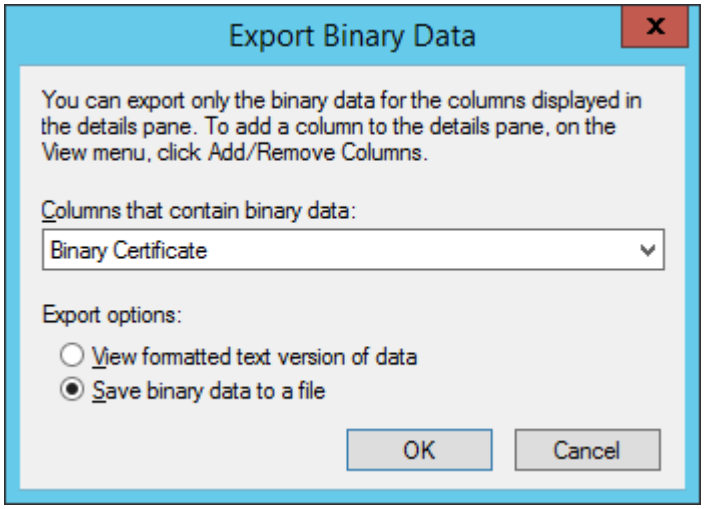
d)El certificado se agregará en **Solicitudes pendientes**. Seleccione el **CSR** en el panel de navegación derecho. En el menú **Acción**, seleccione **Todas las tareas** > **Emitir**.



4. Exporte el **Certificado personalizado emitido** al archivo *.tmp*.

a)Seleccione **Certificados** emitidos en el panel de la izquierda. Haga clic con el botón derecho del ratón en el certificado que desea exportar y haga clic en **Todas las tareas** > **Exportar datos binarios**.

b)En el cuadro de diálogo **Exportar datos binarios**, elija **Certificado binario** en la lista desplegable. En **Opciones de exportación**, haga clic en **Guardar datos binarios en un archivo** y, a continuación, haga clic en **Aceptar**.



c)En el cuadro de diálogo Guardar datos binarios, mueva la ubicación del archivo en la que desea guardar el certificado y, a continuación, haga clic en**Guardar**.

5. Importe el archivo *..tmp*.

a)Vaya a Certificado (equipo local) > haga clic con el botón derecho del ratón en Personal y seleccione Todas las tareas > Importar.

b)Haga clic en **Siguiente**.

c)Localice el archivo binario *.tmp* guardado anteriormente mediante **Examinar** y haga clic en **Abrir**. Seleccione Colocar todos los certificados en el siguiente almacén > **Personal**. Haga clic en **Siguiente**.

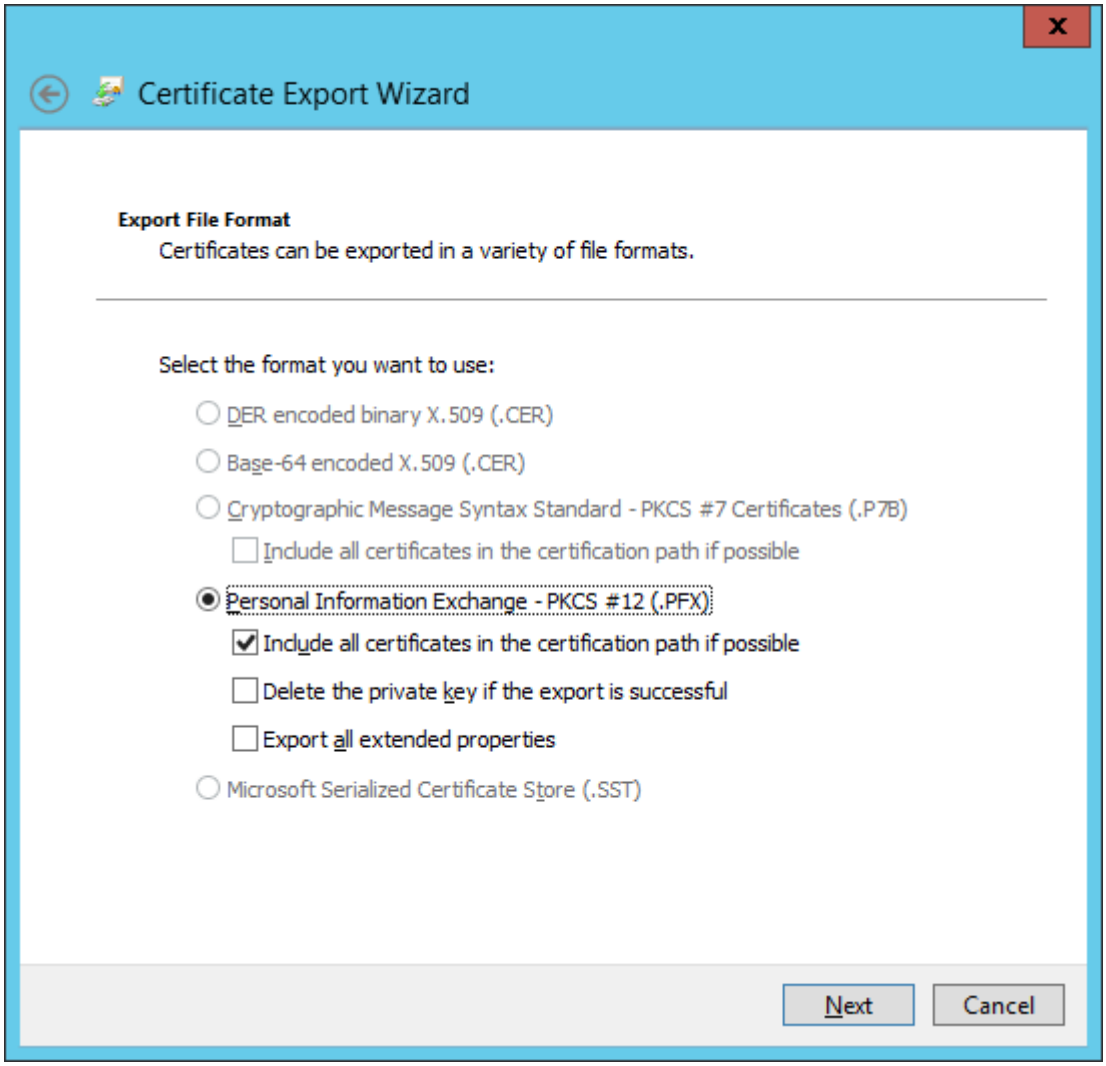
d)Haga clic en **Finalizar** para importar el certificado.

6. Exporte el certificado, incluyendo la clave privada, como archivo *.pfx*.

a)En **Certificados (equipo local)**, despliegue **Personal** y haga clic en **Certificados**, seleccione el nuevo certificado que desea exportar y, en el menú **Acción**, seleccione **Todas las tareas** > **Exportar**.

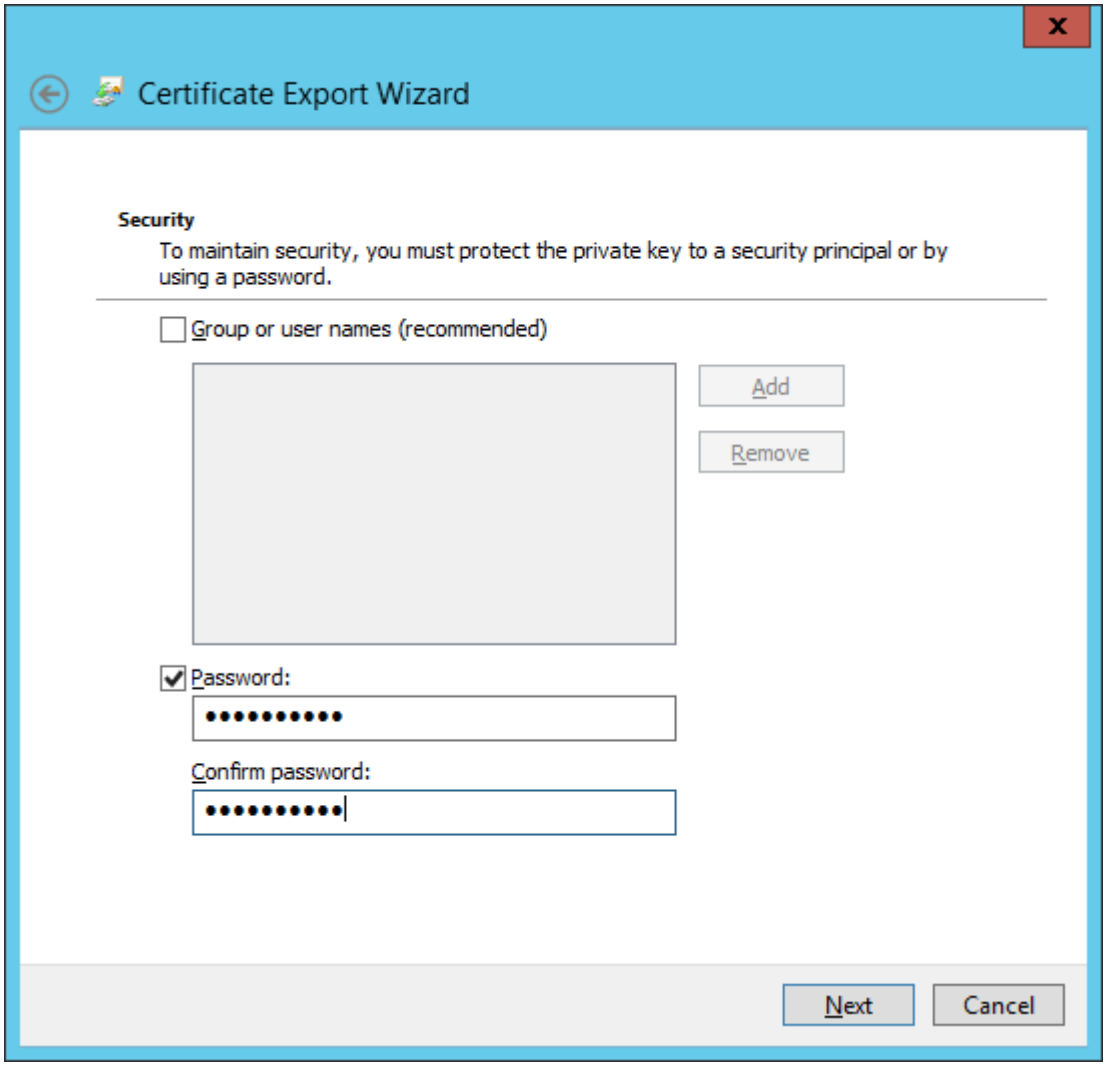
b)En **Asistente para exportación de certificados**, haga clic en **Exportar la clave privada**. (Esta opción solo aparecerá si la clave privada está marcada como exportable y tiene acceso a la clave privada).

c)En Formato de archivo de exportación, seleccione **Personal Information Exchange -PKCS #12 (.PFX)**, marque la casilla de verificación situada junto a **Incluir todos los certificados en la ruta de exportación si es posible** y, a continuación, haga clic en **Siguiente**.



d)**Contraseña**: escriba una contraseña para cifrar la clave privada que está exportando. En el campo **Confirmar contraseña**, escriba la misma contraseña de nuevo y, a continuación, haga clic en **Siguiente**.

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



e)**Nombre de archivo**: introduzca un nombre de archivo y una ruta para el archivo *.pfx* que guardará el certificado exportado y la clave privada. Haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

El ejemplo anterior le muestra cómo crear un certificado de ESET Management Agent. Repita los mismos pasos para los certificados de ESET PROTECT Server.
No puede utilizar este certificado para firmar otro certificado nuevo en la Consola web.

7. Exportar autoridad certificadora:

a)Abra Administrador de servidores y haga clic en **Herramientas** > **Autoridad certificadora**.

b)En el árbol **Autoridad certificadora (local)**, seleccione la ficha **Su servidor (normalmente FQDN)** > **Propiedades** > ficha **General** y haga clic en **Ver certificado**.

c)En la ficha **Detalles**, haga clic en **Copiar a archivo**. Se abrirá el **Asistente para exportación de certificados**.

d)En la ventana **Formato de archivo de exportación**, seleccione **DER binario codificado X.509 (.CER)** y haga clic en **Siguiente**.

e)Haga clic en **Examinar** para seleccionar la ubicación en la que se guardará el archivo *.cer* y, a continuación, haga clic en **Siguiente**.

f)Haga clic en **Finalizar** para exportar la autoridad certificadora.

Para obtener instrucciones detalladas de cómo utilizar los certificados personalizados en ESET PROTECT On-Prem, consulte el siguiente capítulo.

Cómo utilizar certificados personalizados con ESET PROTECT On-Prem

Para continuar desde el capítulo anterior:

1. Importe su autoridad certificadora de terceros en ESET PROTECT Web Console.

2. Configure el nuevo certificado del servidor personalizado en ESET PROTECT Web Console.

> Si ya tiene instancias de ESET Management Agent que se conectan a ESET PROTECT Server, aplique una política para cambiar el certificado personalizado de los ESET Management Agent:
> 1.Abra ESET PROTECT Web Console.
> 2.Haga clic en **Políticas** > **Nueva**. Escriba el Nombre de la política.
> 3.Despliegue **Configuración** y seleccione **ESET Management Agent** en el menú desplegable.
> 4.Despliegue **Conexión** y haga clic en **Cambiar certificado** junto a **Certificado**.
> 5.Haga clic en **Certificado personalizado** y seleccione el certificado personalizado para ESET Management Agent.
> 6.Escriba la contraseña del 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 **ESET Management Agent** y seleccione **Cambiar**.

4. Haga clic en **Siguiente** y ejecute **Reparar**.

5. Conserve los ajustes de host y puerto del servidor y, a continuación, haga clic en **Siguiente**.

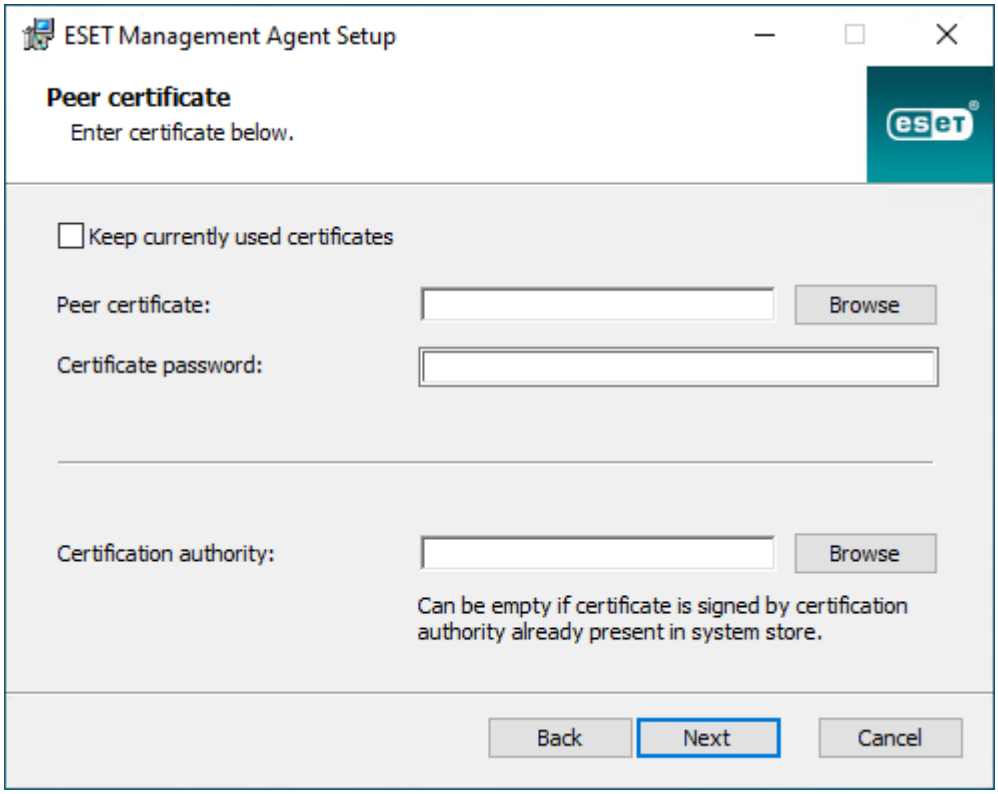
6. Haga clic en **Examinar** junto a **Certificado de igual** y busque el archivo del certificado *.pfx* personalizado.

7. Escriba la contraseña del certificado que especificó en el paso 6.

8. Haga clic en **Examinar** junto a **Autoridad certificadora y seleccione el archivo** .der (clave pública) exportado desde la Consola web. Debe ser una clave pública firmada con el certificado personalizado.

9. Haga clic en **Siguiente** y complete la reparación.

10. ESET Management Agent ahora ya utiliza el certificado *.pfx*.



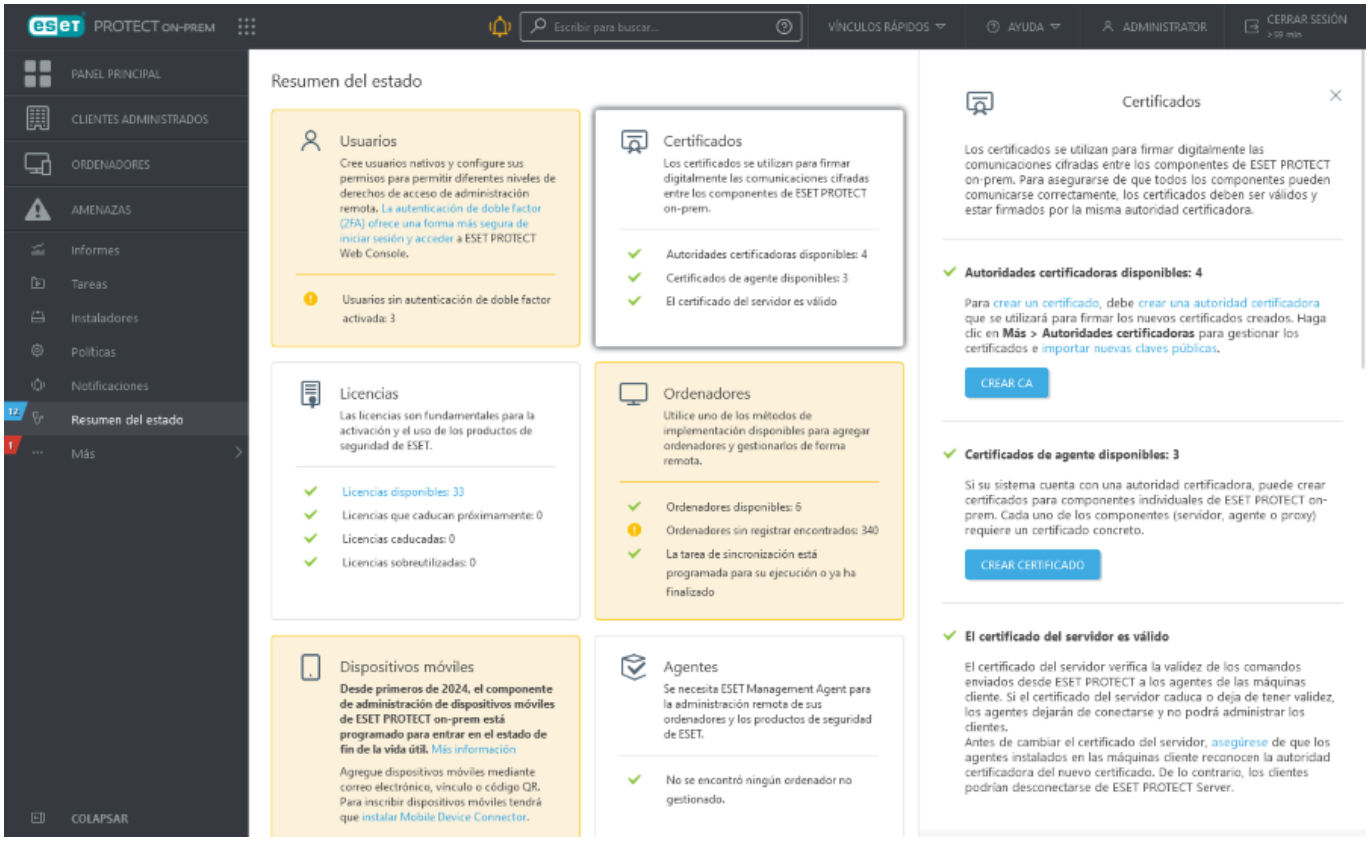
Certificado con caducidad próxima: informe y sustitución

ESET PROTECT On-Prem puede avisarle si un certificado o una autoridad certificadora van a caducar. Existen **Notificaciones** predefinidas para el certificado de ESET PROTECT y la autoridad certificadora de ESET PROTECT en la ficha **Notificaciones**.

Para activar esta función, haga clic en **Modificar notificación** y especifique los detalles en la sección Distribución, como, por ejemplo, la dirección de correo electrónico o la captura SNMP. Cada usuario puede ver únicamente las notificaciones correspondientes a los certificados que están en su grupo de inicio (si se le han asignado permisos de **Lectura** de los **Certificados**).

Asegúrese de primero haber configurado los ajustes de la conexión SMTP en **Más** > **Ajustes.** Tras hacerlo puede modificar la notificación para agregar la dirección de correo electrónico de distribución.

La ESET PROTECT Web Console informa de una advertencia si un certificado o una autoridad certificadora está a punto de caducar en menos de 90 días. La advertencia aparece en Ordenadores, Resumen del estado, Certificados de iguales y Autoridades certificadoras.



Para sustituir una autoridad certificadora o un certificado que van a caducar, siga estos pasos:

1. Cree una nueva autoridad certificadora con un nuevo periodo de validez (si el anterior va a terminar), idealmente con validez inmediata.

2. Cree nuevos certificados de iguales para ESET PROTECT Server y otros componentes (Agent/MDM) dentro del periodo de validez de la autoridad certificadora nueva.

3. Cree políticas para establecer nuevos certificados de igual. Aplique las políticas a los componentes de ESET PROTECT, ERA Proxy, MDM y a ESET Management Agent en todos los ordenadores cliente de su red.

4. Espere a que la nueva autoridad certificadora y los certificados de igual se apliquen y los clientes se repliquen.

> Le recomendamos esperar 24 horas o comprobar si todos sus componentes de ESET PROTECT (agentes) se han replicado al menos dos veces. Puede aplicar la replicación del agente en **Ordenadores** haciendo clic en el ordenador y seleccionando **Enviar llamada de activación**.

5. Sustituya el certificado del servidor en la configuración de ESET PROTECT Server para que los clientes puedan autenticarse utilizando los nuevos certificados de igual.

6. Reinicie el servicio ESET PROTECT Server.

7. Cuando haya realizado todos los pasos indicados anteriormente, todos los clientes se conecten a ESET PROTECT On-Prem y todo funcione como se espera, revoque los antiguos certificados de igual y elimine la autoridad certificadora antigua.

Autoridades certificadoras

Las autoridades certificadoras aparecen en la sección **Autoridades certificadoras**, desde donde además se administran. Si cuenta con varias autoridades certificadoras, podrá aplicar un filtro para ordenarlas.

> A las autoridades certificadoras y a los certificados se accede utilizando los mismos permisos que para la función **Certificados**. Los certificados y autoridades creados durante la instalación, y los creados posteriormente por el administrador, están en el grupo estático **Todo**. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Haga clic en **Acciones** para administrar la autoridad certificadora seleccionada:

- **Nuevo**: crear una nueva autoridad certificadora
- **Etiquetas** - Edite las etiquetas (puede asignar, cancelar la asignación, crear y eliminar).
- **Modificar**: cambie la descripción de la autoridad certificadora.
- **Registro de auditoría** - Permite ver el Registro de auditoría del elemento seleccionado.
- **Eliminar**: eliminar la autoridad certificadora seleccionada
- Importar clave pública
- Exportar clave pública: utilice esta opción para hacer una copia de seguridad de sus autoridades certificadoras.
- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen suficientes derechos para el grupo de destino. Cambiar el grupo de acceso resulta útil para resolver 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.

Filtros y personalización del diseño

Puede personalizar la vista de pantalla actual de Web Console:

- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

Cómo dividir el acceso a certificados y autoridades

Si el *administrador* no quiere permitir que el usuario *John* acceda a las autoridades certificadoras 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. Llamar a este conjunto de permisos *Permisos para certificados*.
   b. Agregar un grupo llamado *Certificados* en la sección **Grupos estáticos**.
   c. En la sección **Funcionalidad**, seleccionar **Escritura** 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 del grupo **Todo** al grupo recién creado **Certificados**:
   a. Diríjase a **Más** > **Certificados de iguales**.
   b. Marcar las casillas situadas junto a los certificados que quiera mover.
   c. Hacer clic en **Acciones** > **Grupo de acceso**, seleccionar el grupo **Certificados** y, a continuación, hacer clic en **Aceptar**.

John ya puede modificar y utilizar los certificados movidos. No obstante, las autoridades certificadoras están almacenadas fuera del alcance de este usuario. *John* ni siquiera podrá utilizar las autoridades existentes (del grupo **Todo**) para firmar certificados.

Crear una nueva autoridad certificadora

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 certificadora

Escriba la **Descripción** de la autoridad certificadora y seleccione una **Frase de contraseña**. Esta **Frase de contraseña** debe contener como mínimo 12 caracteres.

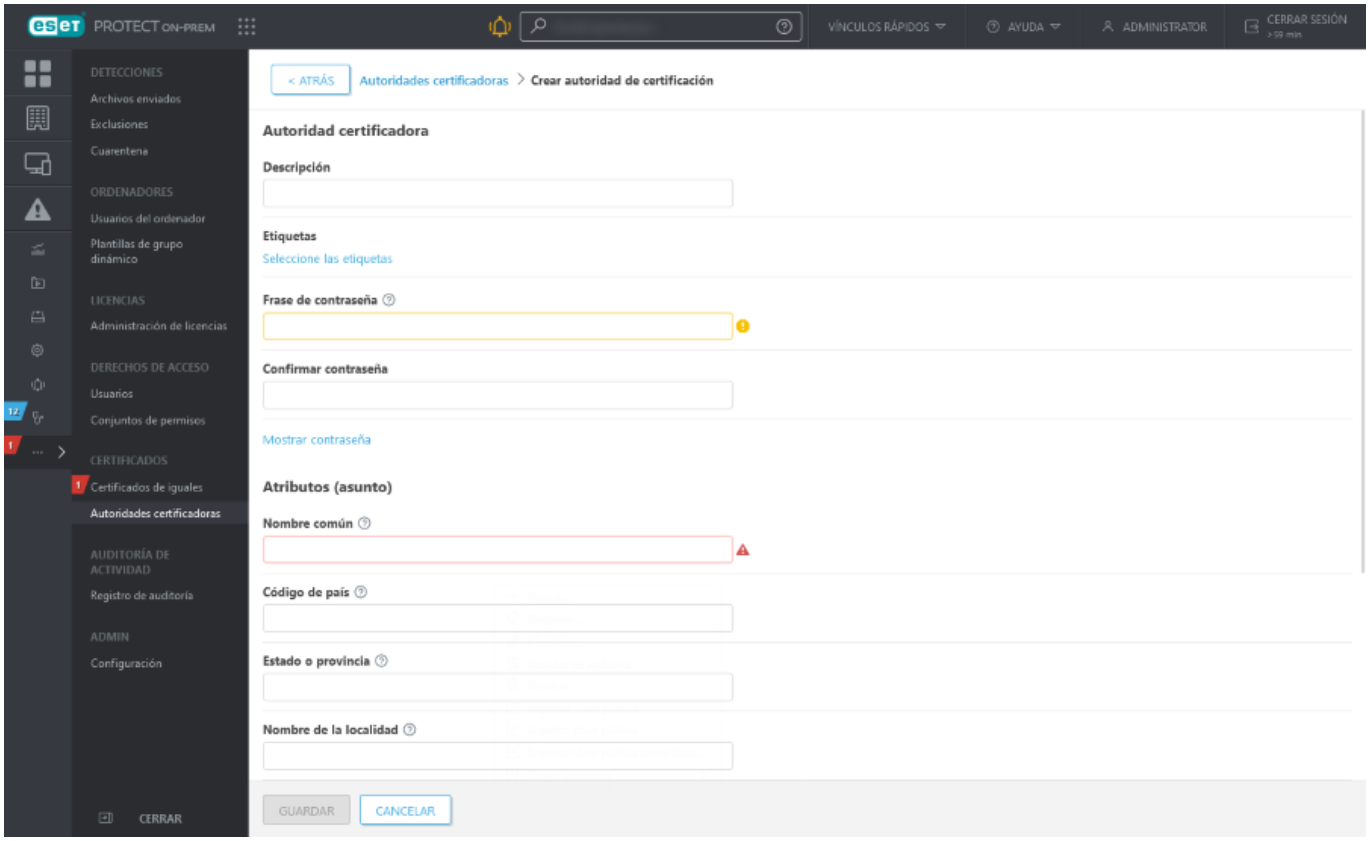
Atributos (asunto)

1. Escriba el **Nombre común** (nombre) de la autoridad certificadora. Con el fin de diferenciar las diversas autoridades certificadoras, seleccione un nombre exclusivo. Si lo desea, puede introducir información descriptiva sobre la autoridad certificadora.

2. Introduzca los valores **Válido desde** y **Válida hasta** para asegurarse de que el certificado es válido.

El valor Válido desde de todos los certificados y las autoridades certificadoras creadas durante la instalación de los componentes de ESET PROTECT se establece en 2 días antes de la creación del certificado.
El valor Válido desde de todos los certificados y las autoridades de certificación creados en ESET PROTECT Web Console se establece en 1 día antes de la creación del certificado. La finalidad de esta medida es cubrir todas las discrepancias de tiempo posibles entre los sistemas afectados.
Por ejemplo, una autoridad certificadora y un certificado creados el 12 de enero de 2017 durante la instalación, tendrán un valor Válido desde predefinido del 10 de enero de 2017 a las 10 00:00:00, mientras que una autoridad certificadora y un certificado creados el 12 de enero de 2017 en ESET PROTECT Web Console tendrán un valor Válido desde predefinido del 11 de enero de 2017 a las 00:00:00.

3. Haga clic en **Guardar** para guardar la nueva autoridad certificadora. Al hacerlo, esta aparecerá en la lista de autoridades certificadoras disponible en **Más** > **Autoridades certificadoras**, y ya está disponible para utilizarla. La autoridad certificadora se crea en el grupo principal del usuario que la ha creado.



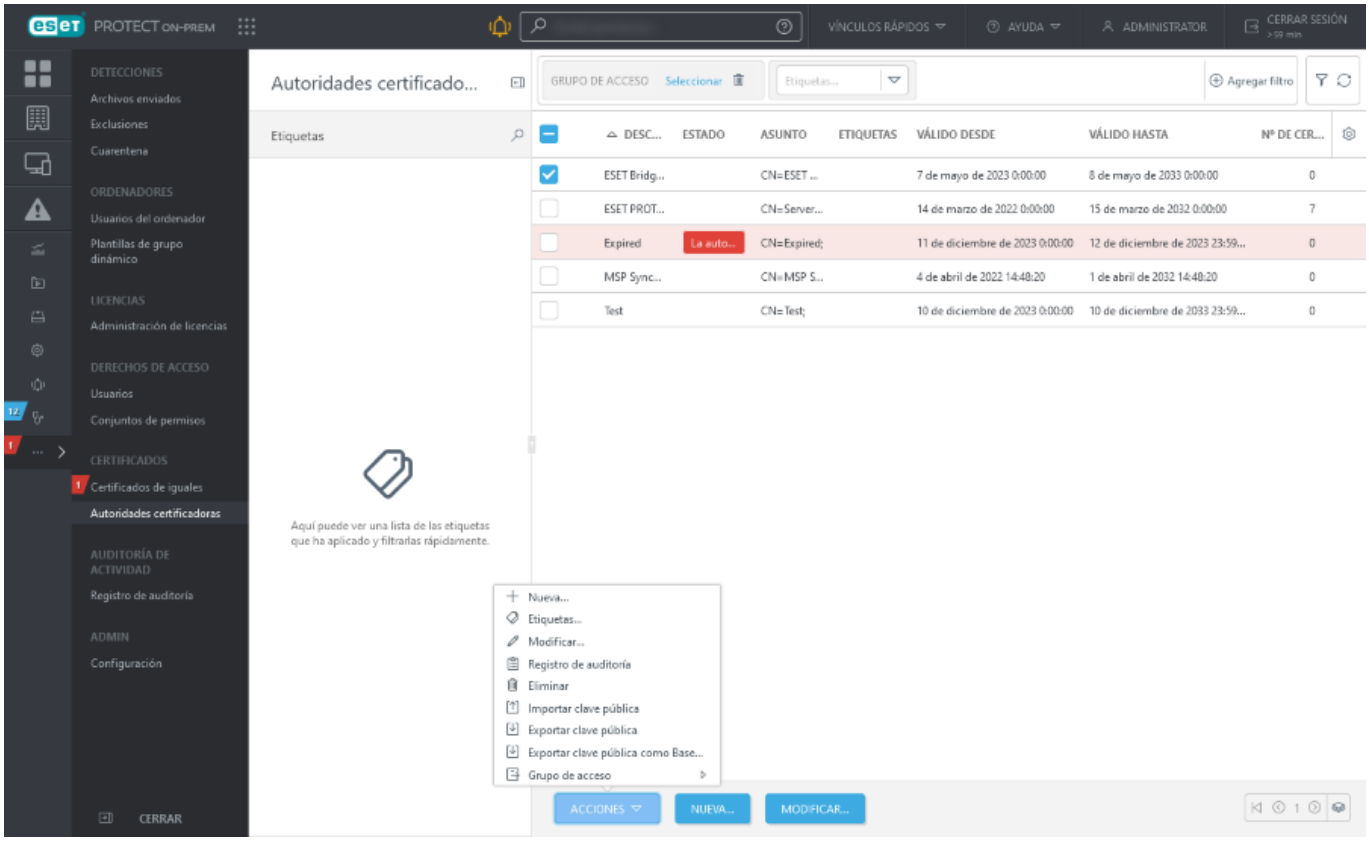
Para gestionar la autoridad certificadora, marque la **casilla de verificación** situada junto a la autoridad certificadora en la lista y utilice el menú contextual (haga clic con el botón izquierdo en la autoridad certificadora) o el botón **Acción** situado al final de la página. Las opciones disponibles son Importar clave pública y Exportar una clave pública o **Modificar** la autoridad certificadora.

Exportar una clave pública

Para exportar una autoridad certificadora, haga clic en **Más** > **Autoridades certificadoras**.

> Para exportar una clave pública, un usuario debe tener derechos de Uso de Certificados. Consulte la lista completa de derechos de acceso para obtener más información.

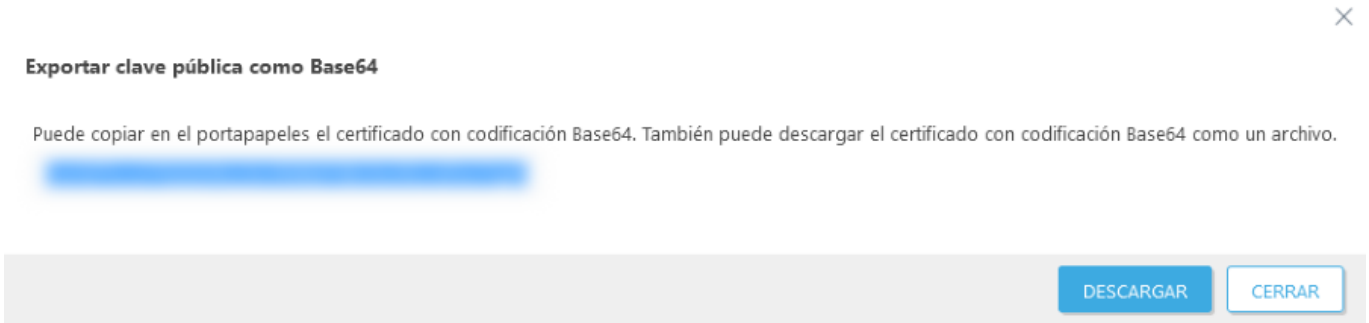
1. Seleccione en la lista la autoridad certificadora que desee usar, y active la casilla de verificación situada junto a ella.



2. Seleccione una de las opciones de exportación:

a.Seleccione **Acciones** > **Exportar clave pública**. Seleccione esta opción si quiere importar la clave pública en otra instalación de ESET PROTECT On-Prem (migración de un servidor a otro). Escriba el nombre de la clave pública y haga clic en **Guardar**. La clave pública se exportará como archivo *.der*.

b.Seleccione **Acciones** > **Exportar clave pública como Base64**. Puede copiar la cadena del certificado con codificación Base64 o hacer clic en **Descargar** para descargar el certificado con codificación Base64 como un archivo.



Si elimina la autoridad certificadora de ESET PROTECT predeterminada y crea una nueva, no funcionará. Antes de reemplazar la autoridad certificadora, debe crear y distribuir certificados de iguales firmados por la nueva autoridad. También debe cambiar el certificado del servidor en la **Más** > Configuración y, posteriormente, reiniciar el servicio ESET PROTECT Server.

Importar una clave pública

Para importar una autoridad certificadora externa, haga clic en **Más** > **Autoridades certificadoras**.

1.Haga clic en el botón **Acciones** y, luego, seleccione **Importar clave pública**.

2.**Elija el archivo que desea cargar**: haga clic en **Examinar** y desplácese hasta el archivo que desee importar. Solo puede importar un archivo *.der*.

3.Introduzca la **Descripción** del certificado y haga clic en **Importar**. La autoridad certificadora ya se ha importado correctamente.

Registro de auditoría

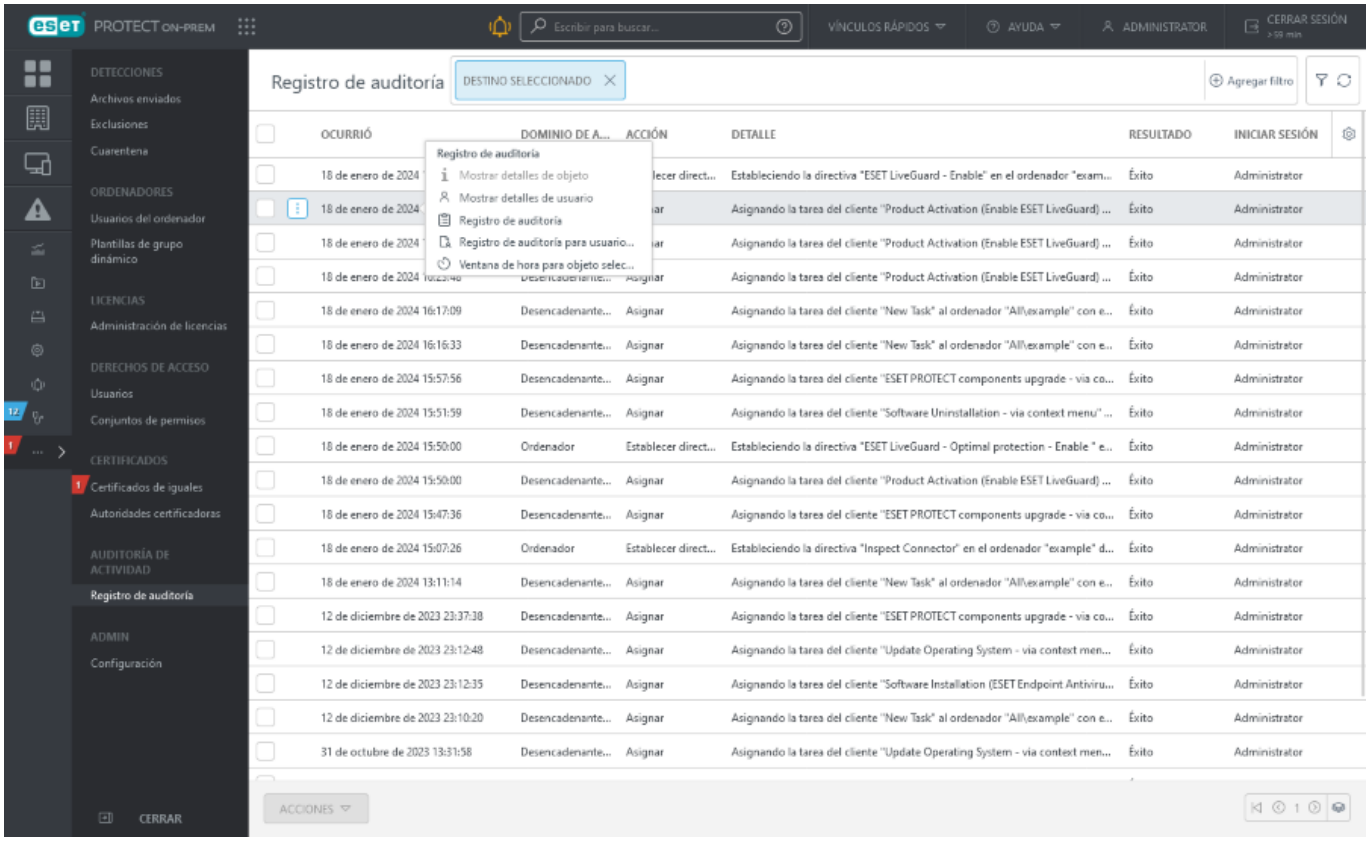
Cuando un usuario realiza una acción en ESET PROTECT Web Console, se registra la acción. Los registros de auditoría se crean si un objeto de ESET PROTECT Web Console (por ejemplo, un ordenador, una política, una detección, etc.) se crea o modifica.

Registro de auditoría es una nueva pantalla disponible en ESET PROTECT On-Prem. Registro de auditoría contiene la misma información que el Informe de registro de auditoría, pero permite un filtrado cómodo de los datos mostrados. También puede ver directamente el registro de auditoría filtrado de diferentes objetos de Web Console haciendo clic en el objeto de consola web y seleccionando **Registro de auditoría**.

Registro de auditoría permite al administrador inspeccionar las actividades realizadas en ESET PROTECT Web Console, sobre todo si hay más usuarios de Web Console.

Para ver el registro de auditoría, el usuario de Web Console debe tener un conjunto de permisos con la funcionalidad **Registro de auditoría**.

Con el permiso Registro de auditoría, el usuario puede ver las acciones registradas del resto de usuarios y dominios, incluso las relacionadas con los activos que el usuario no tiene permisos suficientes para ver.



Haga clic en una línea de Registro de auditoría para realizar las siguientes acciones:

Mostrar detalles de objeto	Mostrar los detalles del objeto auditado.
Mostrar detalles de usuario	Mostrar los detalles del usuario que realizó la acción en el objeto.
Registro de auditoría	Mostrar el Registro de auditoría del objeto seleccionado.
Registro de auditoría para usuario seleccionado	Mostrar el Registro de auditoría del usuario seleccionado.
Ventana de hora para objeto seleccionado	Mostrar el Registro de auditoría del objeto seleccionado con un filtro activado de hora a la que se produjo.

Haga clic en **Agregar filtro** para filtrar la vista de la tabla por varios criterios:

- **<= Ocurrió**: establezca la fecha y la hora antes de la cual se produjo la acción.
- **>= Ocurrió**: establezca la fecha y la hora después de la cual se produjo la acción.
- **Acción**: seleccione la acción que se realizó.
- **Auditar dominio**: seleccione el objeto de Web Console modificado.
- **Auditar usuario**: seleccione el usuario de Web Console que realizó la acción.
- **Resultado**: seleccione el resultado de la acción.

Configuración

En esta sección puede configurar opciones específicas para el servidor de ESET PROTECT propiamente dicho. Estos ajustes son similares a las políticas, pero se aplican directamente en ESET PROTECT Server.

Conexión

Puerto de servidor (requiere reiniciar): es el puerto de conexión entre los servidores y los agentes de ESET PROTECT. Para cambiar esta opción y que el cambio surta efecto, es necesario reiniciar el servicio ESET PROTECT Server. El cambio de puerto podría requerir modificaciones en la configuración del cortafuegos.

Puerto de Web Console (requiere reiniciar): puerto de conexión entre ESET PROTECT Web Console y ESET PROTECT Server. El cambio de puerto podría requerir modificaciones en la configuración del cortafuegos.

Seguridad avanzada (requiere reiniciar): este ajuste activa la seguridad avanzada de la comunicación de red de los componentes de ESET PROTECT. La seguridad avanzada está habilitada de forma predeterminada.

Certificado (requiere reiniciar): aquí puede administrar certificados de ESET PROTECT Server. Haga clic en Cambiar certificado y seleccione el certificado de ESET PROTECT Server que debe utilizar su ESET PROTECT ERA Server. Para obtener más información, consulte Certificados de igual.

Estos cambios requieren el reinicio del servicio de ESET PROTECT Server. Consulte nuestro artículo de la base de conocimiento para ver las instrucciones.

Actualizaciones

Intervalo de actualización: intervalo con el que se recibirán las actualizaciones. Puede seleccionar un intervalo regular y configurar los ajustes o utilizar una expresión CRON.

Servidor de actualizaciones: el servidor de actualizaciones del que ESET PROTECT Server recibe las actualizaciones de las versiones de productos de ESET y los componentes de ESET PROTECT. Para actualizar ESET PROTECT On-Prem 11.0 desde un mirror (herramienta Mirror), establezca la dirección completa de la carpeta de actualización `era6` (según la ubicación raíz de su servidor HTTP). Por ejemplo:

```
http://your_server_address/mirror/eset_upd/era6
```

Tipo de actualización: seleccione el tipo de actualización de módulos de ESET PROTECT Server que desea recibir. Puede saber la versión actual de los módulos de ESET PROTECT Server que tiene instalada en **Ayuda** > **Acerca de**.

Actualización normal	Las actualizaciones de los módulos de ESET PROTECT Server se descargarán automáticamente del servidor de ESET en el que haya menos tráfico de red. Configuración predeterminado.
Actualización de prueba	Estas actualizaciones se han sometido a pruebas internas y estarán disponibles al público en general en breve. La ventaja de activar las actualizaciones de prueba es tener acceso a las actualizaciones más recientes de los módulos de ESET PROTECT Server. En algunos casos, las actualizaciones de prueba pueden ayudar a resolver problemas con ESET PROTECT Server. No obstante, las actualizaciones previas a su lanzamiento pueden no ofrecer la máxima estabilidad en todo momento, y no deben utilizarse en servidores de producción en los que se necesite la máxima disponibilidad y estabilidad. Las actualizaciones de prueba solo están disponibles cuando se define AUTOSELECT en el parámetro **Servidor de actualizaciones**.

Configuración avanzada

Proxy HTTP: utilice un servidor proxy para facilitar el tráfico de Internet hacia los clientes de su red. Si instala ESET PROTECT On-Prem con el instalador Todo en uno, el proxy HTTP está activado de forma predeterminada. La configuración de Proxy HTTP no se aplica para la comunicación con servidores de autenticación de doble factor.

Llamada de activación: ESET PROTECT Server puede ejecutar una replicación instantánea de ESET Management Agent en un equipo cliente desde EPNS. Esto es útil cuando no quiere esperar al intervalo regular en el que el ESET Management Agent se conecta al ESET PROTECT Server. Por ejemplo, cuando desea que una tarea se ejecute de inmediato en los clientes o si desea que una política se aplique directamente.

Wake on LAN: configure **Direcciones de multidifusión** si quiere enviar llamadas Wake on LAN a una o más direcciones IP.

Servidor SMTP: utilice un servidor SMTP para permitir que ESET PROTECT Server envíe mensajes de correo electrónico (por ejemplo, informes o notificaciones por correo electrónico). Especifique los detalles de su servidor SMTP.

Active Directory: puede preajustar su configuración de AD. ESET PROTECT On-Prem usa sus credenciales de forma predeterminada en las tareas de sincronización con Active Directory (sincronización de usuarios, sincronización de grupos estáticos). Si los campos relacionados se dejan en blanco en la configuración de la tarea, ESET PROTECT On-Prem usa las credenciales preajustadas. Utilice un usuario de AD de solo lectura, ESET PROTECT On-Prem no realiza ningún cambio en la estructura de AD.

Si se está ejecutando ESET PROTECT Server en Linux (o un dispositivo virtual), deberá tener un archivo de configuración de *Kerberos* correctamente configurado. Puede configurar *Kerberos* para que se sincronice con varios dominios.

Si ESET PROTECT Server se está ejecutando en un equipo Windows conectado a un dominio, solo es necesario el campo **Cliente**. Se puede llevar a cabo la sincronización entre más dominios si estos dominios han establecido confianza.

- **Host** - Escriba el nombre de servidor o la dirección IP de su controlador de dominio.
- **Nombre de usuario** - Escriba el nombre de usuario de su controlador de dominio con el siguiente formato:
  - `DOMAIN\username` (ESET PROTECT Server en ejecución en Windows)
  - `username@FULL.DOMAIN.NAME` o `username` (ESET PROTECT Server en ejecución en Linux).

> Escriba el dominio en mayúsculas, ya que este formato es necesario para autenticar las consultas correctamente en un servidor de Active Directory.

- **Contraseña**: escriba la contraseña que se usa para iniciar sesión en su controlador de dominio.
- **Contenedor raíz**: especifique el identificador completo de un contenedor de AD, como por ejemplo: `CN=John,CN=Users,DC=Corp`. Se usa como **Nombre distinguido** preajustado. 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).

En Windows, ESET PROTECT utiliza el protocolo cifrado LDAPS (LDAP a través de SSL) de forma predeterminada para todas las conexiones de Active Directory (AD). También puede configurar LDAPS en el dispositivo virtual de ESET PROTECT.
Para establecer una conexión con Active Directory a través de LDAPS, realice los siguientes ajustes:
1. El controlador de dominio debe tener instalado un certificado de máquina. Para emitir un certificado para su controlador de dominio, siga los pasos indicados a continuación:
a)Abra el **Administrador de servidores**, haga clic en **Administrar** > **Agregar roles y características** e instale la autoridad (**Servicios de certificados de Active Directory** > **Autoridad certificadora**). Se creará una nueva autoridad certificadora en **Autoridades certificadoras de confianza**.
b)Diríjase a **Inicio** > escriba `certmgr.msc` y pulse **Entrar** para ejecutar el complemento **Certificados** Microsoft Management Console > **Certificados: ordenador local** > **Personal** > haga clic con el botón derecho del ratón en el panel vacío > **Todas las tareas** > **Solicitar nuevo certificado** > rol **Inscribir controlador de dominio** role.
c)Compruebe que el certificado emitido contenga el FQDN del controlador de dominio.
d)En el servidor de ESET PROTECT, importe la autoridad certificadora que generó para el almacén de certificados (con la herramienta `certmgr.msc`) en la carpeta de autoridades certificadoras de confianza.
2. Cuando proporcione la configuración de conexión al servidor de Active Directory, escriba el FQDN del controlador de dominio (como se indica en el certificado del controlador de dominio) en el campo **Servidor** o en el campo **Host**. La dirección IP ya no es suficiente para LDAPS.
Si desea activar el uso del protocolo LDAP, marque la casilla de verificación **Usar LDAP en lugar de Active Directory** en la tarea Sincronización de grupos estáticos o Sincronización de usuarios.

Servidor de Syslog: puede usar ESET PROTECT On-Prem para enviar notificaciones y mensajes de eventos a su servidor de Syslog. También puede exportar registros desde el producto de ESET de un ordenador cliente y enviarlos al servidor de Syslog.

Grupos estáticos: permite el emparejado automático de los ordenadores encontrados con los ordenadores que ya están presentes en los grupos estáticos. El emparejado actúa en el nombre de host del que informa ESET Management Agent y, si no puede confiarse en él, se debe desactivar. Si el emparejado falla, el ordenador se colocará en el grupo Perdidos y encontrados.

Repositorio: la ubicación del repositorio en el que se almacenan todos los archivos de instalación.

- El repositorio predeterminado de ESET está establecido en **AUTOSELECT** (apunta a: *http://repository.eset.com/v1*). Este ajuste determina automáticamente el servidor de repositorio que ofrece la mejor conexión según la ubicación geográfica (dirección IP) de ESET PROTECT Server (mediante CDN, Red de distribución de contenido). Por tanto, no tiene que cambiar la configuración del repositorio.
- Si lo desea, puede ajustar un repositorio que usa solo los servidores de ESET: *http://repositorynocdn.eset.com/v1*.
- No use nunca una dirección IP para acceder al repositorio de ESET.
- Puede crear y utilizar un repositorio sin conexión.

Participar en el programa para la mejora del producto: active o desactive el envío de informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto).

Nivel de detalle de seguimiento de registros: establezca el nivel de detalle del registro para determinar la cantidad de información que se recogerá y registrará de **Trazar** (datos meramente informativos) a **Fatal** (la información más importante).

Aquí puede encontrar los archivos de registro más recientes de ESET PROTECT Server:

- Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

- Linux: */var/log/eset/RemoteAdministrator/Server/*

Puede configurar la 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 periódicamente los registros. La limpieza de la base de datos elimina estos tipos de registro: Registros de SysInspector, registros de diagnóstico, registros que ya no se recopilan (registros de dispositivos eliminados, registros de plantillas de informe eliminadas). El proceso de limpieza de la base de datos se ejecuta, de forma predeterminada, todas las noches a medianoche. Los cambios realizados en este ajuste tendrán efecto en la siguiente limpieza. Puede establecer el intervalo de limpieza de estos tipos de registro:

Tipo de registro	Ejemplo de tipo de registro
Registros de detección	• 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 del registro de auditoría.
Registros de supervisión	• Control de dispositivos • Control de acceso web • Usuarios registrados

Los registros de diagnóstico se borran todos los días. El usuario no puede cambiar el intervalo de limpieza.

Durante la limpieza de la base de datos, los elementos de Detecciones que corresponden a los registros de incidentes desinfectados también se eliminan (sea cual sea el estado de la detección). De forma predeterminada, el periodo de limpieza de registros de incidentes (y detecciones) está establecido en 6 meses. Puede cambiar el intervalo en **Más** > Configuración.

Personalización

Personalizar interfaz de usuario: puede agregar un logotipo personalizado a ESET PROTECT Web Console, a los informes generados mediante la tarea del servidor y a las notificaciones por correo electrónico.

	Web Console	Informes	Notificaciones
Ninguno	Diseño básico, sin logotipo personalizado	Logotipo de ESET PROTECT On-Prem colocado en el lado izquierdo del pie de página.	Logotipo de ESET PROTECT On-Prem colocado en el lado izquierdo del encabezado de la página.
Personalización de marca conjunta	Logotipo personalizado para Web Console	Un logotipo personalizado en el pie de página del informe: el logotipo de ESET PROTECT On-Prem se coloca a la izquierda y su logotipo a la derecha.	Un logotipo personalizado en el encabezado de la notificación: el logotipo de ESET PROTECT On-Prem se coloca a la izquierda y su logotipo a la derecha.

	Web Console	Informes	Notificaciones
Etiquetado en blanco (requiere licencia MSP)	Logotipo personalizado para Web Console	Un logotipo personalizado en el pie de página del informe: sin logotipo de ESET PROTECT On-Prem, solo su logotipo a la izquierda.	Un logotipo personalizado en el encabezado de la notificación, en el lado izquierdo. Junto a él aparece **Con tecnología de ESET PROTECT On-Prem**.

Logotipo de la empresa

- **Logotipo con fondo oscuro** (encabezado de Web Console)- Este logotipo aparecerá en la esquina superior izquierda de Web Console.

- **Logotipo con fondo claro**: este logotipo aparecerá en el encabezado (para propietarios de licencia MSP) o en el pie de página (ajuste Personalización de marca conjunta) de los informes generados mediante la tarea del servidor y en el encabezado de las notificaciones por correo electrónico.

Haga clic en  para seleccionar un logotipo. Haga clic en para descargar el logotipo actual. Haga clic en para quitar el logotipo actual.

Informes y notificaciones

- **Personalizar informes**: active esta opción para usar el logotipo seleccionado en los informes o para agregar un texto de pie de página.

- **Texto del pie de página del informe**: escriba el texto que se agregará a la esquina inferior derecha de los informes generados en formato PDF.

No puede utilizarse un logotipo personalizado junto con texto de pie de página personalizado. El logotipo tiene la misma posición que el texto del pie de página. Si se utilizan simultáneamente el logotipo y el pie de página, solo será visible el logotipo. Si se utiliza el ajuste **Etiquetado en blanco**, el logotipo personalizado aparecerá en la esquina superior izquierda del informe; se colocará un logotipo de **ESET** de menor tamaño en la esquina inferior derecha en vez del texto del pie de página.

Seguridad avanzada

La seguridad avanzada incluye una comunicación de red segura entre los componentes de ESET PROTECT:

- Las autoridades certificadoras y los certificados utilizan SHA-256 (en lugar de SHA-1).

- El servidor de ESET PROTECT utiliza la máxima seguridad posible (TLS 1.3 o 1.2) para la comunicación con los agentes, Syslog y SMTP.

- Usuarios de MDM: ESET PROTECT Server utiliza 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 – Se recomienda **usar la versión más reciente de OpenSSL1.1.1**. ESET Management Agent es compatible con OpenSSL 3.x. La versión mínima compatible de OpenSSL para Linux es openssl-1.0.1e-30.

Puede haber más versiones de OpenSSL instaladas en un sistema a la vez. En su sistema debe haber al menos una versión compatible.

- Use el comando `openssl version` para mostrar la versión predeterminada actual.
- Puede enumerar todas las versiones de OpenSSL presentes en su sistema. Vea las extensiones de nombre de archivo con el comando `sudo find / -iname *libcrypto.so*`
- Puede comprobar si su cliente Linux es compatible utilizando el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`

- macOS

La seguridad avanzada está habilitada de forma predeterminada.

Servidor SMTP

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

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

No puede usar una cuenta de correo electrónico de Google como servidor 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 ordenadores encontrados

Si existen varias instancias del mismo ordenador en ESET PROTECT On-Prem (por ejemplo, si se vuelve a instalar ESET Management Agent en un ordenador cliente ya administrado), la función **Emparejar automáticamente los ordenadores encontrados** se ocupará de esto y emparejará estas instancias en una sola. Eso debería eliminar la necesidad de verificar y clasificar manualmente los ordenadores encontrados.

El emparejado actúa en el nombre de host del que informa ESET Management Agent y, si no puede confiarse en él, le recomendamos que desactive **Emparejar automáticamente los ordenadores encontrados**. Si el emparejado falla, el ordenador se colocará en el grupo **Perdidos y encontrados**. La idea es que, si ESET Management Agent se vuelve a instalar en un ordenador ya administrado, se empareje de forma automática y se coloque correctamente en ESET PROTECT On-Prem sin que usted tenga que intervenir. Además, el nuevo ESET Management Agent obtendrá inmediatamente sus políticas y tareas.

- Si esta opción está **desactivada**, los ordenadores que deberían colocarse en el grupo **Perdidos y encontrados** se emparejarán con el primer ordenador no administrado que se encuentre (marcador de posición, icono de círculo) en cualquier lugar del árbol de ESET PROTECT On-Prem. Si no hay ningún marcador de posición con el mismo nombre, el ordenador se colocará en Perdidos y encontrados.

- Si esta opción está **activada (valor predeterminado)**, los ordenadores que deberían colocarse en **Perdidos y encontrados** se emparejarán con el primer ordenador no administrado que se encuentre (marcador de posición, icono de círculo) en cualquier lugar del árbol de ESET PROTECT On-Prem. Si no hay ningún marcador de posición con el mismo nombre, el ordenador se emparejará con el primer ordenador administrado que se encuentre (alerta o icono de marca de verificación) en cualquier lugar del árbol de ESET PROTECT On-Prem. Si este emparejamiento también falla, el ordenador se colocará en Perdidos y encontrados.

Si no desea que se produzcan emparejamientos automáticos, desactive esta opción. Siempre podrá verificar y ordenar los ordenadores manualmente.

Exportar registros a Syslog

ESET PROTECT On-Prem puede exportar determinados registros/eventos y enviarlos a su servidor de Syslog. Eventos de las siguientes categorías de registro se exportarán al servidor de Syslog: Detección, Cortafuegos, HIPS, Auditoría y ESET Inspect. Los eventos se generan en cualquier ordenador cliente administrado en el que se ejecute un producto de ESET (por ejemplo, ESET Endpoint Security). Estos eventos se pueden procesar mediante cualquier solución de Gestión de eventos e información de seguridad (SIEM) capaz de importar los eventos desde un servidor de Syslog. Los eventos se escriben en el servidor de Syslog mediante ESET PROTECT On-Prem.

1. Para activar el servidor de Syslog, haga clic en **Más** > **Configuración** > **Configuración avanzada** > **Servidor de Syslog** > **Usar servidor de Syslog**.

2. Para activar la exportación, haga clic en **Más** > **Configuración** > **Configuración avanzada** > **Registro** >

Exportar registros a Syslog.

Todos los registros exportados están disponibles para los usuarios de Syslog sin limitaciones. Todos los mensajes del registro de auditoría se exportan a Syslog.

3. Elija uno de los siguientes formatos para los mensajes de eventos:

- JSON (JavaScript Object Notation)
- LEEF (Log Event Extended Format): formato utilizado por la aplicación de IBM Qradar.
- CEF (formato de evento común)

Para filtrar los registros de sucesos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.

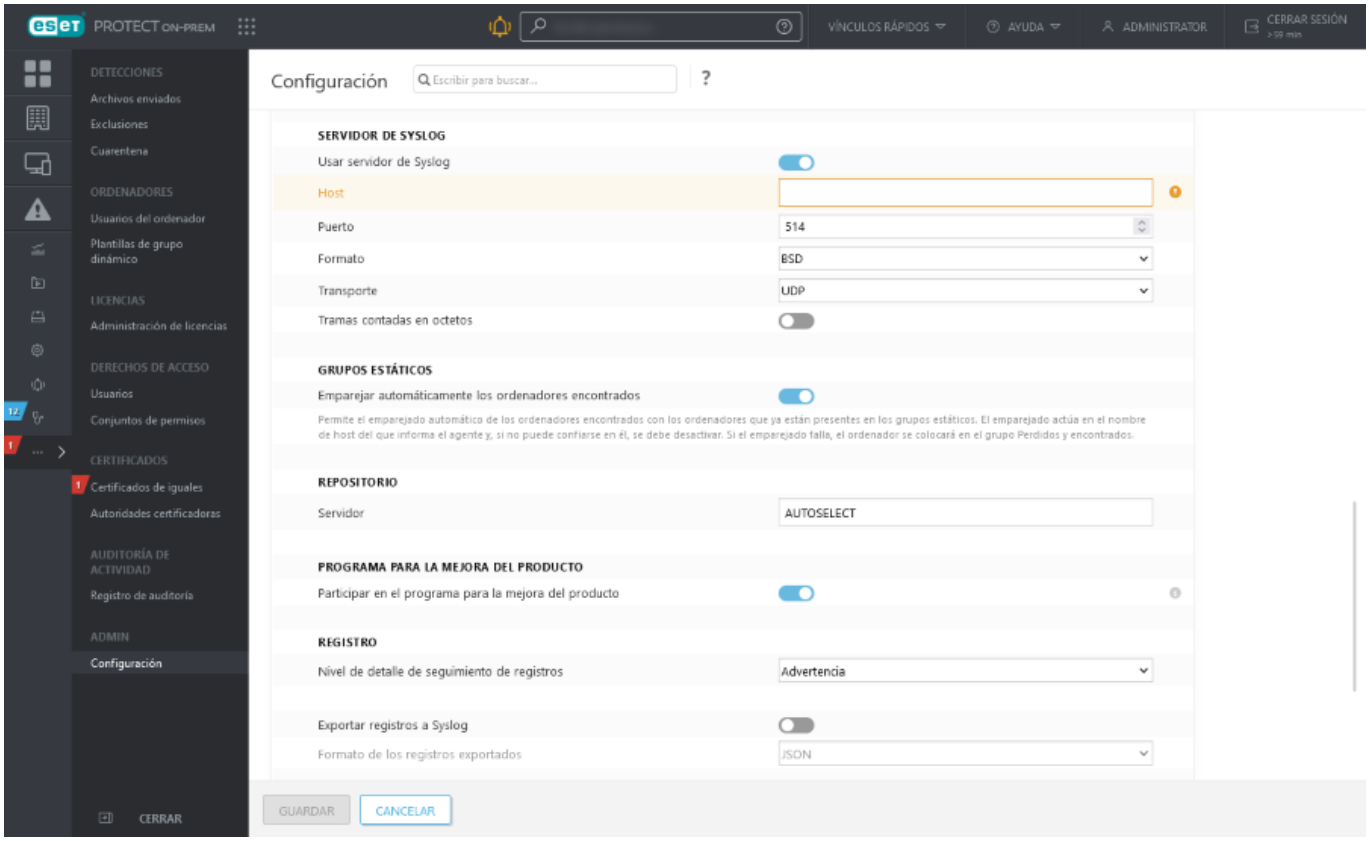
Servidor de Syslog

Si tiene un servidor de Syslog ejecutándose en su red, puede Exportar registros a Syslog para recibir determinados sucesos (Suceso de detección, Suceso de adición al cortafuegos, Suceso de adición al HIPS, etc.) desde ordenadores cliente en los que se ejecute ESET Endpoint Security. Puede configurar ESET PROTECT Server para que envíe notificaciones a su servidor de Syslog.

Para activar el servidor de Syslog:

1. Vaya a **Más** > **Configuración** > **Configuración avanzada** > **Servidor de Syslog** y haga clic en el conmutador de alternancia situado junto a **Usar servidor de Syslog**.
2. Especifique los siguientes ajustes obligatorios:
   a. **Host** (dirección IP o nombre de host del destino de los mensajes de Syslog)
   b. Número de **Puerto** (el valor predeterminado es 514).
   c. **Formato** del registro: **BSD** (especificación), **Syslog** (especificación)
   d. Protocolo de **Transport** para enviar mensajes a Syslog (**UDP**, **TCP**, **TLS**)
3. Desplácese hacia abajo hasta **Registro** y active el interruptor **Exportar registros a Syslog**.

Tras realizar cambios, haga clic en **Guardar**.



constantemente se escriben archivos de registro de las aplicaciones. Syslog actúa únicamente como medio con el que exportar determinados sucesos asíncronos, como notificaciones o diversos eventos del ordenador cliente.

Eventos exportados a formato JSON

JSON en un formato ligero para el intercambio de datos. Se basa en la recopilación de pares de nombre/valor y una lista ordenada de valores.

Eventos exportados

Esta sección contiene detalles sobre el formato y el significado de los atributos de todos los eventos exportados. El mensaje del evento presenta el formato de un objeto JSON con algunas claves obligatorias y otras opcionales. Cada evento exportado contendrá la siguiente clave:

event_type	cadena		Tipo de eventos exportados: • Threat_Event (detecciones de **Antivirus**) • FirewallAggregated_Event (detecciones de **Cortafuegos**) • HipsAggregated_Event (detecciones de **HIPS**) • Audit_Event (registro de auditoría) • FilteredWebsites_Event web (sitios web filtrados: **protección web**) • EnterpriseInspectorAlert_Event (alertas de ESET Inspect) • BlockedFiles_Event (archivos bloqueados)
ipv4	cadena	opcional	Dirección IPv4 del ordenador que genera el evento.
ipv6	cadena	opcional	Dirección IPv6 del ordenador que genera el evento.
hostname	cadena		Nombre de host del ordenador que genera el evento.

event_type	cadena		Tipo de eventos exportados: • Threat_Event (detecciones de **Antivirus**) • FirewallAggregated_Event (detecciones de **Cortafuegos**) • HipsAggregated_Event (detecciones de **HIPS**) • Audit_Event (registro de auditoría) • FilteredWebsites_Event web (sitios web filtrados: **protección web**) • EnterpriseInspectorAlert_Event (alertas de ESET Inspect) • BlockedFiles_Event (archivos bloqueados)
source_uuid	cadena		UUID del ordenador que genera el evento.
occurred	cadena		Hora UTC en la que el evento tuvo lugar. Tiene el formato %d-%b-%Y %H:%M:%S
severity	cadena		Gravedad del evento. Los posibles valores (de menos grave a más grave) son: `Información`, `Aviso`, `Advertencia`, `Error`, `Crítico` y `Fatal`.
group_name	cadena		La ruta completa al grupo estático del ordenador que genera el evento. Si la ruta de acceso tiene más de 255 caracteres, group_name solo contiene el nombre del grupo estático.
group_description	cadena		Descripción del grupo estático.
os_name	cadena		Información sobre el sistema operativo del ordenador.

Todos los tipos de sucesos indicados a continuación con todos los niveles de gravedad se registran en el servidor de Syslog. Para filtrar los registros de sucesos 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) que se haya instalado en el ordenador administrado, y ESET PROTECT On-Prem solo informa de los datos recibidos. Por lo tanto, ESET no puede proporcionar una lista exhaustiva de todos los valores. Le recomendamos que compruebe su red y filtre los registros en función de los valores recibidos.

Claves personalizadas según event_type:

Threat_Event

Todos los eventos de detección de **Antivirus** generados por equipos administrados se reenviarán a Syslog. Clave específica del evento de detección:

threat_type	cadena	opcional	Tipo de detección
threat_name	cadena	opcional	Nombre de la detección
threat_flags	cadena	opcional	Marcadores relacionados con la detección
scanner_id	cadena	opcional	ID del escáner
scan_id	cadena	opcional	ID del análisis
engine_version	cadena	opcional	Versión del motor de análisis
object_type	cadena	opcional	Tipo de objeto relacionado con este evento
object_uri	cadena	opcional	URL del objeto
action_taken	cadena	opcional	Acción realizada por el punto de acceso
action_error	cadena	opcional	Mensaje de error si la "acción" no se ha realizado correctamente
threat_handled	bool	opcional	Indica si la detección se gestionó o no
need_restart	bool	opcional	Indica si es necesario reiniciar o no

threat_type	cadena	opcional	Tipo de detección
username	cadena	opcional	Nombre de la cuenta de usuario relacionada con el evento
processname	cadena	opcional	Nombre del proceso relacionado con el evento
circumstances	cadena	opcional	Breve descripción de la causa del evento
hash	cadena	opcional	Hash SHA1 de la secuencia de datos (detección).
firstseen	cadena	opcional	Hora y fecha en las que se detectó la detección por primera vez en ese equipo. ESET PROTECT On-Prem utiliza diferentes formatos de fecha y hora para el atributo firstseen (y para cualquier otro atributo de fecha y 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 el cortafuegos de ESET (detecciones de **Cortafuegos**) los agrega la instancia de ESET Management Agent que administra para no desperdiciar ancho de banda durante la replicación de ESET Management Agent/ESET PROTECT Server. Clave específica del evento de cortafuegos:

event	cadena	opcional	Nombre del evento
source_address	cadena	opcional	Dirección del origen del evento
source_address_type	cadena	opcional	Tipo de dirección del origen del evento
source_port	número	opcional	Puerto del origen del evento
target_address	cadena	opcional	Dirección del destino del evento
target_address_type	cadena	opcional	Tipo de dirección del destino del evento
target_port	número	opcional	Puerto del destino del evento
protocol	cadena	opcional	Protocolo
account	cadena	opcional	Nombre de la cuenta de usuario relacionada con el evento
process_name	cadena	opcional	Nombre del proceso relacionado con el evento
rule_name	cadena	opcional	Nombre de la regla
rule_id	cadena	opcional	ID de la regla
inbound	bool	opcional	Indica si la conexión fue entrante o no
threat_name	cadena	opcional	Nombre de la detección
aggregate_count	número	opcional	El número de los mensajes exactamente iguales generados por el punto de acceso entre dos replicaciones consecutivas entre el ESET PROTECT Server y el ESET Management Agent encargado de la gestión.
action	cadena	opcional	Acción realizada
handled	cadena	opcional	Indica si la detección se gestionó 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 de HIPS (detecciones de **HIPS**) se filtran por **Gravedad** antes de enviarse de nuevo como mensajes de Syslog. Los atributos específicos del HIPS son los siguientes:

application	cadena	opcional	Nombre de la aplicación
operation	cadena	opcional	Operación
target	cadena	opcional	Destino
action	cadena	opcional	Acción realizada
action_taken	cadena	opcional	Acción realizada por el punto de acceso
rule_name	cadena	opcional	Nombre de la regla
rule_id	cadena	opcional	ID de la regla
aggregate_count	número	opcional	El número de los mensajes exactamente iguales generados por el punto de acceso entre dos replicaciones consecutivas entre el ESET PROTECT Server y el ESET Management Agent encargado de la gestión.

application	cadena	opcional	Nombre de la aplicación
handled	cadena	opcional	Indica si la detección se gestionó 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 reenvía los mensajes del registro de auditoría interno a Syslog. Los atributos específicos son los siguientes:

domain	cadena	opcional	Dominio del registro de auditoría
action	cadena	opcional	Acción que se está realizando
target	cadena	opcional	Destino en el que se está realizando la acción
detail	cadena	opcional	Descripción detallada de la acción
user	cadena	opcional	Usuario de seguridad implicado

domain	cadena	opcional	Dominio del registro de auditoría
result	cadena	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	cadena	opcional	Nombre del proceso relacionado con el evento
username	cadena	opcional	Nombre de la cuenta de usuario relacionada con el evento
hash	cadena	opcional	Hash SHA1 del objeto filtrado
event	cadena	opcional	Tipo de suceso
rule_id	cadena	opcional	ID de la regla
action_taken	cadena	opcional	Acción realizada
scanner_id	cadena	opcional	ID del escáner
object_uri	cadena	opcional	URL del objeto

target_address	cadena	opcional	Dirección del destino del evento
target_address_type	cadena	opcional	Tipo de dirección del destino del evento 25769803777 = IPv4; 25769803778 = IPv6)
handled	cadena	opcional	Indica si la detección se gestionó 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 al Syslog. Los atributos específicos son los siguientes:

processname	cadena	opcional	Nombre del proceso que provoca esta alarma
username	cadena	opcional	Propietario del proceso
rulename	cadena	opcional	Nombre de la regla que activa esta alarma

processname	cadena	opcional	Nombre del proceso que provoca esta alarma
count	número	opcional	Número de alertas de este tipo generadas desde la última alerta
hash	cadena	opcional	Hash SHA1 de la alarma
eiconsolelink	cadena	opcional	Enlace a la alarma en la consola de ESET Inspect On-Prem
eialarmid	cadena	opcional	Subparte del identificador del vínculo de alarma ($1 en ^http.*/alarm/([0-9]+)$)
computer_severity_score	número	opcional	Nivel de gravedad del ordenador
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 los archivos bloqueados por ESET Inspect On-Prem a Syslog. Los atributos específicos son los siguientes:

processname	cadena	opcional	Nombre del proceso relacionado con el evento

username	cadena	opcional	Nombre de la cuenta de usuario relacionada con el evento
hash	cadena	opcional	Hash SHA1 del archivo bloqueado
object_uri	cadena	opcional	URL del objeto
action	cadena	opcional	Acción realizada
firstseen	cadena	opcional	Hora y fecha en las que se detectó por primera vez en ese equipo (formato de fecha y hora).
cause	cadena	opcional	
description	cadena	opcional	Descripción del archivo bloqueado
handled	cadena	opcional	Indica si la detección se gestionó o no

Eventos exportados a formato LEEF

Para filtrar los registros de sucesos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.

El formato LEEF es un formato de eventos personalizado para IBM® Security QRadar®. Los eventos tienen atributos estándar y personalizados:

- ESET PROTECT On-Prem utiliza algunos de los atributos estándar descritos en la documentación oficial de IBM.
- Los atributos personalizados son los mismos que en formato JSON. El atributo deviceGroupName contiene la ruta completa al grupo estático del ordenador que genera el evento. Si la ruta de acceso tiene más de 255 caracteres, deviceGroupName solo contiene el nombre del grupo estático. El atributo deviceOSName contiene información sobre el sistema operativo del ordenador y el atributo deviceGroupDescription contiene la descripción del grupo estático.

Categorías de eventos:

- Detecciones del 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 sucesos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.

CEF es un formato de registro de texto desarrollado por ArcSight™. El CEF formato incluye un encabezado CEF 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
Device Event Class ID (Signature ID):	109	Identificador único de la categoría de evento de dispositivo: • 100–199 evento de amenaza • 200–299 evento de cortafuegos • 300–399 HIPS evento • 400–499 evento de auditoría • 500–599 ESET Inspect evento • 600–699 evento de archivos bloqueados • 700–799 evento de sitios web filtrados
Event Name	Detected port scanning attack	Una breve descripción de lo que ocurrió en el evento
Severity	5	Nivel de registro • 2 – Información • 3 – Aviso • 5 – Advertencia • 7 – Error • 8 – Crítico • 10 – Fatal

Extensiones CEF comunes a 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 ordenador que genera el evento.
c6a1	2001:0db8:85a3:0000:0000:8a2e:0370:7334	Dirección IPv6 del ordenador que genera el evento.

Nombre de la extensión	Ejemplo	Descripción
c6a1Label	Device IPv6 Address	
dvchost	COMPUTER02	Nombre de cliente del ordenador con el suceso
deviceExternalId	39e0feee-45e2-476a-b17f-169b592c3645	UUID del ordenador que genera el evento.
rt	Jun 04 2017 14:10:0	Hora UTC en la que el evento tuvo lugar. El formato es %b %d %Y %H:%M:%S
ESETProtectDeviceGroupName	All/Lost & found	La ruta completa al grupo estático del ordenador que genera el evento. Si la ruta de acceso tiene más de 255 caracteres, ESETProtectDeviceGroupName solo contiene el nombre del grupo estático.
ESETProtectDeviceOsName	Microsoft Windows 11 Pro	Información sobre el sistema operativo del ordenador.
ESETProtectDeviceGroupDescription	Lost & found static group	Descripción del grupo estático.

Extensiones CEF por categoría de evento

Eventos 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 del escáner
cs4Label	Scanner ID	
cs5	virlog.dat	ID del análisis
cs5Label	Scan ID	
cs6	Failed to remove file	Mensaje de error si la "acción" no se ha realizado correctamente
cs6Label	Action Error	

Nombre de la extensión	Ejemplo	Descripción
cs7	Event occurred on a newly created file	Breve descripción de la causa del evento
cs7Label	Circumstances	
cs8	0000000000000000000000000000000000000000	Hash SHA1 de la secuencia de datos (detección).
cs8Label	Hash	
act	Cleaned by deleting file	La acción la realizó el equipo
filePath	file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC	Objeto URI
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	Reiniciar es necesario (1) o no es necesario (0)
cn2Label	Restart Needed	
suser	172-MG\\Administrator	Nombre de la cuenta de usuario relacionada 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 el equipo. El formato es %b %d %Y %H:%M:%S

Ejemplo de registro de CEF de evento de amenaza:

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 cortafuegos

Nombre de la extensión	Ejemplo	Descripción
msg	TCP Port Scanning attack	Nombre del evento
src	127.0.0.1	Dirección IPv4 del origen del evento
c6a2	2001:0db8:85a3:0000:0000:8a2e:0370:7334	Dirección IPv6 del origen del evento
c6a2Label	Source IPv6 Address	
spt	36324	Puerto del origen del evento
dst	127.0.0.2	Dirección IPv4 del destino del evento
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	Dirección IPv6 del destino del evento
c6a3Label	Destination IPv6 Address	
dpt	24	Puerto de destino del evento
proto	http	Protocolo
act	Blocked	Acción realizada
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
suser	172-MG\\Administrator	Nombre de la cuenta de usuario relacionada con el evento
deviceProcessName	someApp.exe	Nombre del proceso relacionado con el evento
deviceDirection	1	La conexión era entrante (0) o saliente (1)
cnt	3	El número de los mismos mensajes generados por el equipo entre dos replicaciones consecutivas entre ESET PROTECT On-Prem y ESET Management Agent
cs1		ID de la regla
cs1Label	Rule ID	
cs2	custom_rule_12	Nombre de la regla
cs2Label	Rule Name	
cs3	Win32/Botnet.generic	Nombre de la amenaza
cs3Label	Threat Name	

Ejemplo de registro de CEF de evento del cortafuegos:

```
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 la 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	Acción realizada
cs2	custom_rule_12	Nombre de la 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 equipo entre dos replicaciones consecutivas entre ESET PROTECT On-Prem y ESET Management Agent

Ejemplo de registro de CEF de evento 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 está realizando

Nombre de la extensión	Ejemplo	Descripción
suser	Administrator	Usuario de seguridad implicado
duser	Administrator	Usuario de seguridad objetivo (por ejemplo, para intentos de inicio de sesión)
msg	Authenticating native user 'Administrator'	Descripción detallada de la acción
cs1	Native user	Dominio del registro de auditoría
cs1Label	Audit Domain	
cs2	Success	Resultado de la acción
cs2Label	Result	

Ejemplo de registro de CEF de evento 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 provoca esta alarma
suser	HP\\home	Propietario del proceso
cs2	custom_rule_12	Nombre de la regla que activa esta alarma
cs2Label	Rule Name	
cs3	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	Hash SHA1 de alarma
cs3Label	Hash	
cs4	https://inspect.eset.com:443/console/alarm/126	Vínculo a la alarma en ESET Inspect On-Prem Web Console
cs4Label	EI Console Link	
cs5	126	Subparte del identificador del vínculo de alarma ($1 en ^http.*/alarm/([0-9]+)$)
cs5Label	EI Alarm ID	
cn1	275	Nivel de gravedad del ordenador
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 de registro de CEF de evento de 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 en archivos bloqueados

Nombre de la extensión	Ejemplo	Descripción
act	Execution blocked	Acción realizada
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
suser	HP\\home	Nombre de la cuenta de usuario relacionada con el evento
deviceProcessName	C:\\Windows\\explorer.exe	Nombre del proceso relacionado con el 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 el equipo. El formato es %b %d %Y %H:%M:%S
cs2	Blocked by Administrator	Causa
cs2Label	Cause	

Ejemplo de registro de CEF de evento 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 sitio web filtrados

Nombre de la extensión	Ejemplo	Descripción
msg	An attempt to connect to URL	Tipo de suceso
act	Blocked	Acción realizada
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
suser	Peter	Nombre de la cuenta de usuario relacionada con el evento
deviceProcessName	Firefox	Nombre del proceso relacionado con el evento
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 del destino del evento
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	Dirección IPv6 del destino del evento
c6a3Label	Destination IPv6 Address	
cs2	HTTP filter	ID del escáner
cs2Label	Scanner ID	
cs3	8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5	Hash SHA1 del objeto filtrado
cs3Label	Hash	

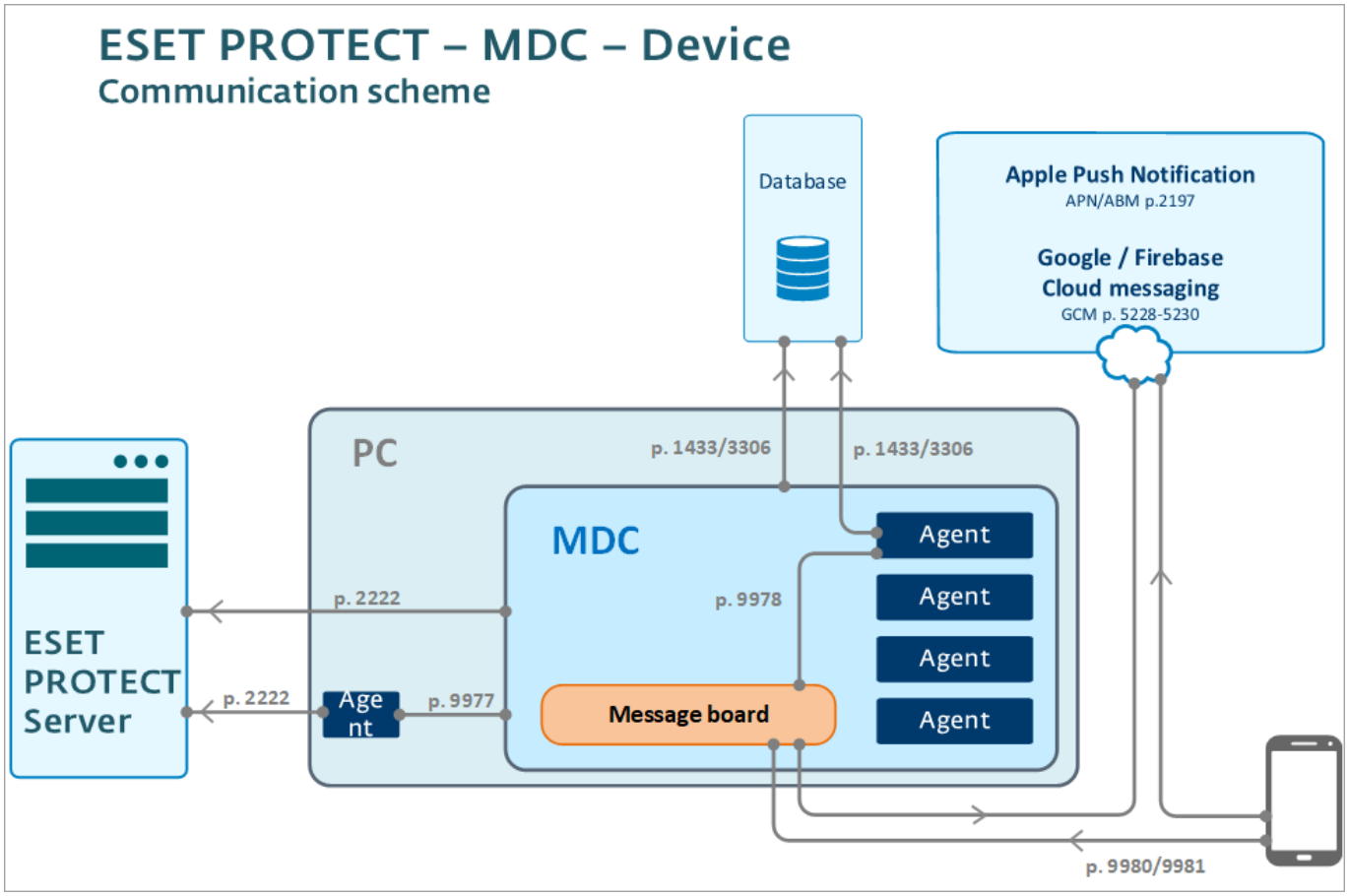
Ejemplo de registro de CEF de evento de sitio web filtrado:

```
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 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) (solo local) llega al fin de la vida útil en enero de 2024. Más información. Le recomendamos migrar a Cloud MDM.

El siguiente diagrama muestra la comunicación entre los componentes de ESET PROTECT y un dispositivo móvil:



Haga clic ver la imagen más grande

Recomendación sobre seguridad para MDM: El dispositivo host de MDM necesita acceso a Internet. Se recomienda que el dispositivo host de MDM esté detrás de un cortafuegos y que solo estén abiertos los puertos necesarios para MDM. También puede implementar un IDS/IPS para supervisar la red en busca de anomalías.

El Conector de dispositivo móvil (MDC) es un componente de ESET PROTECT que permite utilizar la Administración de dispositivos móviles con ESET PROTECT On-Prem, lo que posibilita la administración de dispositivos móviles Android e iOS y la administración de la seguridad móvil.

MDC ofrece una solución sin agente en la que los agentes no se ejecutan directamente en los dispositivos móviles (para ahorrar batería y mejorar el rendimiento del dispositivo móvil). MDC actúa como un host de estos agentes virtuales. MDC almacena datos para y desde dispositivos móviles en su base de datos SQL dedicada.

Es necesario un certificado HTTPS para autenticar la comunicación entre el dispositivo móvil y MDC. Para autenticar la comunicación entre ESET PROTECT Server y MDC, se utiliza un certificado de proxy.

La administración de dispositivos Apple tiene algunos requisitos adicionales. Es necesario un certificado de Apple Push Notification Service para utilizar ESET PROTECT MDC con el fin de administrar dispositivos iOS. El servicio APN permite que ESET MDC se comunique de forma segura con dispositivos móviles Apple. Apple debe firmar directamente este certificado (con el Portal de certificados push de Apple) y enviarlo a MDC a través de una política. Posteriormente, los dispositivos iOS podrían inscribirse en ESET PROTECT MDC.

En ciertos países, Apple Business Manager (ABM) está disponible. ABM es un nuevo y potente método de inscripción de dispositivos iOS corporativos. Con ABM puede inscribir dispositivos automáticamente en MDC sin

contacto directo con el dispositivo y también con una interacción mínima del usuario. ABM amplía considerablemente las prestaciones de iOS MDM y permite la personalización completa de la configuración del dispositivo.

Después de realizar correctamente la instalación y configuración del Conector de dispositivo móvil, se podrán inscribir los dispositivos móviles. Después de realizar la inscripción correctamente, el dispositivo móvil puede administrarse desde la Consola web de ESET PROTECT.

Configuración y ajustes de MDM

El componente ESET PROTECT Mobile Device Management/Connector (MDM/MDC) (solo local) llega al fin de la vida útil en enero de 2024. Más información. Le recomendamos migrar a Cloud MDM.

Para aprovechar el componente 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 del dispositivo móvil** (MDC) utilizando el Instalador todo en uno o ejecute la instalación de componentes para Windows o Linux. También puede implementar MDM como un dispositivo virtual. Asegúrese de haber cumplido con los requisitos previos antes de la instalación.

Si está instalando MDC utilizando el instalador todo en uno, el certificado HTTPS firmado por la autoridad certificadora de ESET PROTECT On-Prem se genera automáticamente durante el proceso. El certificado está protegido por contraseña (con una contraseña generada de forma aleatoria) y el certificado no es visible desde **Más** > **Certificados de igual**.
Si desea instalar ESET PROTECT On-Prem con el instalador todo en uno y utilizar un certificado HTTPS de terceros, instale ESET PROTECT On-Prem primero y, a continuación, cambie su certificado HTTPS con una política (en **Política del Conector de dispositivo móvil de ESET** > **General** > **Cambiar certificado** > **Certificado personalizado**).
Si instala el componente MDC por sí mismo, puede utilizar lo siguiente:
a) certificado firmado por la autoridad certificadora de ESET PROTECT On-Prem (**Básico** > **Producto**: Conector del dispositivo móvil**Host**: nombre del host/dirección IP del MDC; **Firmar** > **Método de firma**: Autoridad certificadora; **Autoridad certificadora**: ESET PROTECT Autoridad certificadora
b) cadena de certificados HTTPS de un tercero firmados por una CA que cuente con la confianza de Apple (lista de CA en las que confía Apple).

2. Active ESET PROTECT MDC con la tarea del cliente Activación del producto. El procedimiento es el mismo que al activar un producto de seguridad de ESET en un ordenador cliente (no se utilizará una unidad de licencia).

3. Ejecute una tarea del servidor Sincronización de usuarios (recomendado). Esto le permite sincronizar automáticamente los usuarios con Active Directory o LDAP a efectos de los usuarios del ordenador.

Si tiene previsto gestionar exclusivamente dispositivos **Android** (no va a gestionar dispositivos iOS), puede avanzar al paso 7.

4. Cree un certificado de APN/ABM. ESET PROTECT MDM utiliza este certificado para la inscripción de dispositivos iOS. Los certificados que se agreguen a su perfil de inscripción también deben agregarse a su perfil de ABM.

5. Cree una nueva directiva para el Conector del dispositivo móvil de ESET para activar APNS.

Siga estas instrucciones para inscribir un dispositivo iOS con Apple Business Manager (ABM).

6. Inscriba los dispositivos móviles utilizando una tarea de Inscripción de dispositivo. Configure la tarea para inscribir dispositivos para Android o iOS. Esto también puede hacerse desde la ficha **Ordenadores** o **Grupos** haciendo clic en **Agregar nuevo** > **Dispositivos móviles** teniendo seleccionado un **Grupo estático** (**Agregar nuevo** no se puede utilizar en grupos dinámicos).

7. Si no ha indicado una licencia durante la inscripción del dispositivo, active los dispositivos móviles utilizando una tarea del cliente Activación del producto: elija una licencia de ESET Endpoint Security. Se utilizará una unidad de licencia para cada dispositivo móvil.

La tarea **Activación del producto** puede activar un producto móvil, ESET Endpoint para Android, también 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 utilizar 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 ha asignado usuarios durante la inscripción del dispositivo.

9. Ahora ya puede empezar a aplicar directivas y a gestionar los dispositivos móviles. Por ejemplo, Crear una directiva para el MDM de iOS: cuenta de Exchange ActiveSync, que configurará automáticamente su cuenta de correo, sus contactos y su calendario en los dispositivos iOS. También puede aplicar restricciones en un dispositivo iOS o agregar una conexión Wi-Fi.

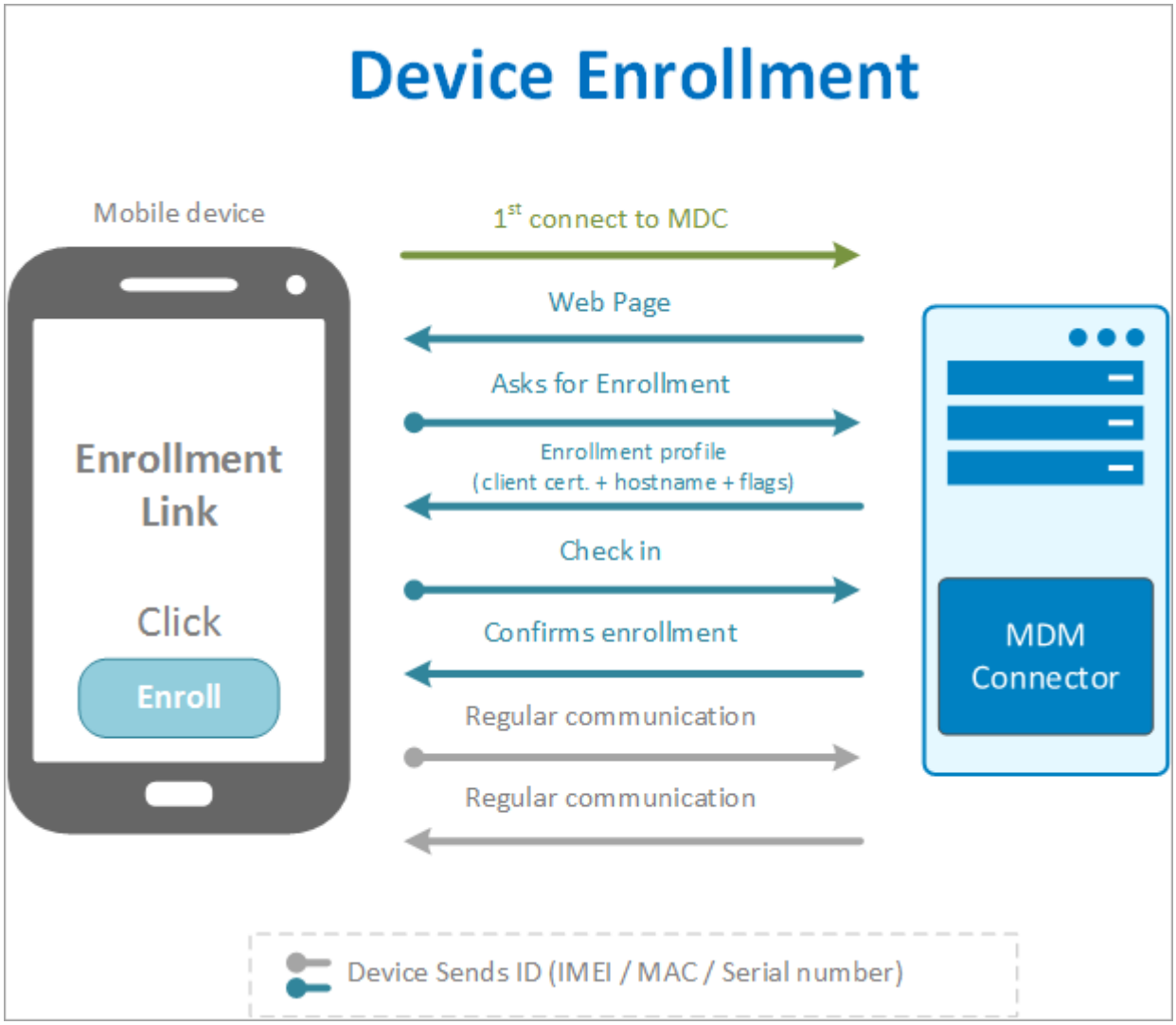
Resolución de problemas

- Puede utilizar **Inscribir de nuevo** en un dispositivo móvil dañado o borrado. El vínculo para inscribirlo de nuevo se enviará por correo electrónico.
- La tarea Detener administración (desinstalar ESET Management Agent) cancelará la inscripción en MDM de un dispositivo móvil y lo quitará de ESET PROTECT On-Prem.
- Para actualizar MDC, utilice la tarea Actualización de componentes de ESET PROTECT.
- Consulte también Resolución de problemas de MDM

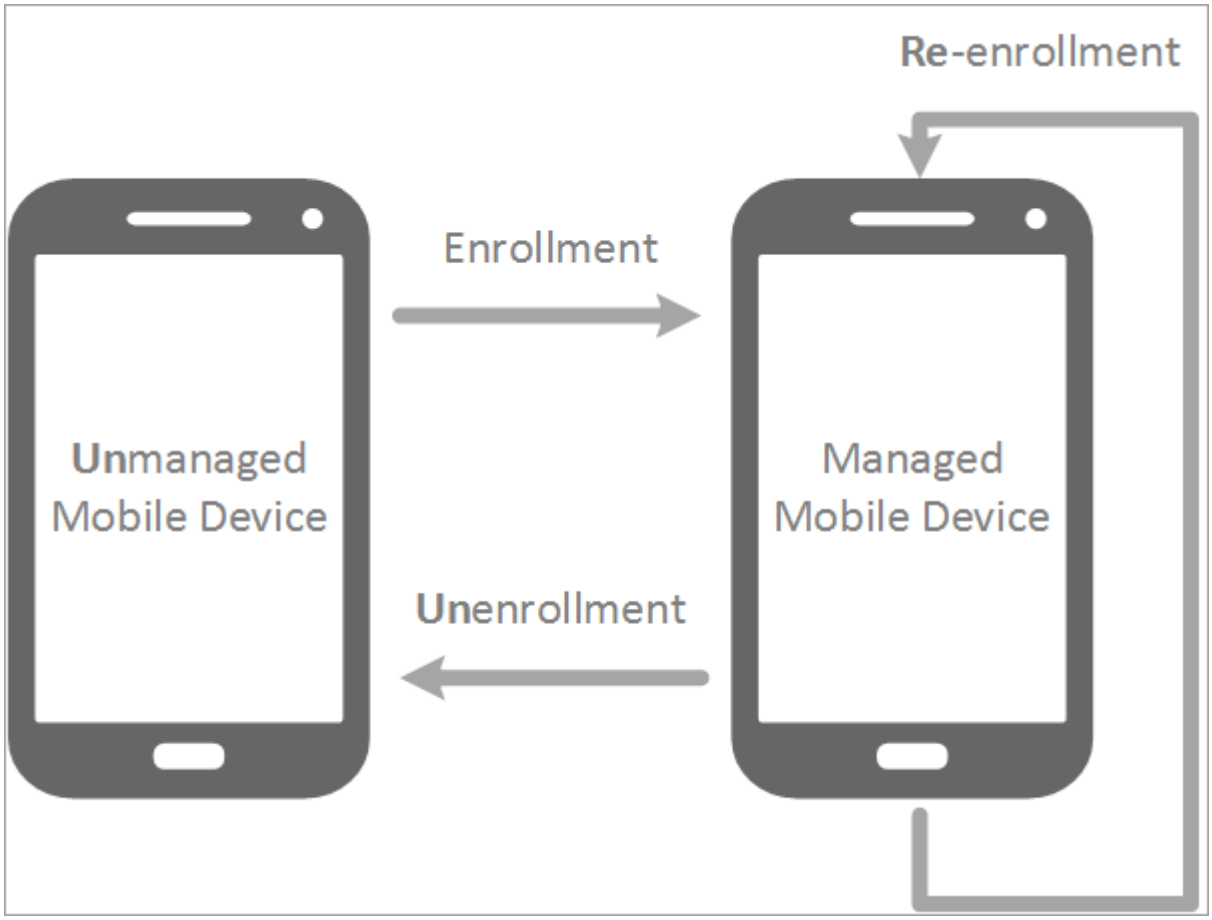
Inscripción de dispositivo

Los dispositivos móviles pueden administrarse a través de ESET PROTECT On-Prem y un producto de seguridad de ESET en ejecución en el dispositivo móvil. Para empezar a administrar dispositivos móviles tendrá que inscribirlos en ESET PROTECT On-Prem (ya no es necesario introducir el IMEI ni otros números de identificación en el dispositivo móvil).

En el diagrama que aparece a continuación se muestra cómo el dispositivo móvil se comunica con el Conector del dispositivo móvil durante el proceso de inscripción:



En este diagrama se explica cuándo se pueden utilizar la inscripción, la repetición de la inscripción y la cancelación de la inscripción, así como la diferencia entre dispositivos administrados y no administrados.



- **Inscripción**: la inscripción solo puede utilizarse cuando MDM no administra el dispositivo. En este caso, el dispositivo no existe en la sección **Ordenadores**. Eliminar un dispositivo de la Consola web no lo convierte en un dispositivo no administrado, por lo que dicho dispositivo aparecerá en la Consola web tras realizar correctamente una replicación. El estado administrado de un dispositivo solo se puede cancelar mediante el proceso de anulación de inscripción. Cada token de inscripción es único y de un solo uso. Una vez utilizado, el token no puede volver a utilizarse.

- **Repetición de la inscripción**: La repetición de la inscripción solo puede utilizarse si el dispositivo es un dispositivo administrado. El token de repetición de la inscripción es siempre diferente del token de inscripción y, como él, solo puede utilizarse una vez.
Para repetir la inscripción de un dispositivo, abra la sección **Ordenadores** y seleccione el dispositivo móvil cuya inscripción quiera repetir. Abra el menú **Ordenador** y seleccione **Móvil > Inscribir de nuevo**.

- **Cancelación de la inscripción**: Cancelar la inscripción es la forma correcta de dejar de administrar un dispositivo. La cancelación de la inscripción se realiza utilizando la tarea del cliente Detener administración. Si el dispositivo no responde, pueden transcurrir hasta 3 días hasta que el dispositivo se quite. Si solo quiere quitar el dispositivo para inscribirlo de nuevo, utilice la repetición de la inscripción.

> Siga estas instrucciones para inscribir un dispositivo iOS con Apple Business Manager (ABM).

Puede inscribir dispositivos móviles en la sección **Ordenadores** o en Más > Grupos. Seleccione el **Grupo estático** al que desee agregar los dispositivos móviles, haga clic en **Agregar dispositivo** > **Dispositivos móviles** y, a continuación, seleccione uno de los siguientes métodos de inscripción:

- **Android o iOS/iPadOS**: hay dos métodos de inscripción.

  - Enviar correo electrónico – Inscripción en masa de dispositivos móviles por correo electrónico. Esta

opción es la mejor si debe inscribir un gran número de dispositivos móviles o si cuenta con dispositivos móviles a los que no tiene acceso físico. Para utilizar esta opción se necesita participación activa del usuario o propietario del dispositivo móvil.

oEscanear código QR: inscripción de un solo dispositivo móvil. Podrá inscribir un dispositivo móvil cada vez, y tendrá que repetir el proceso con cada dispositivo. Solo le recomendamos que utilice esta opción si tiene que inscribir pocos dispositivos móviles. Esta opción es adecuada si no quiere que los usuarios/propietarios de los dispositivos móviles hagan nada, y desea realizar todas las tareas de inscripción usted mismo. Además, puede utilizar esta opción si tiene nuevos dispositivos móviles que se entregarán a los usuarios cuando estén completamente configurados.

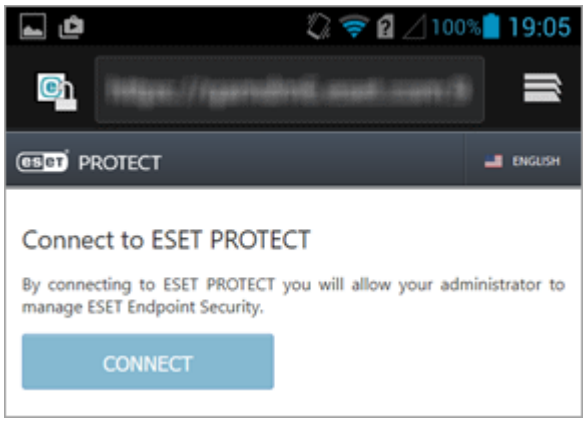
- **Inscripción individual como propietario del dispositivo (solo Android 7 y posteriores)**: inscripción de un solo dispositivo móvil únicamente para dispositivos Android. Podrá inscribir un dispositivo móvil cada vez, y tendrá que repetir el proceso con cada dispositivo móvil. El proceso de inscripción solo es posible en dispositivos móviles nuevos (recién sacados de la caja) o tras un borrado o restablecimiento de la configuración predeterminada. Este proceso de inscripción proporcionará más derechos de administración al administrador que al usuario del dispositivo móvil.

Inscripción de dispositivo Android

Cuando ESET Endpoint Security para Android (EESA) se encuentra activado en el dispositivo móvil existen dos contextos de inscripción. Puede activar EESA en el dispositivo móvil por medio de la tarea Activación del producto (opción recomendada). El otro contexto es el de dispositivos móviles en los que la aplicación ESET Endpoint Security para Android ya se encuentra activada.

EESA ya está activado: siga los pasos indicados a continuación para inscribir su dispositivo:

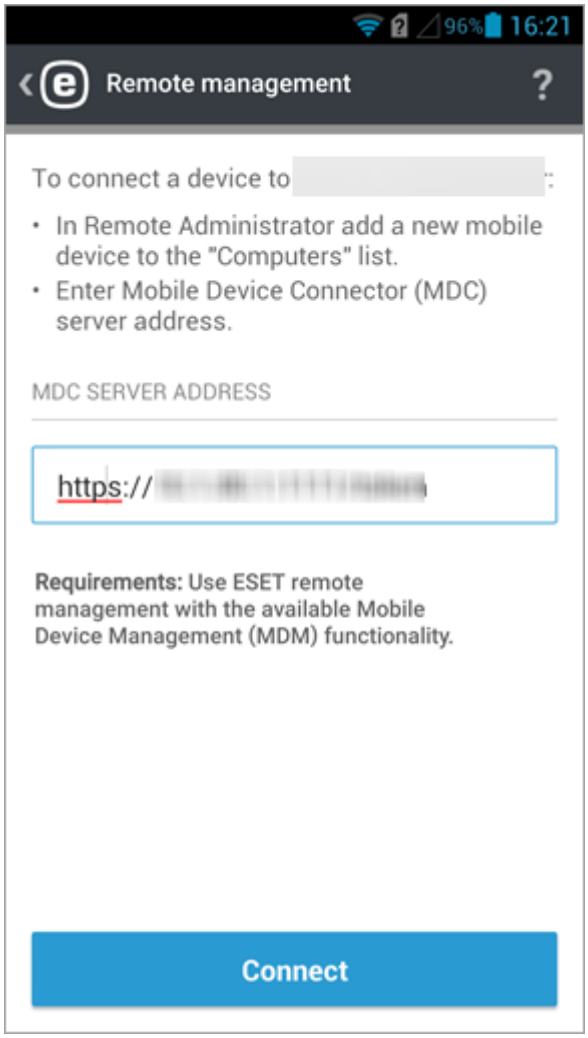
1. Pulse la URL del vínculo de inscripción (incluido el número de puerto) recibida por correo electrónico o escríbala en el navegador manualmente (por ejemplo, *https://eramdm:9980/<token>*). Puede que se le pida que acepte un certificado SSL: haga clic en **Aceptar** si está de acuerdo y, a continuación, haga clic en **Conectar**.



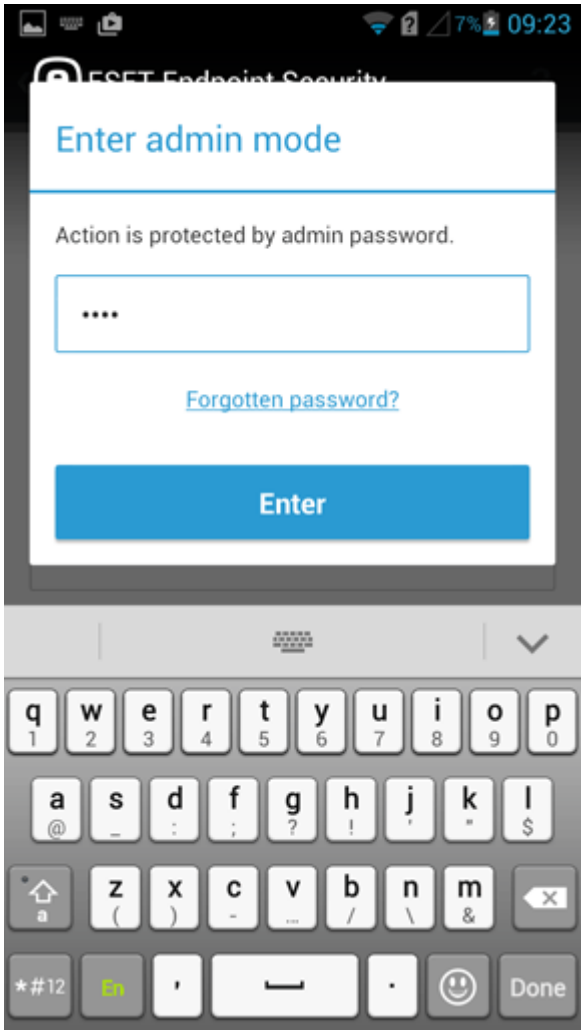
Si no tiene ESET Endpoint Security instalado en el dispositivo móvil, se le redirigirá automáticamente a Google Play para que descargue la aplicación.

Si se muestra la notificación **No se encontró ninguna aplicación para abrir este vínculo**, intente abrir el vínculo de inscripción en el navegador web predeterminado de Android.

2. Revise los datos de conexión (dirección y puerto del servidor del Conector del dispositivo móvil) y haga clic en **Conectar**.



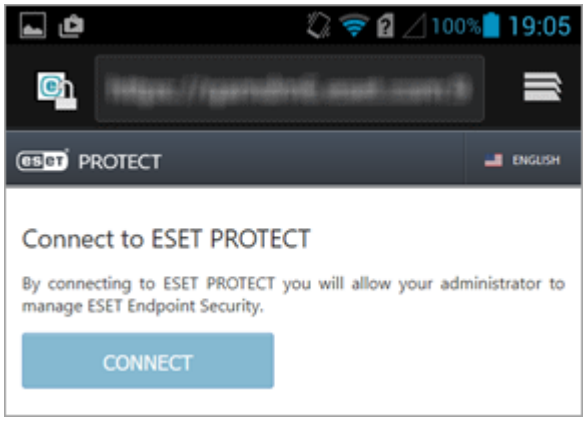
3. Escriba la contraseña del modo de administración de ESET Endpoint Security en el campo que aparece en blanco y pulse **Intro**.



4. Este dispositivo móvil está ahora administrado por ESET PROTECT On-Prem; pulse **Finalizar**.

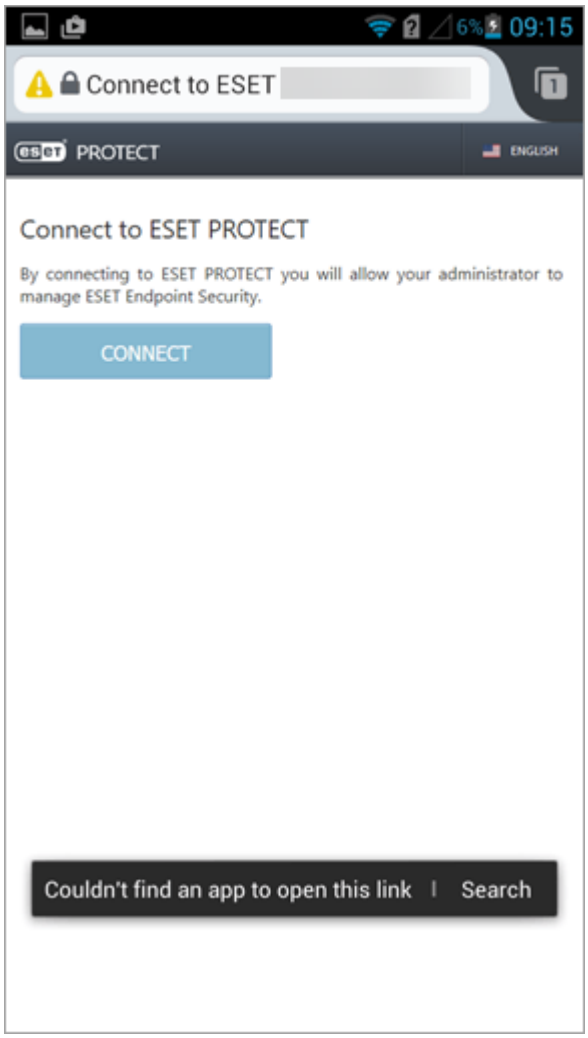
EESA aún no activado: siga los pasos indicados a continuación para activar el producto e inscribir su dispositivo:

1. Pulse la URL del vínculo de inscripción (incluido el número de puerto) y escríbala en el navegador manualmente (por ejemplo, *https://esmcmdm:9980/<token>*); también puede utilizar el **Código QR** proporcionado. Puede que se le pida que acepte un certificado SSL: haga clic en **Aceptar** si está de acuerdo y, a continuación, haga clic en **Conectar**.

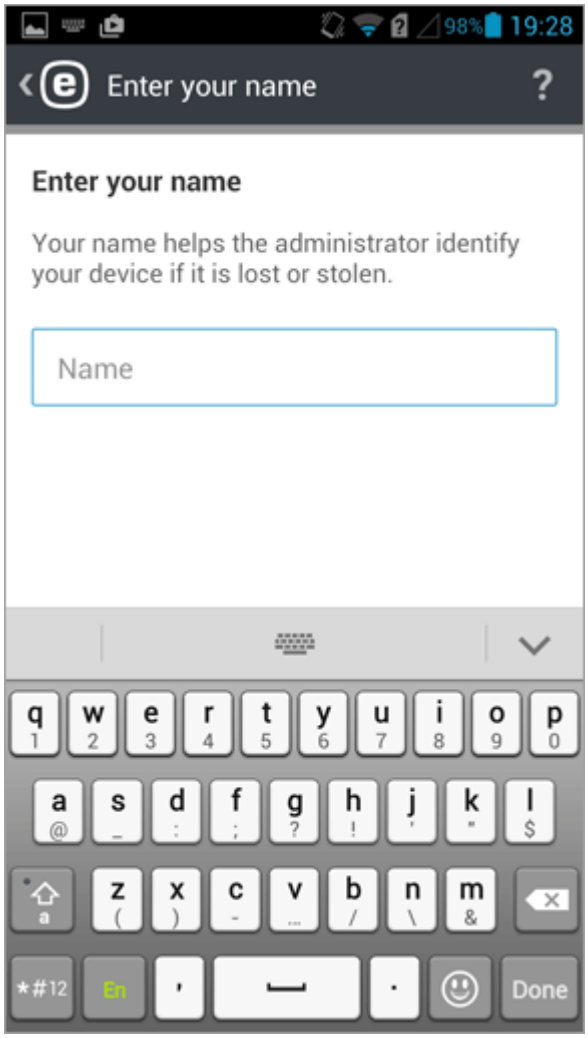


Si no tiene ESET Endpoint Security instalado en el dispositivo móvil, se le redirigirá automáticamente a Google Play para que descargue la aplicación.

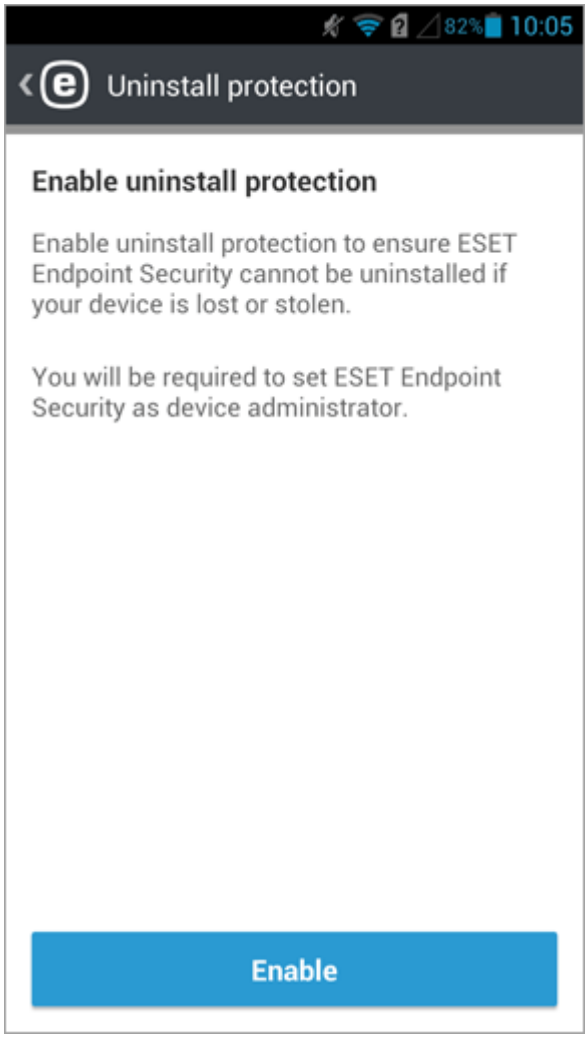
Si se muestra la notificación **No se encontró ninguna aplicación para abrir este vínculo**, intente abrir el vínculo de inscripción en el navegador web predeterminado de Android.



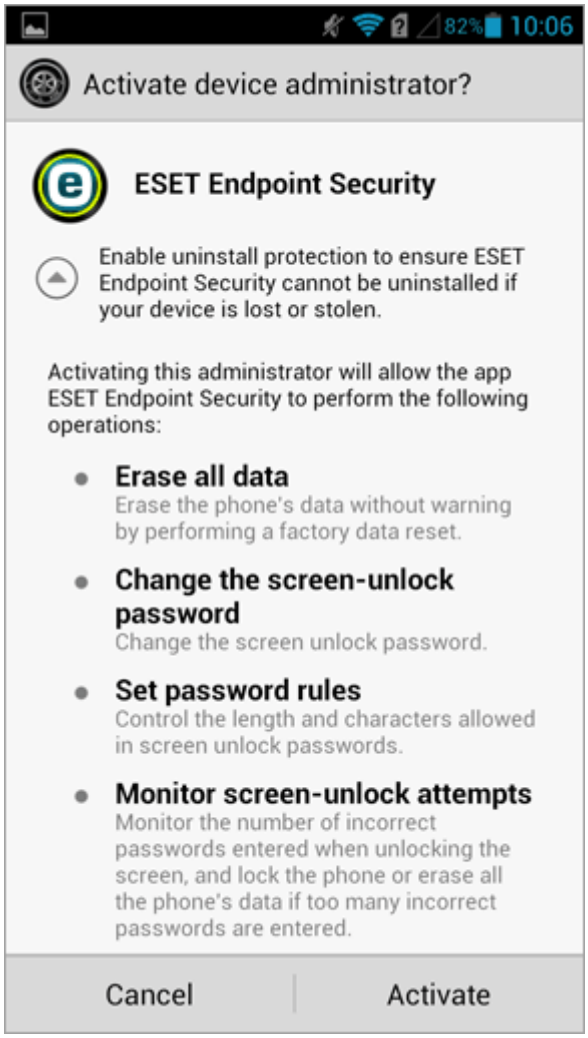
2. Escriba el nombre del dispositivo móvil. (Este nombre no está visible en ESET PROTECT On-Prem'. Solo es relevante para Antirrobo y para el registro de diagnóstico).



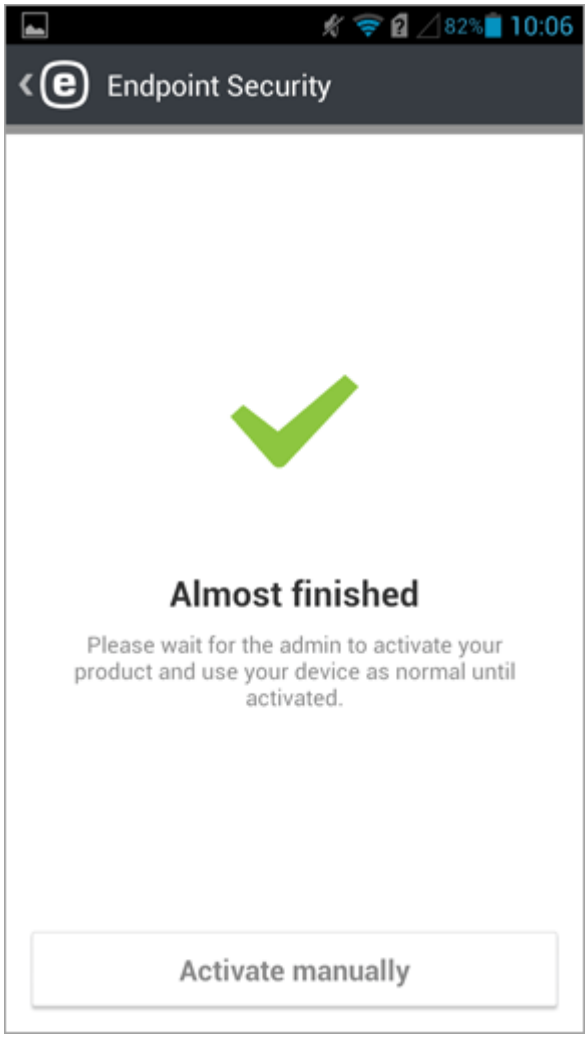
3. Pulse **Activar** para activar la protección de desinstalación.



4. Pulse **Activar** para activar el administrador del dispositivo.



5. En este punto puede salir de la aplicación ESET Endpoint Security para Android en el dispositivo móvil y abrir la Consola web de ESET PROTECT.



6. En la Consola web de ESET PROTECT, vaya a **Tareas del cliente** > **Móvil** > Activación del producto y haga clic en **Nuevo**.

La tarea del cliente Activación del producto podría tardar cierto tiempo en ejecutarse en el dispositivo móvil. Tras la correcta ejecución de la tarea, la aplicación ESET Endpoint Security para Android se activa y ESET PROTECT On-Prem puede administrar el dispositivo móvil. El usuario ya podrá usar la aplicación ESET Endpoint Security para Android. Mientras la aplicación ESET Endpoint Security para Android esté abierta, se mostrará el menú principal:

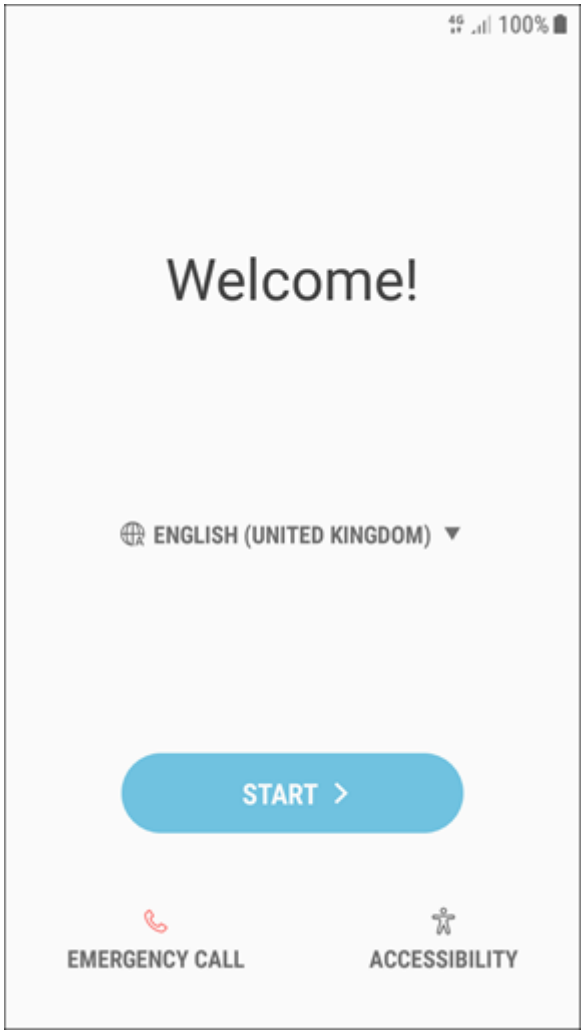
Inscripción de dispositivo Android como propietario del dispositivo

Este tipo de inscripción solo está disponible para dispositivos Android con Android v7 y posteriores. El dispositivo Android debe ser nuevo o debe haberse borrado o restablecido su configuración predeterminada para poder realizar su inscripción siguiendo los pasos que se indican a continuación.

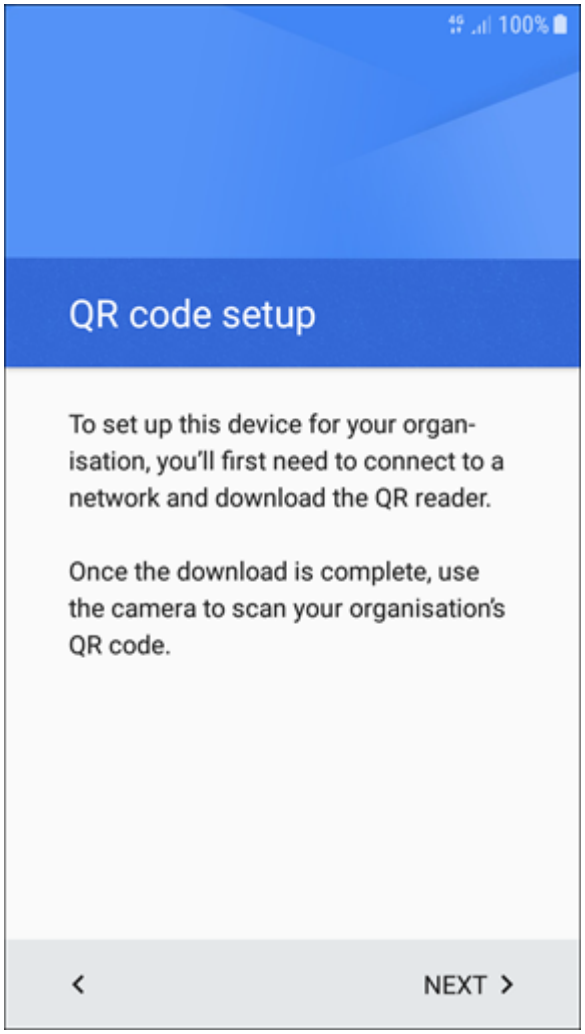
1. Encienda el dispositivo móvil.

2. Introduzca el pin de la tarjeta SIM.

3. En la pantalla de bienvenida, seleccione el idioma que prefiera y, a continuación, pulse seis (6) veces un lugar de la pantalla alrededor del texto "Bienvenida" para iniciar la configuración del código QR.

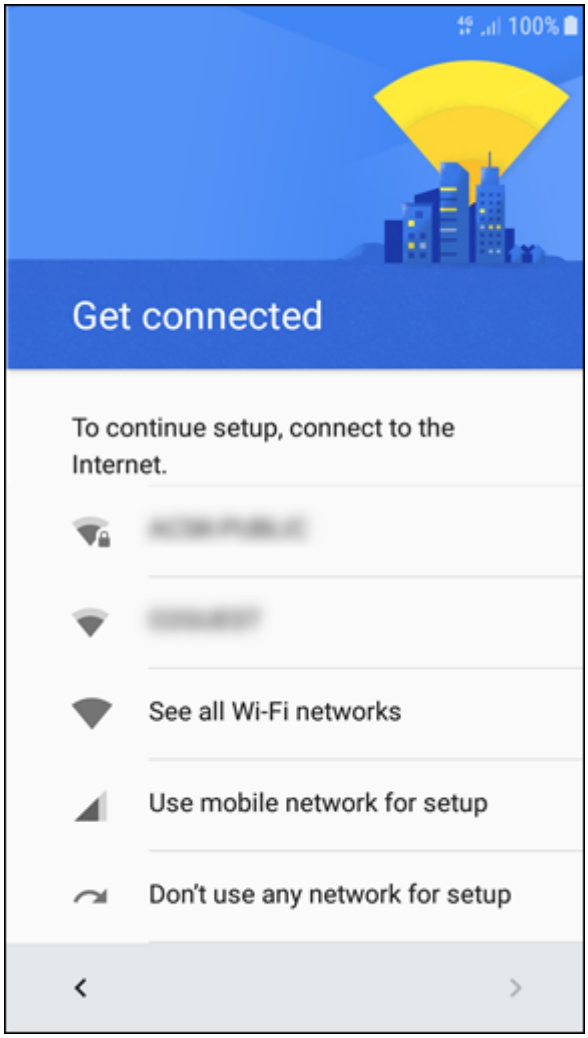


4. Si realizó el paso anterior correctamente, verá la pantalla **Configuración del código QR**. Pulse **SIGUIENTE** para continuar.



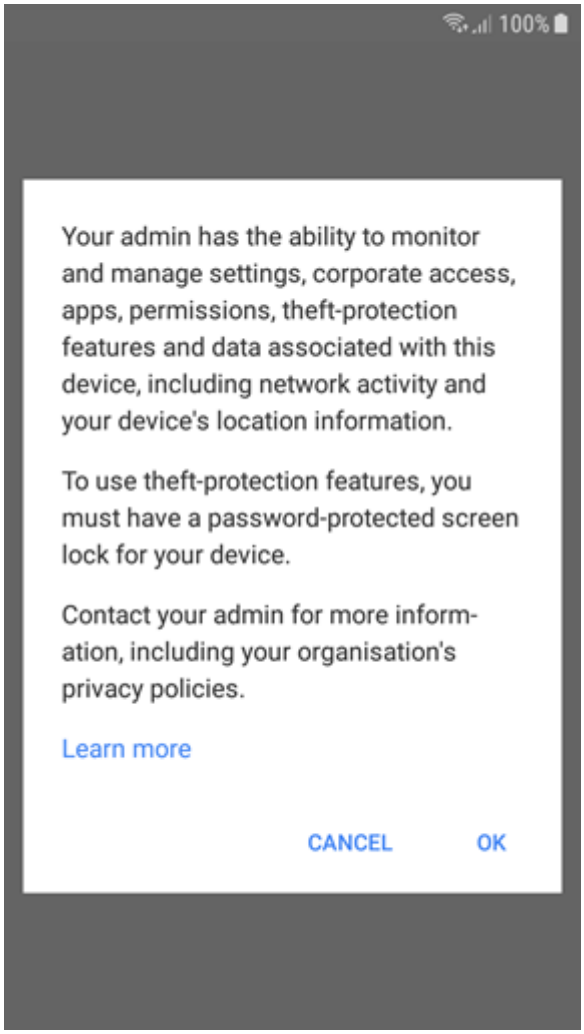
> En el caso de algunos dispositivos, es posible que deba cifrar su almacenamiento (a veces también es necesario conectar el cargador). Seleccione el tipo de cifrado que desee y siga las instrucciones de la pantalla.

5. Seleccione una conexión a Internet. Se utilizará para descargar el lector de códigos QR necesario para el siguiente paso.

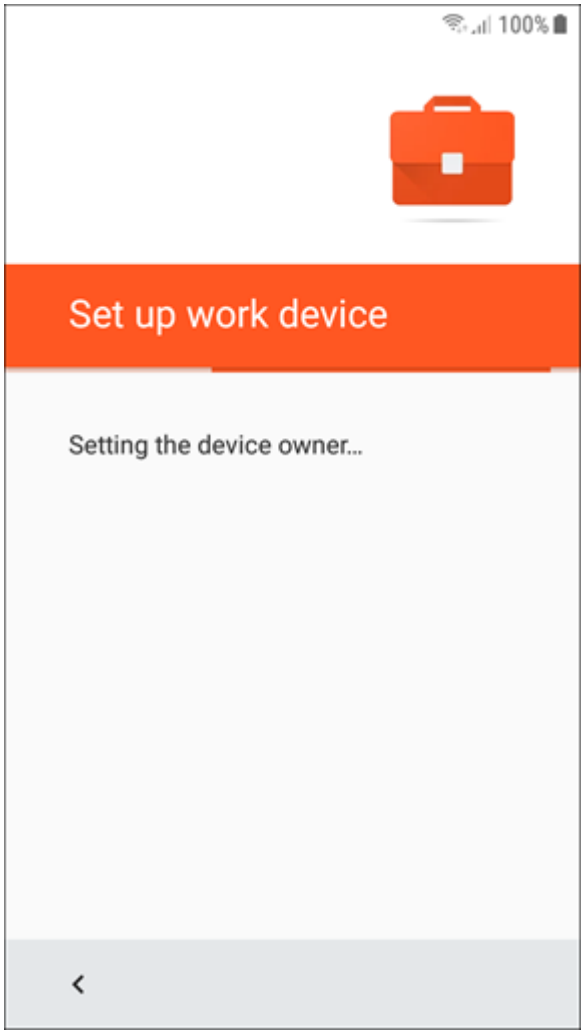


6. Se instalará el lector de códigos QR. Cuando finalice la instalación, escanee el código QR generado en la Consola web de ESET PROTECT.

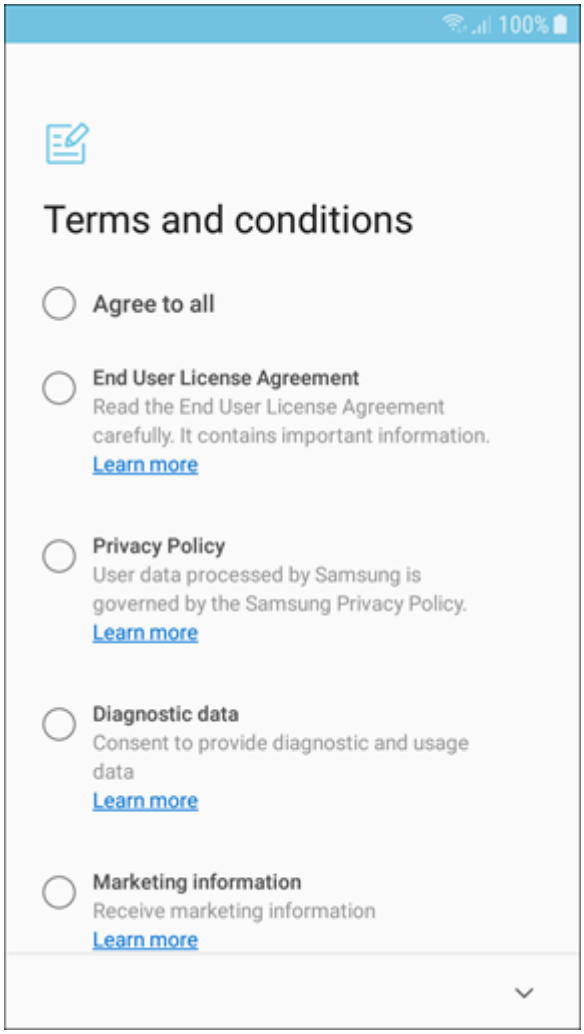
7. Se le pedirá que confirme que comprende que está concediendo más derechos de propietario del dispositivo al administrador. Pulse **Aceptar** para continuar.



8. Se instalará la aplicación ESET Endpoint Security para Android y se aplicarán los permisos necesarios.



9. Pulse **Aceptar todo** para permitir la transferencia de datos de marketing y diagnóstico, la Política de privacidad y el CLUF.



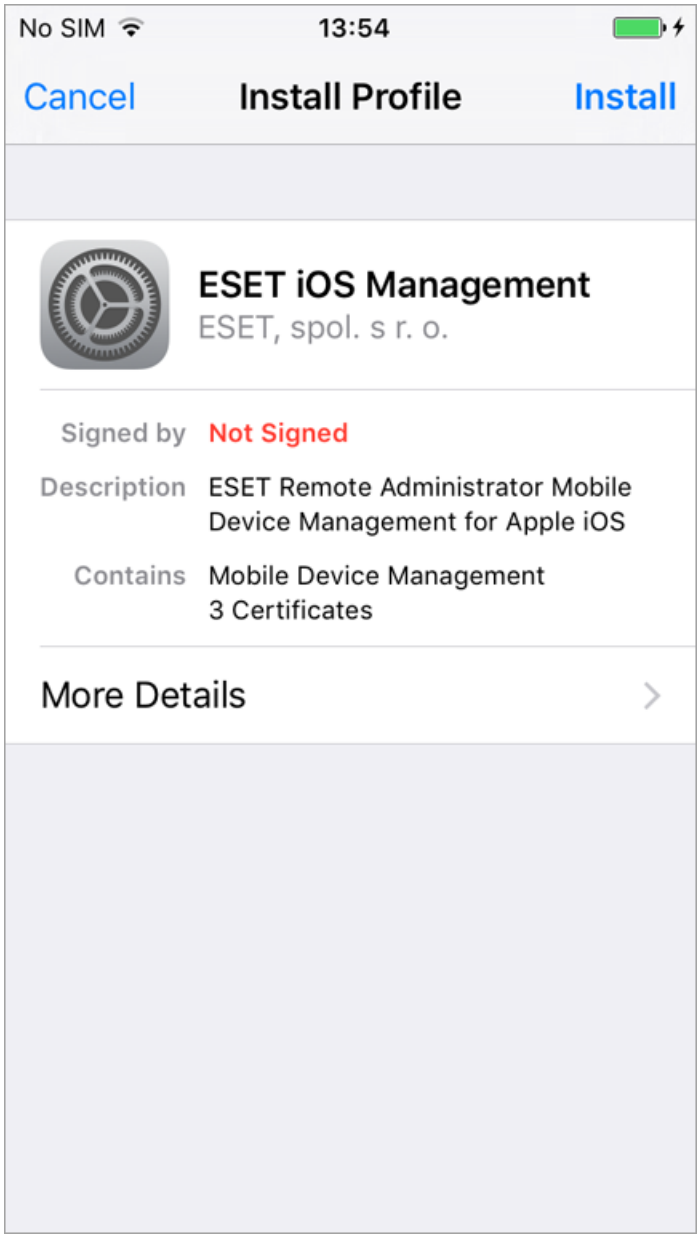
10. El dispositivo está inscrito en el modo Propietario del dispositivo.

Inscripción de dispositivo iOS

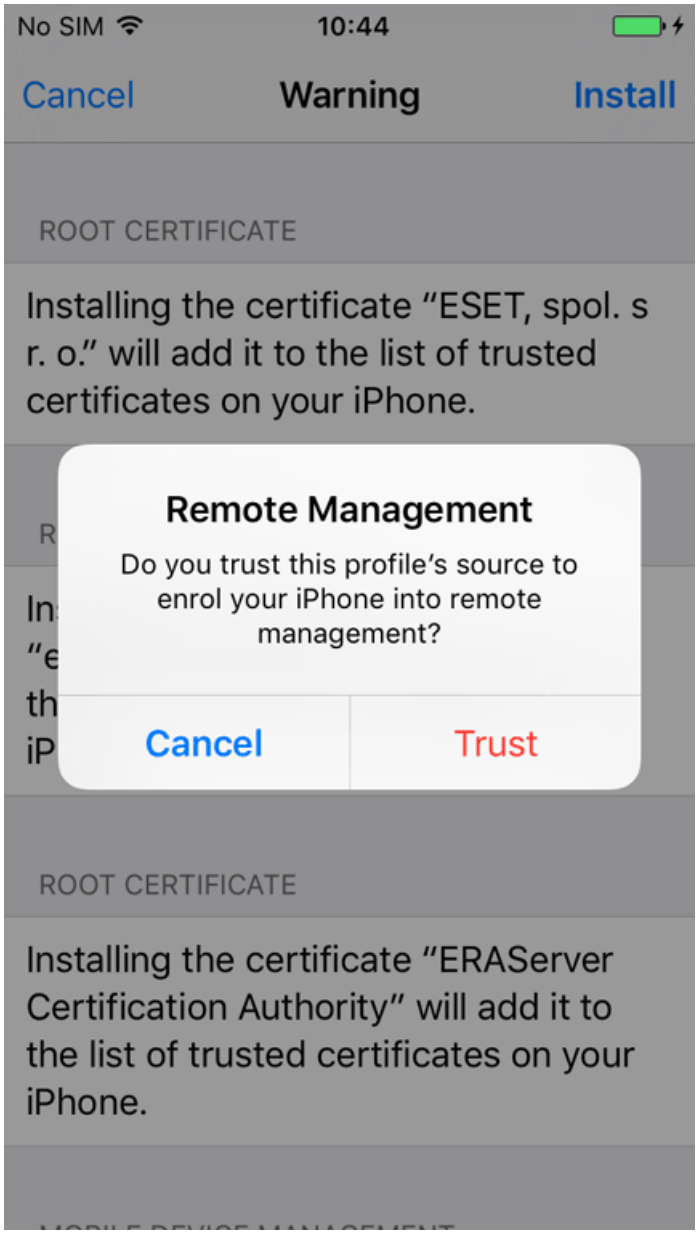
Siga estas instrucciones para inscribir un dispositivo iOS con Apple Business Manager (ABM).

1. Pulse la URL del vínculo de inscripción (incluido el número de puerto) y escríbala en el navegador manualmente (por ejemplo, *https://eramdm:9980/<token>*); también puede utilizar el **Código QR** proporcionado.

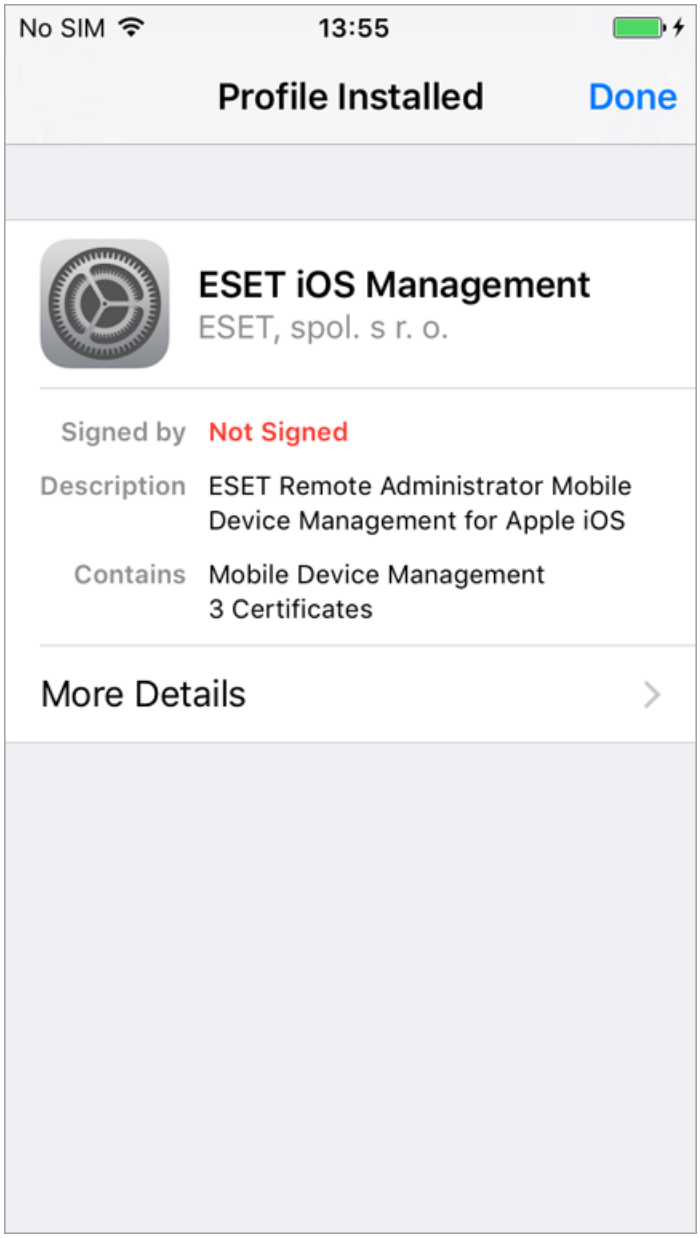
2. Pulse **Instalar** para continuar en la pantalla **Instalar perfil** del proceso de inscripción de MDM.



3. Pulse **Confiar** para permitir la instalación del nuevo perfil.

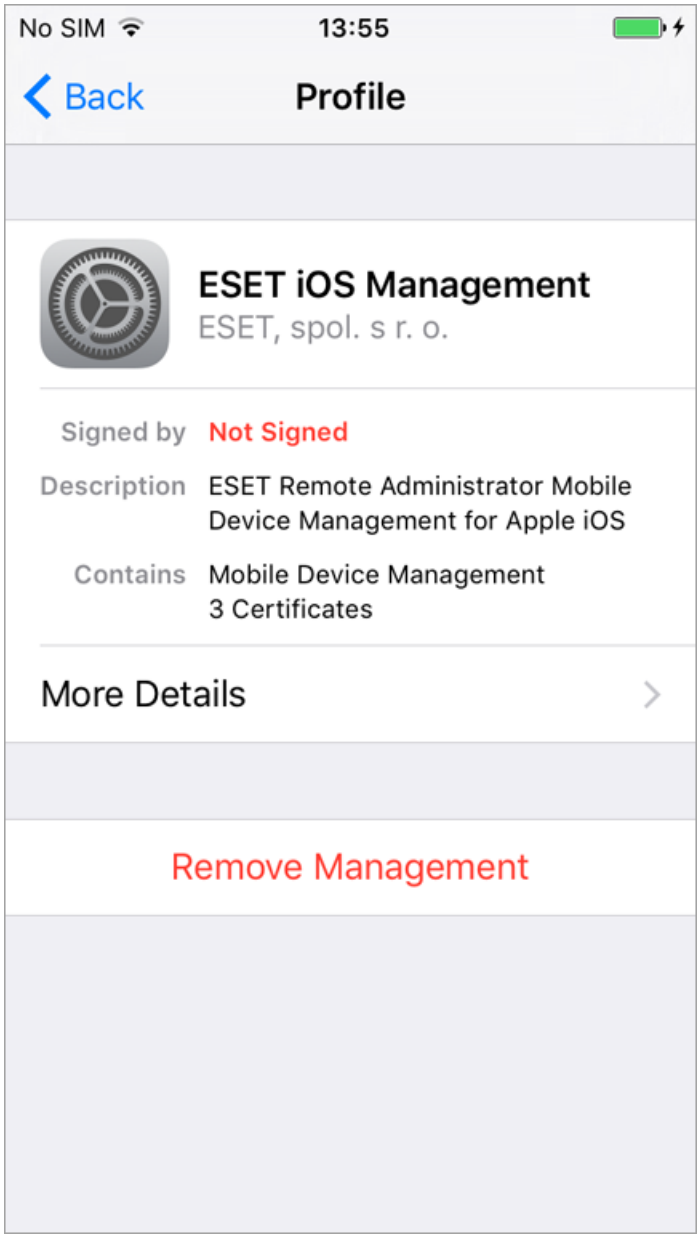


4. Después de instalar el nuevo perfil, el campo **Firmado por** mostrará que el perfil **no está firmado**. Esto se debe a que iOS no reconoce el certificado. Para tener un perfil de inscripción firmado, utilice el certificado HTTPS firmado por la autoridad certificadora de confianza de Apple. También puede utilizar 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 usuarios o grupos.

Al quitar el perfil de inscripción se quitan todos los ajustes de la empresa (Correo, Calendario, Contactos, etc.) y el dispositivo móvil iOS no se administrará. Si un usuario quita el perfil de inscripción, ESET PROTECT On-Prem no tendrá constancia de ello, y el estado del dispositivo cambiará a y, posteriormente, a después de 14 días, porque el dispositivo no se conecta. No se indicará de ningún otro modo que el perfil de inscripción se ha quitado.



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 también con una interacción mínima del usuario. La inscripción ABM de Apple ofrece a los administradores la opción de personalizar todo el proceso de configuración del dispositivo. También ofrece la opción de impedir que los usuarios quiten el perfil de MDM del dispositivo. Puede inscribir los dispositivos iOS que ya tenga (si cumplen los requisitos de ABM para dispositivos iOS) y todos los dispositivos iOS que compre en el futuro. Para obtener más información sobre Apple ABM, consulte la Guía de ABM de Apple y la documentación de ABM de Apple.

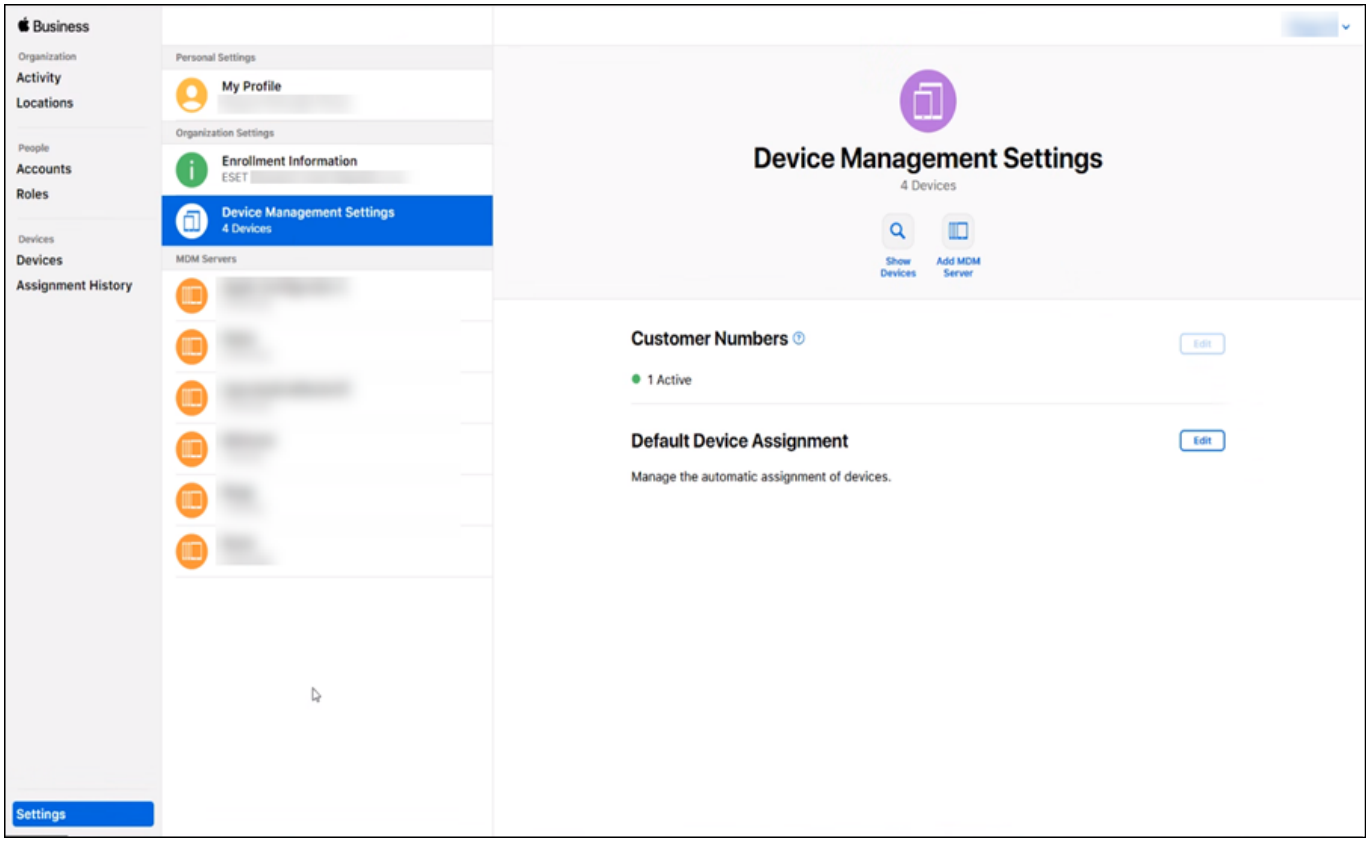
Sincronizar su ESET PROTECT MDM con el servidor de Apple ABM:

1. Compruebe que se cumplan todos los requisitos de ABM de Apple, tanto los requisitos de la cuenta como los requisitos del dispositivo.

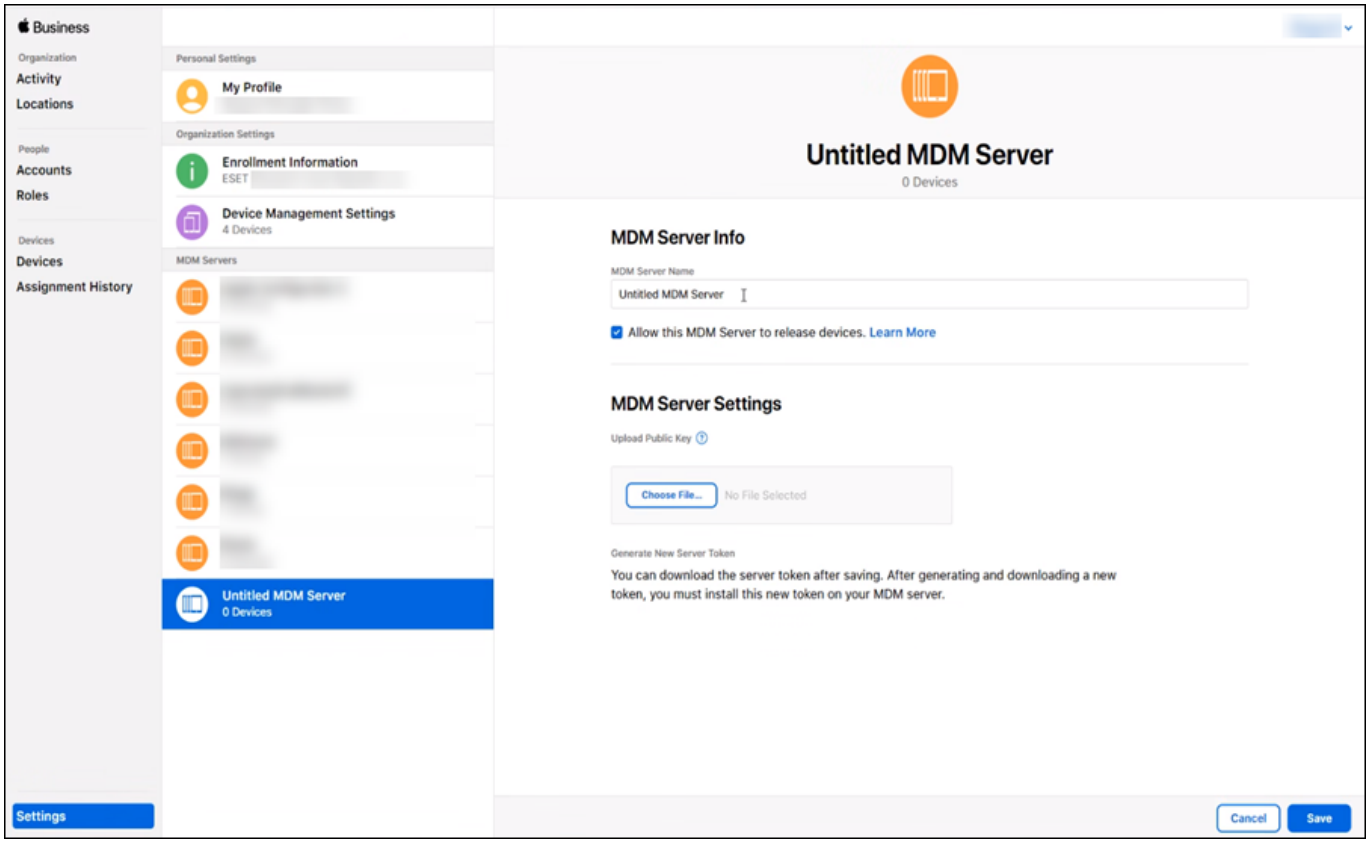
Cuenta de ABM:

- El programa solo está disponible en determinados países. Visite la Página web de Apple ABM para ver si ABM está disponible en su país.
- Los requisitos de la cuenta de Apple ABM están disponibles en estos sitios web: Requisitos del Programa de implementación de Apple y Requisitos del Programa de inscripción de dispositivos de Apple.
- Consulte todos los requisitos del dispositivo de ABM.

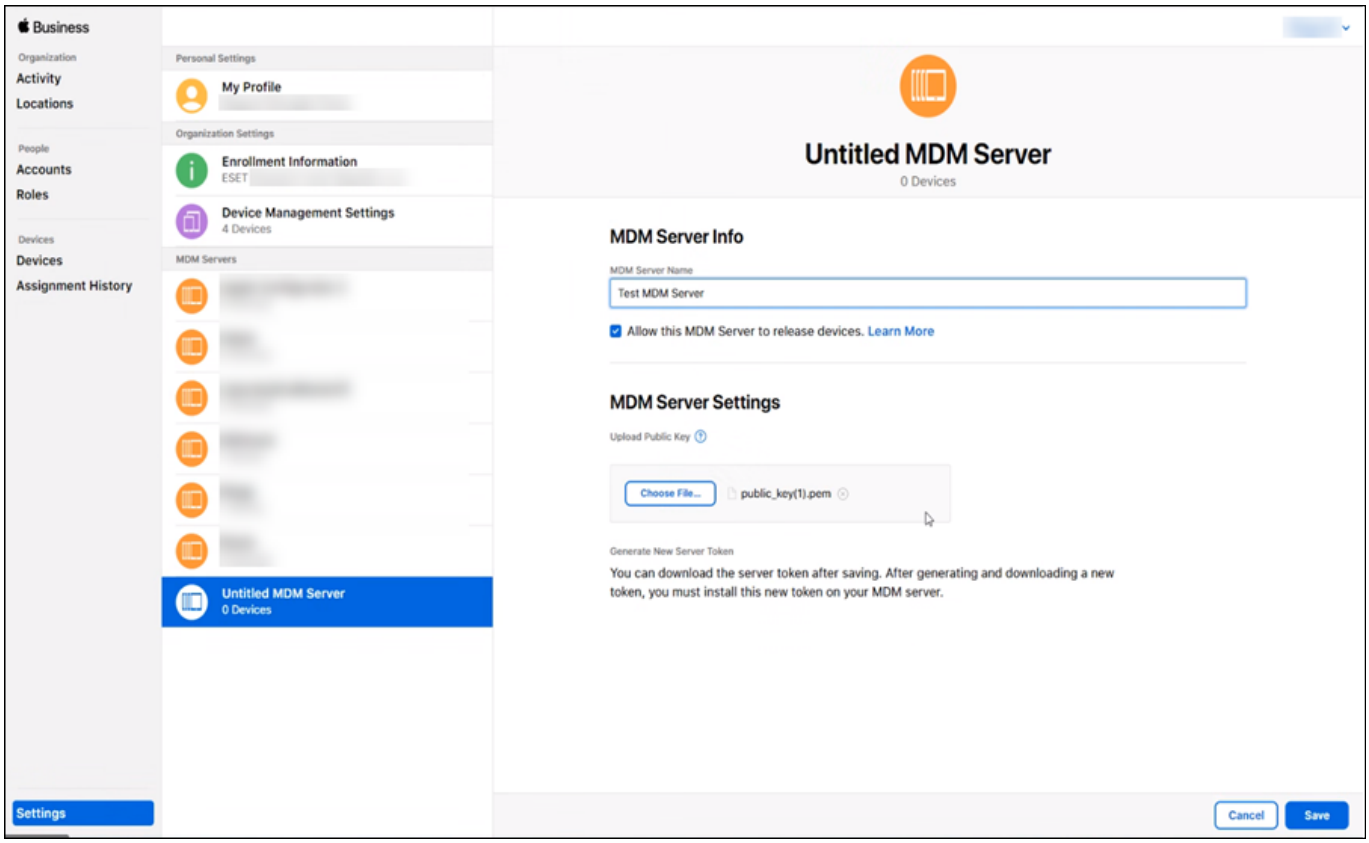
2. Inicie sesión en su cuenta de Apple ABM (si no tiene una cuenta de Apple ABM, puede crearla).
3. En la sección **Ajustes de gestión de dispositivos,** seleccione **Agregar servidor MDM**.



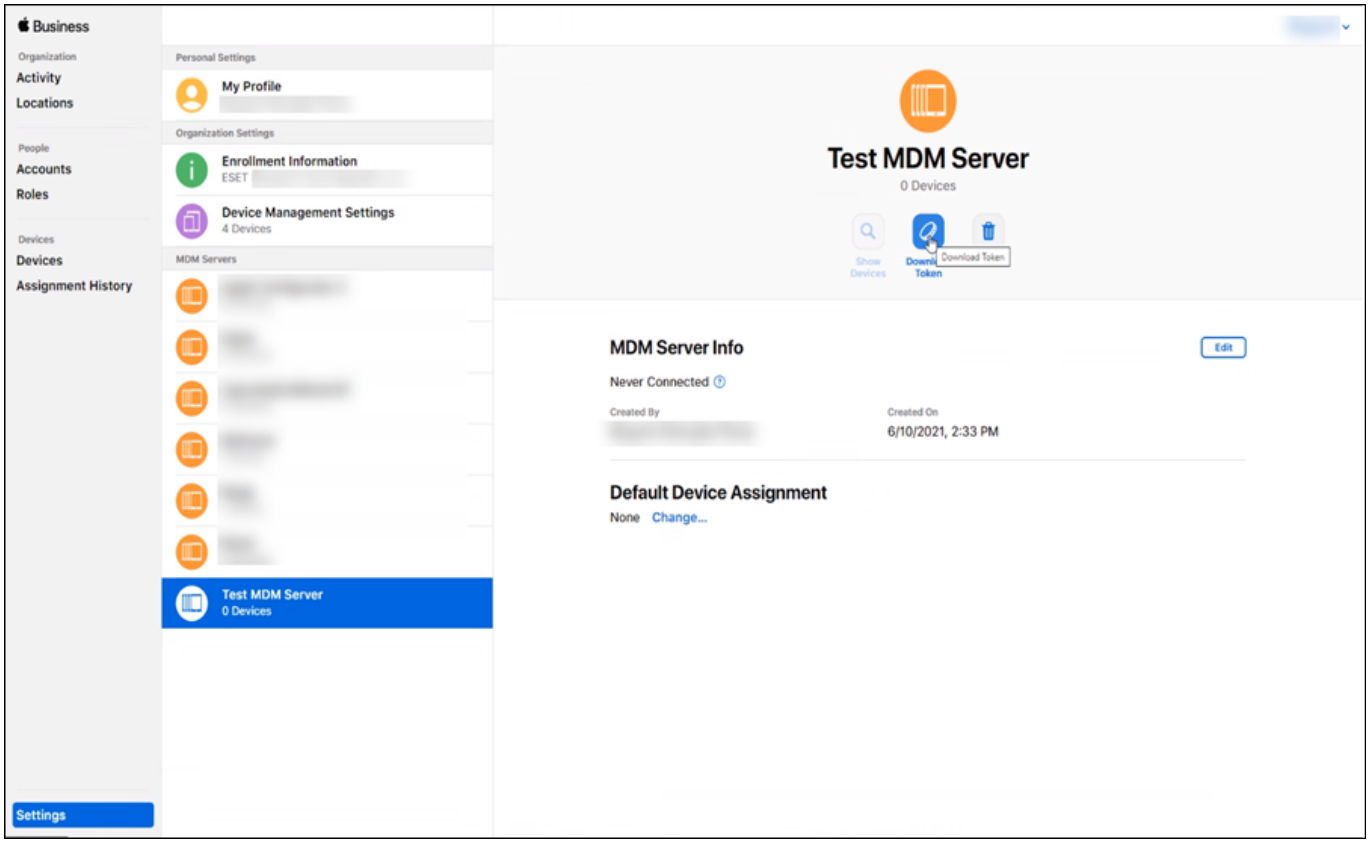
4. En la pantalla Servidor MDM sin título, escriba el **nombre del servidor MDM**, por ejemplo: "MDM_Server".



5. Cargue su clave pública en el portal de ABM. Haga clic en **Elegir archivo**, seleccione el archivo de clave pública (es el certificado APNS que descargó del Portal de certificados push de Apple) y haga clic en **Guardar**.



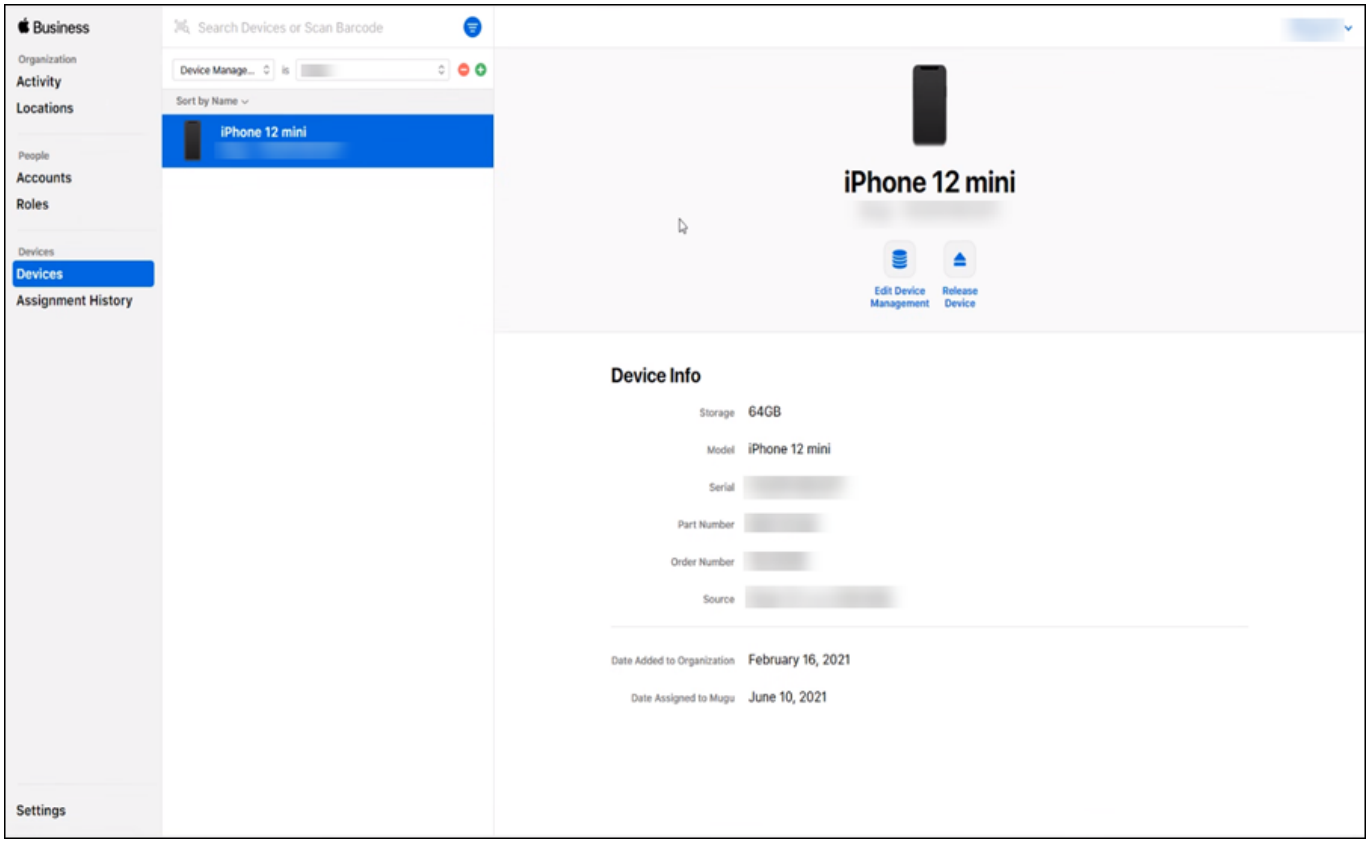
6. Haga clic en **Descargar token** para descargar su token ABM de Apple. Este archivo se cargará en la política de MDC de ESET PROTECT en **Apple Business Manager (ABM)** > **Cargar token de autorización**.



Agregue el dispositivo iOS al ABM de Apple

El siguiente paso es asignar dispositivos iOS a su servidor MDM virtual en el portal de Apple ABM. Puede asignar sus dispositivos iOS por número de serie o número de orden o cargando una lista de números de serie correspondientes a los dispositivos de destino en formato CSV. De cualquiera de las dos formas, debe asignar el dispositivo iOS al servidor MDM virtual (lo creó en los pasos anteriores).

1. Vaya a la sección **Dispositivos** del portal de ABM, seleccione el dispositivo que desea asignar y haga clic en **Editar gestión de dispositivos**.



2. Tras seleccionar el servidor MDM en la lista, confirme la selección y se asignará el dispositivo móvil a su servidor MDM.

⚠ Cuando se quita un dispositivo del portal de ABM, se quita de forma permanente: no podrá volver a agregarlo.

Después puede salir del portal de ABM de Apple y continuar en la Consola web de ESET PROTECT.

⚠ Si está inscribiendo dispositivos iOS en uso (que cumplen los requisitos del dispositivo), se les aplicará una nueva configuración de la política tras restablecer los valores de fábrica del dispositivo de destino.

Para completar el proceso de inscripción, debe cargar el certificado APNS en la Política para MDC que se le asignará al servidor MDM. (Esta Política para MDC desempeñará la función de la configuración del servidor MDM).

ℹ Si su dispositivo iOS muestra el mensaje de que no puede descargar el perfil de ESET durante la inscripción, compruebe que el servidor MDM de ABM esté correctamente configurado (que tenga los certificados adecuados) y que haya asignado el dispositivo iOS correcto al ESET PROTECT MDM Server que seleccionó en Apple ABM.

Solución de problemas: volver a agregar un dispositivo ABM eliminado

Si ha eliminado un dispositivo ABM de la lista de dispositivos en la consola web de ESET PROTECT, siga los pasos que se indican a continuación para volver a agregarlo a la consola web de ESET PROTECT:

1. Anule la asignación del dispositivo del servidor de administración de dispositivos móviles en ABM. No libere el dispositivo en el portal de ABM.

2. Espere 30 minutos.

3. Vuelva a asignar el dispositivo al servidor de administración de dispositivos móviles.

Inscripción por correo electrónico

Este método es ideal para la inscripción en masa de dispositivos móviles. Puede enviar un vínculo de inscripción por correo electrónico a cualquier número de dispositivos. Cada dispositivo móvil recibirá un token único de un solo uso basado en la dirección de correo electrónico.

Es obligatorio configurar un servidor SMTP para la inscripción en masa por correo electrónico. Vaya a **Más** > Configuración, despliegue **Configuración avanzada** y especifique los detalles del servidor SMTP.

1.Para agregar nuevos dispositivos móviles, vaya a la sección **Ordenadores**. Seleccione el **Grupo estático** al que desee agregar los 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 que cree un **Nuevo grupo estático** (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 configuraciones**

o**Mobile Device Connector** se seleccionará automáticamente. Si tiene más de un MDC, seleccione el FQDN del MDC que quiera utilizar. Si aún no tiene instalado el Conector del dispositivo móvil, consulte los capítulos Instalación del Conector del dispositivo móvil: Windows o Linux para acceder a las instrucciones de instalación.

o**Licencia**: haga clic en **Seleccionar** y elija la licencia que se utilizará para la activación. Se creará una tarea de cliente de Activación del producto para el dispositivo móvil. Se utilizará una unidad de licencia (una por cada dispositivo móvil).

o**Etiquetas**: seleccione o agregue las etiquetas pertinentes para identificar el dispositivo móvil.

7.Diríjase a **Configuración del producto**.

8. Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

9.Diríjase a **Lista**.

10. **Lista de dispositivos**: especifique los dispositivos móviles que desee inscribir; puede utilizar las opciones que se indican a continuación para agregar dispositivos móviles.

- **Agregar**: una sola entrada; debe escribir manualmente una dirección de correo electrónico asociada

con el dispositivo móvil al que se va a enviar el mensaje de correo electrónico de inscripción. Si asigna un usuario al dispositivo móvil haciendo clic en **Emparejar con usuario existente** y seleccionando el usuario, la dirección de correo electrónico se sobrescribe con la especificada en la pantalla **Más** > Usuarios del ordenador. Si desea agregar otro dispositivo móvil, haga clic de nuevo en **Agregar** y envíe la información necesaria.

• **Agregar usuario**: puede agregar dispositivos marcando las casillas de los usuarios correspondientes en **Más** > Usuarios del ordenador. Haga clic en **Cancelar emparejamiento** si desea corregir la lista de dispositivos móviles que se van a inscribir. Si cancela el emparejamiento de un usuario asignado, ese usuario aparecerá como no emparejado. Haga clic en **Emparejar** para seleccionar el usuario que desee asignar a un dispositivo no emparejado. Haga clic en el icono de la **Papelera** para eliminar una entrada.

• **Importar CSV**: un método que facilita la tarea de agregar un gran número de dispositivos móviles. Cargue un archivo *.csv* que contenga la lista de dispositivos que desee agregar; consulte Importar CSV si desea obtener más información.

• **Pegar del portapapeles** – Importe una lista personalizada de direcciones separadas por delimitadores personalizados (esta función tiene un comportamiento similar al de la importación de CSV).

Le recomendamos que asigne al menos un usuario a cada dispositivo móvil. Si desea utilizar políticas personalizadas en iOS, debe asignarse un usuario a cada dispositivo.
Le recomendamos que especifique el **nombre del dispositivo** en cada entrada cuando utilice el método de importación de CSV. Este es el nombre del dispositivo mostrado en la sección **Ordenadores**. Si deja vacío el campo **Nombre del dispositivo**, se utilizará en su lugar la dirección de correo electrónico, y aparecerá como Nombre del dispositivo en **Ordenadores** y en **Grupos**. Esto puede causar confusión, sobre todo si utiliza la misma dirección de correo electrónico para inscribir varios dispositivos. Esta dirección de correo electrónico aparecerá varias veces, y le impedirá distinguir un dispositivo de otro.

11. Diríjase a **Inscripción**.

12. **Vista previa de mensaje de correo electrónico**: una plantilla de mensaje predefinida que contiene los detalles necesarios para que el usuario se inscriba. Las **Instrucciones** se muestran bajo el **Contenido** en el mensaje de correo electrónico de inscripción, y contienen el **nombre del dispositivo** (o una dirección de correo electrónico) y el vínculo de inscripción (URL). Si utiliza una dirección de correo electrónico para inscribir varios dispositivos móviles, se mostrará una lista de dispositivos, cada uno con su propio vínculo de inscripción (URL) asignado. También hay instrucciones que el usuario del dispositivo móvil (iOS y Android) debe seguir para completar la inscripción.

13. Al hacer clic en **Enviar** se envía un mensaje de correo electrónico a cada dirección de correo electrónico con el vínculo o los vínculos de inscripción y las instrucciones correspondientes.

14. Para completar la inscripción del dispositivo, siga estos pasos o pida a los usuarios/propietarios de los dispositivos móviles que los sigan:

- Inscripción de dispositivo Android
- Inscripción de dispositivo iOS

Inscripción individual mediante vínculo o código QR

Al inscribir un dispositivo móvil utilizando un vínculo de inscripción o un código QR necesitará acceso físico al dispositivo. Además, para utilizar el código QR, deberá tener una aplicación de lectura/escáner de códigos QR instalada en el dispositivo móvil.

> Para grandes números de dispositivos móviles, le recomendamos que utilice la inscripción por correo electrónico.

1.Para agregar nuevos dispositivos móviles, vaya a la sección **Ordenadores**. Seleccione el **Grupo estático al que desee agregar los 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 que cree un **Nuevo grupo estático** (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 configuraciones**

o**Mobile Device Connector** se seleccionará automáticamente. Si tiene más de un MDC, seleccione el FQDN del MDC que quiera utilizar. Si aún no tiene instalado el Conector del dispositivo móvil, consulte los capítulos Instalación del Conector del dispositivo móvil: Windows o Linux para acceder a las instrucciones de instalación.

o**Licencia**: haga clic en **Seleccionar** y elija la licencia que se utilizará para la activación. Se creará una tarea de cliente de Activación del producto para el dispositivo móvil. Se utilizará una unidad de licencia (una por cada dispositivo móvil).

o**Etiquetas**: seleccione o agregue las etiquetas pertinentes para identificar el dispositivo móvil.

7.Diríjase a **Configuración del producto**.

8. Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

9.Diríjase a **Lista**.

10. **Lista de dispositivos**: especifique los dispositivos móviles que desee inscribir; puede utilizar las opciones que se indican a continuación para agregar dispositivos móviles.

- **Agregar**: una sola entrada; debe escribir manualmente una dirección de correo electrónico asociada con el dispositivo móvil al que se va a enviar el mensaje de correo electrónico de inscripción. Si asigna un usuario al dispositivo móvil haciendo clic en **Emparejar con usuario existente** y seleccionando el usuario, la dirección de correo electrónico se sobrescribe con la especificada en la pantalla **Más** > Usuarios del ordenador. Si desea agregar otro dispositivo móvil, haga clic de nuevo en **Agregar** y envíe la

información necesaria.

• **Agregar usuario**: puede agregar dispositivos marcando las casillas de los usuarios correspondientes en **Más** > Usuarios del ordenador. Haga clic en **Cancelar emparejamiento** si desea corregir la lista de dispositivos móviles que se van a inscribir. Si cancela el emparejamiento de un usuario asignado, ese usuario aparecerá como no emparejado. Haga clic en **Emparejar** para seleccionar el usuario que desee asignar a un dispositivo no emparejado. Haga clic en el icono de la **Papelera** para eliminar una entrada.

• **Importar CSV**: un método que facilita la tarea de agregar un gran número de dispositivos móviles. Cargue un archivo *.csv* que contenga la lista de dispositivos que desee agregar; consulte Importar CSV si desea obtener más información.

• **Pegar del portapapeles** – Importe una lista personalizada de direcciones separadas por delimitadores personalizados (esta función tiene un comportamiento similar al de la importación de CSV).

11. Cuando haga clic en **Continuar**, se mostrará una lista de dispositivos con el **Vínculo** de inscripción (URL) y el **código QR** correspondientes. Escriba toda la URL en el navegador del dispositivo móvil 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. También puede utilizar un **código QR**, que puede ser más práctico que escribir la URL, pero requiere un lector/escáner de códigos QR en el dispositivo móvil.

12. Una vez que haya completado la inscripción de todos los dispositivos seleccionados, haga clic en **Finalizar**.

13. Para inscribir realmente los dispositivos móviles, siga estas instrucciones paso a paso:

- Inscripción de dispositivo Android
- Inscripción de dispositivo iOS

Propietario del dispositivo Android (solo Android 7 y versiones posteriores)

Al inscribir un dispositivo móvil Android con un código QR de inscripción, necesitará acceso físico al dispositivo. Asimismo, esta inscripción solo puede realizarse en un dispositivo si es completamente nuevo, se ha restablecido a los valores predeterminados o se han borrado sus datos.

> No es posible utilizar Inscripción por correo electrónico para realizar una inscripción en masa de dispositivos Android como propietario del dispositivo.

1.Para agregar nuevos dispositivos móviles, vaya a la sección **Ordenadores**. Seleccione el **Grupo estático al que desee agregar los dispositivos móviles y** haga clic en **Agregar dispositivo** > **Dispositivos móviles** .

2.Vaya a la sección **Básica**.

3.**Seleccionar tipo**: Seleccionar **Propietario del dispositivo Android (solo Android 7 y versiones posteriores)**.

4.**Distribución**: seleccione **Explorar código QR**.

5.**Grupo principal**: si no tiene un grupo estático específico para dispositivos móviles, le recomendamos que cree un **Nuevo grupo estático** (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 configuraciones**

- **Mobile Device Connector** se seleccionará automáticamente. Si tiene más de un MDC, seleccione el FQDN del MDC que quiera utilizar. Si aún no tiene instalado el Conector del dispositivo móvil, consulte los capítulos Instalación del Conector del dispositivo móvil: Windows o Linux para acceder a las instrucciones de instalación.

- **Licencia**: haga clic en **Seleccionar** y elija la licencia que se utilizará para la activación. Se creará una tarea de cliente de Activación del producto para el dispositivo móvil. Se utilizará una unidad de licencia (una por cada dispositivo móvil).

- **Etiquetas**: seleccione o agregue las etiquetas pertinentes para identificar el dispositivo móvil.

7.Diríjase a **Configuración del producto**.

8. Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

9.Diríjase a **Lista**.

10. **Lista de dispositivos**: especifique los dispositivos móviles que desee inscribir; puede utilizar las opciones que se indican a continuación para agregar dispositivos móviles.

- **Agregar**: una sola entrada; debe escribir manualmente una dirección de correo electrónico asociada con el dispositivo móvil al que se va a enviar el mensaje de correo electrónico de inscripción. Si asigna un usuario al dispositivo móvil haciendo clic en **Emparejar con usuario existente** y seleccionando el usuario, la dirección de correo electrónico se sobrescribe con la especificada en la pantalla **Más** > Usuarios del ordenador. Si desea agregar otro dispositivo móvil, haga clic de nuevo en **Agregar** y envíe la información necesaria.

- **Agregar usuario**: puede agregar dispositivos marcando las casillas de los usuarios correspondientes en **Más** > Usuarios del ordenador. Haga clic en **Cancelar emparejamiento** si desea corregir la lista de dispositivos móviles que se van a inscribir. Si cancela el emparejamiento de un usuario asignado, ese usuario aparecerá como no emparejado. Haga clic en **Emparejar** para seleccionar el usuario que desee asignar a un dispositivo no emparejado. Haga clic en el icono de la **Papelera** para eliminar una entrada.

- **Importar CSV**: un método que facilita la tarea de agregar un gran número de dispositivos móviles. Cargue un archivo *.csv* que contenga la lista de dispositivos que desee agregar; consulte Importar CSV si desea obtener más información.

- **Pegar del portapapeles** – Importe una lista personalizada de direcciones separadas por delimitadores personalizados (esta función tiene un comportamiento similar al de la importación de CSV).

11. Cuando haga clic en **Continuar**, se mostrará una lista de dispositivos con el **Vínculo** de inscripción (URL) y el **código QR** correspondientes. Escriba toda la URL en el navegador del dispositivo móvil 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. También puede utilizar un **código QR**, que puede ser más

práctico que escribir la URL, pero requiere un lector/escáner de códigos 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 directiva para el MDM de iOS: cuenta de Exchange ActiveSync

Esta política rige todos los ajustes del dispositivo iOS. Esta configuración se aplica tanto a los dispositivos iOS ABM como a los que no son ABM.

- La configuración solo para ABM se marca con un ícono de ABM 

. Estos ajustes solo se aplicarán a dispositivos iOS inscritos en el portal de ABM de Apple. Le recomendamos que no personalice estos ajustes exclusivos para ABM al crear una política para dispositivos iOS que no son ABM.

- Algunos ajustes solo pueden aplicarse a un dispositivo iOS con una determinada versión de iOS. Estos ajustes están marcados con un icono que representa la versión de iOS; por ejemplo, iOS versión 11.0 y posteriores 

.

- Si aparecen ambos iconos (icono de ABM e icono de la versión de iOS) junto a un ajuste concreto, el dispositivo debe cumplir ambos requisitos para que no falle la gestión del ajuste.

Vea el siguiente caso de ejemplo, en el que se explica cómo utilizar la política MDM de iOS cuando se quiere configurar una cuenta de correo de Microsoft Exchange:

Puede usar esta directiva para configurar una cuenta de correo, contactos y calendario de Microsoft Exchange en los dispositivos móviles iOS del usuario. La ventaja de usar una directiva de este tipo es que solo tendrá que crear una directiva, que posteriormente podrá aplicar a numerosos dispositivos móviles con iOS sin necesidad de configurar cada uno de ellos por separado. Esto es posible gracias a los atributos del usuario de Active Directory. Debe especificar una variable, por ejemplo `${exchange_login/exchange}`, que se sustituirá con un valor del AD de un usuario concreto.

Si no usa Microsoft Exchange o Exchange ActiveSync, puede configurar manualmente cada uno de los servicios (**Cuentas de correo**, **Cuentas de contactos**, **Cuentas LDAP**, **Cuentas de calendario** y **Cuentas de calendario suscritas**).

En el siguiente ejemplo se muestra cómo crear y aplicar una nueva directiva para configurar automáticamente el correo, los contactos y el calendario para cada usuario de dispositivo móvil iOS utilizando el protocolo Exchange ActiveSync (EAS) para sincronizar estos servicios.

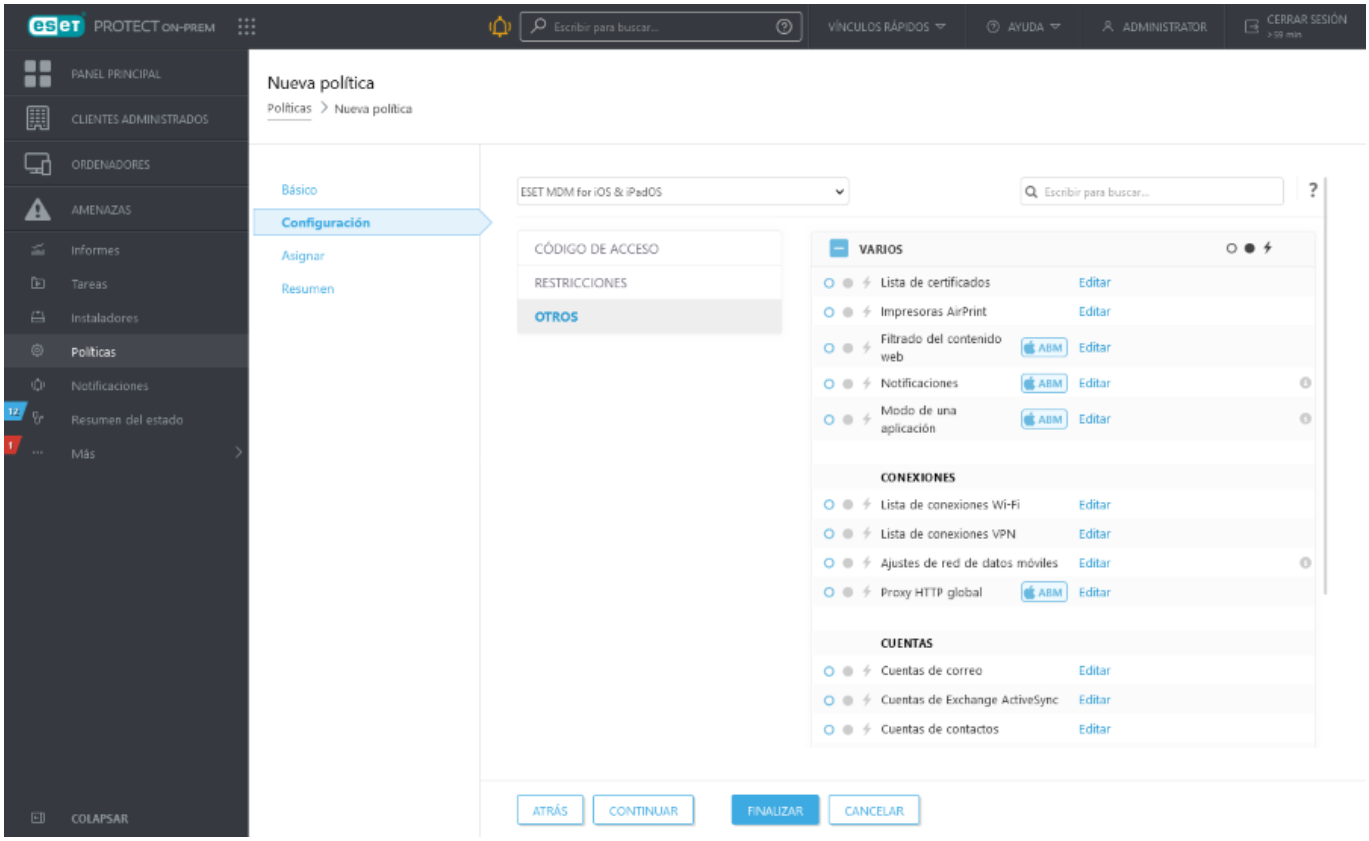
> Antes de comenzar a configurar esta política, asegúrese de haber realizado los pasos descritos en Administración de dispositivos móviles.

Básico

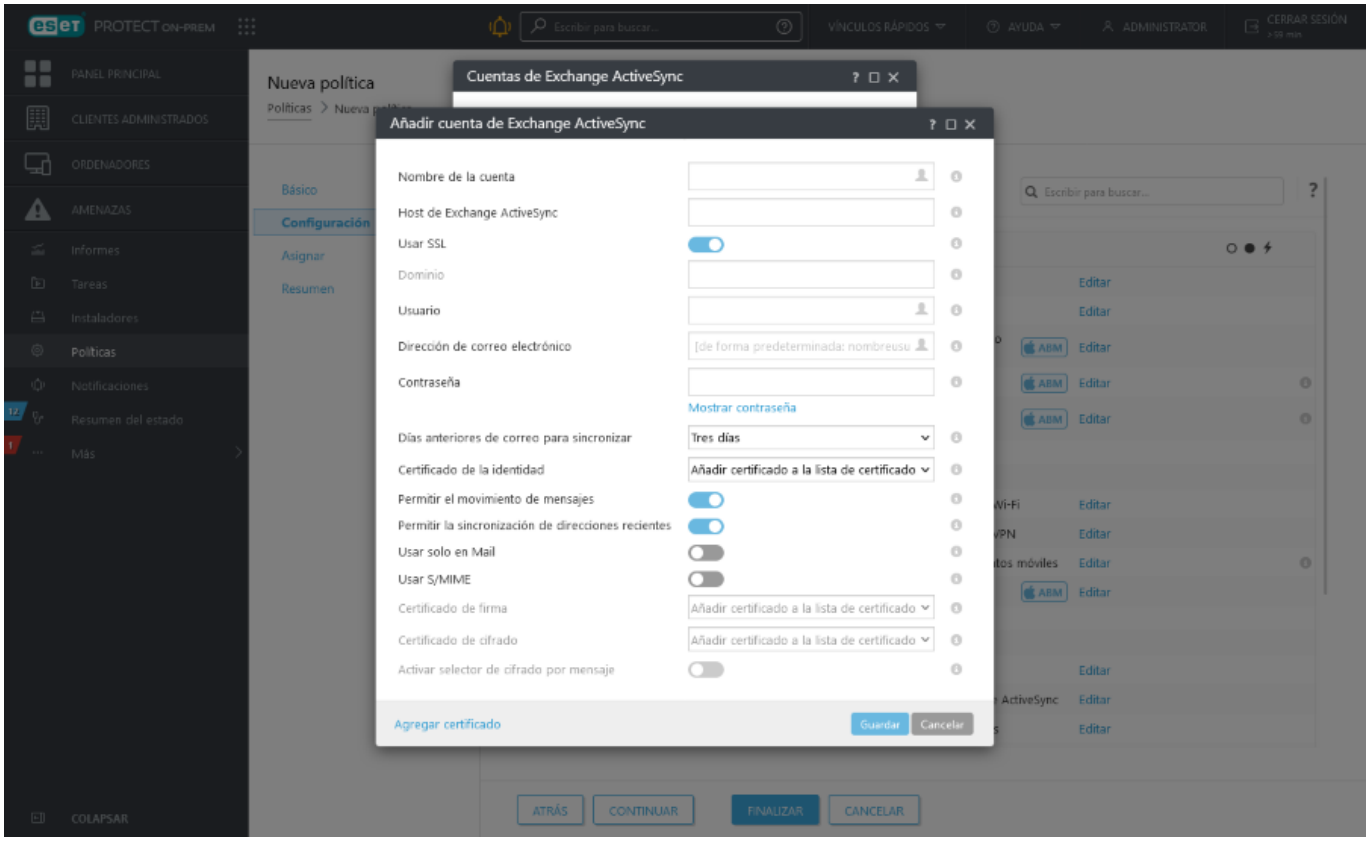
Escriba el **Nombre** de esta directiva. El campo **Descripción** es opcional.

Configuración

Seleccione **ESET MDM para iOS/iPadOS** en la lista desplegable, haga clic en **Otros** para desplegar las categorías y, a continuación, haga clic en **Modificar** junto a **Cuentas de Exchange ActiveSync**.



Haga clic en **Añadir** y especifique los datos de su cuenta de Exchange ActiveSync. Puede usar variables para determinados campos (seleccionar en la lista desplegable), como Usuario o Dirección de correo electrónico. Las variables se sustituirán por los valores reales de Usuarios del ordenador cuando se aplique una política.



• **Nombre de cuenta**: escriba el nombre de la cuenta de Exchange.

• **Host de Exchange ActiveSync**: especifique el nombre de host de la instancia de Exchange Server o su dirección IP.

• **Usar SSL**: esta opción está activada de forma predeterminada. Especifica si la instancia de Exchange Server utiliza la capa de sockets seguros (SSL) para autenticación.

• **Dominio**: este campo es opcional. Puede especificar el dominio al que pertenece esta cuenta.

• **Usuario**: nombre de conexión a Exchange. Seleccione la variable correspondiente en la lista desplegable para usar el atributo de Active Directory para cada usuario.

• **Dirección de correo electrónico**: seleccione la variable correspondiente en la lista desplegable para usar un atributo de Active Directory para cada usuario.

• **Contraseña**: opcional. Se recomienda dejar este campo en blanco. Si se deja en blanco, se pedirá a los usuarios que creen sus propias contraseñas.

• **Días anteriores de correo para sincronizar**: seleccione el número de días anteriores de correo para sincronizar desde la lista desplegable.

• **Certificado de la identidad**: credenciales de conexión a ActiveSync.

• **Permitir el movimiento de mensajes**: si esta opción está activada, los mensajes se pueden mover de una cuenta a otra.

• **Permitir la sincronización de direcciones recientes**: si esta opción está activada, el usuario podrá sincronizar las direcciones utilizadas recientemente en varios dispositivos.

• **Usar solo en Mail**: active esta opción si solo quiere permitir el uso de la aplicación Mail para enviar mensajes de correo electrónico saliente desde esta cuenta.

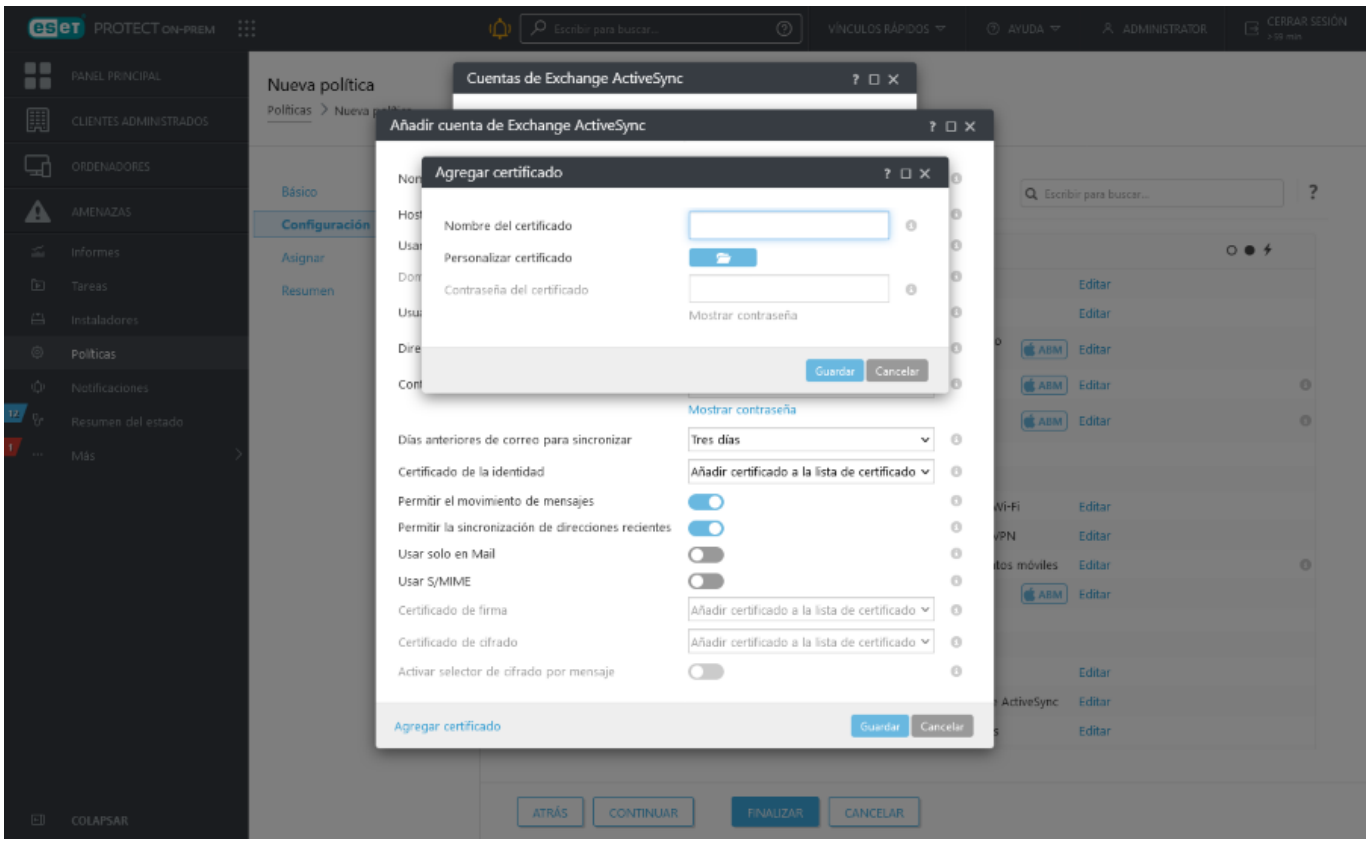
• **Usar S/MIME**: active esta opción para usar el cifrado S/MIME con los mensajes de correo electrónico salientes.

• **Certificado de firma**: credenciales para la firma de los datos MIME.

• **Certificado de cifrado**: credenciales para el cifrado de los datos MIME.

• **Activar selector de cifrado por mensaje**: permita al usuario elegir si desea cifrar cada mensaje.

Si no especifica un valor y deja el campo en blanco, se pedirá a los usuarios de los dispositivos móviles que introduzcan este valor. Por ejemplo una **Contraseña**.

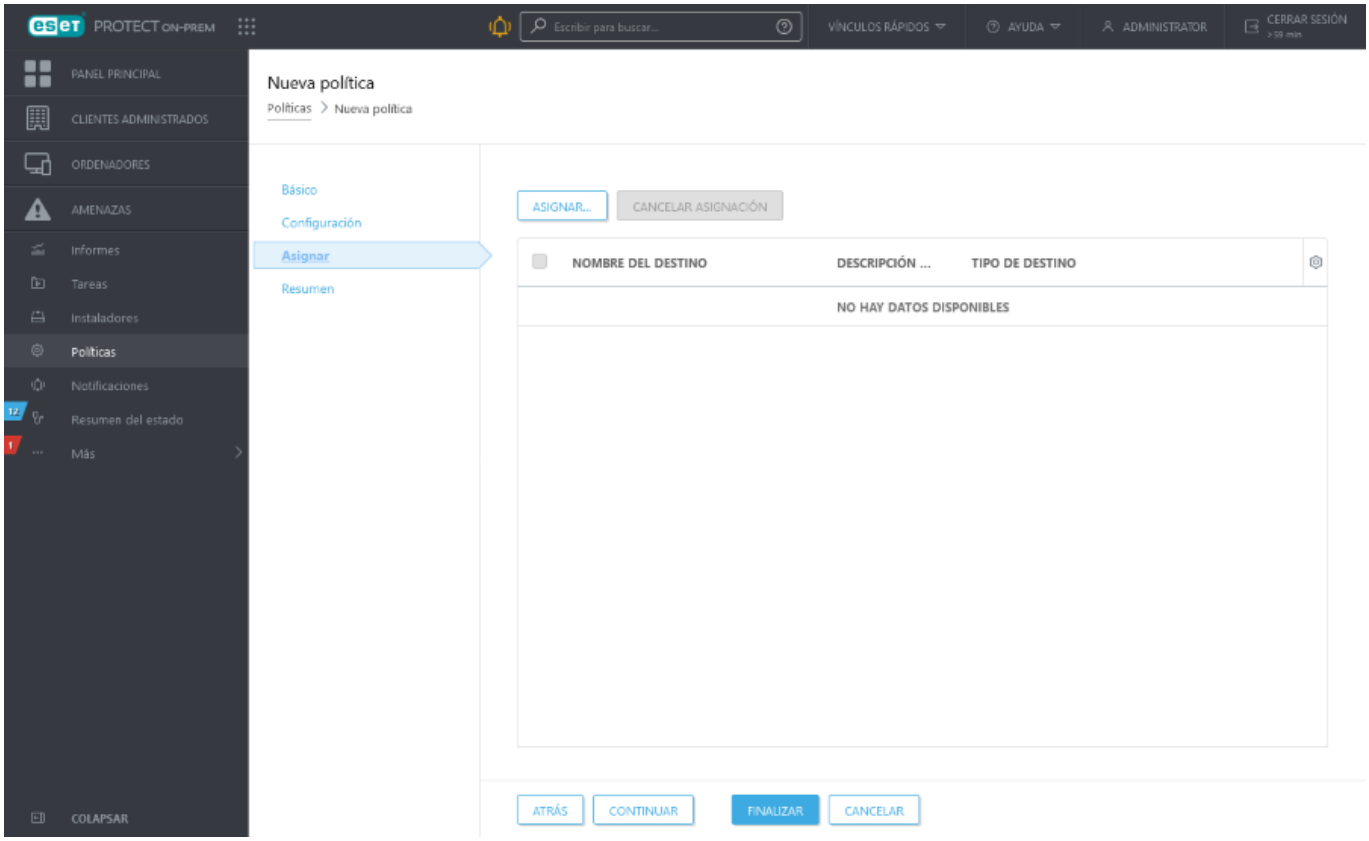


• **Agregar certificado**: puede añadir certificados de Exchange específicos (Identidad del usuario, Firma digital o Certificado de cifrado) en caso de ser necesario.

con los pasos anteriores puede añadir varias cuentas de Exchange ActiveSync, si lo desea. De esta forma habrá más cuentas configuradas en un dispositivo móvil. Si es necesario, también puede modificar las cuentas existentes.

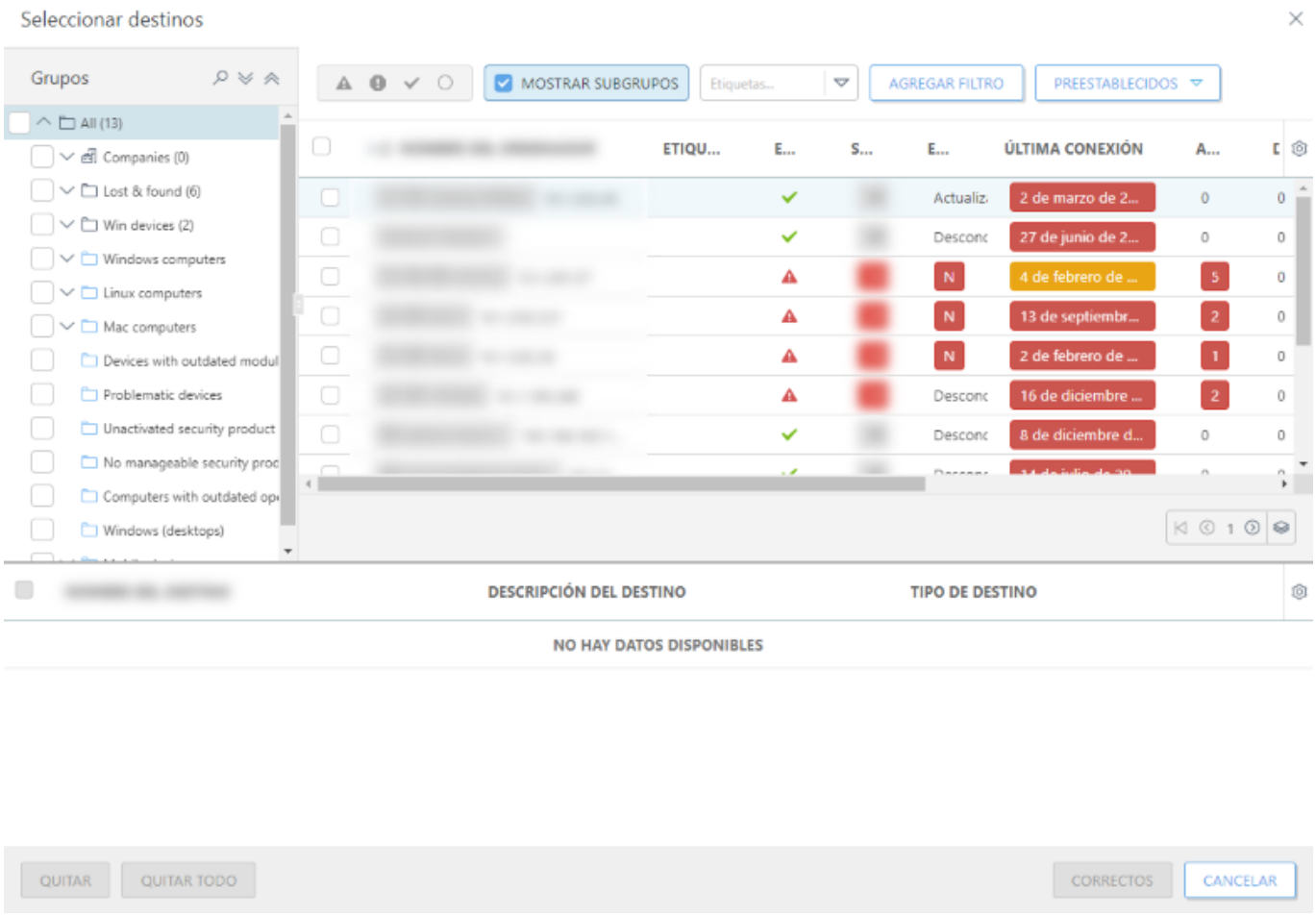
Asignar

Especifique los clientes (ordenadores individuales/dispositivos móviles o grupos enteros) que vayan a ser los destinatarios de esta política.



Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione los ordenadores o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**. La política se aplica a los destinos después de su siguiente conexión con ESET PROTECT Server (en función del intervalo de conexión del agente).

Crear una política para que MDC active APN/ABM para la inscripción de iOS

Cuando cambie el certificado HTTPS utilizado en su política para MDC, siga estos pasos para que los dispositivos móviles no se desconecten de su MDM:
1. Cree y aplique la nueva política que utiliza el nuevo certificado HTTPS.
2. Permita que los dispositivos se registren en el servidor MDM y reciban la nueva política.
3. Verifique que los dispositivos utilicen el nuevo certificado HTTPS (que se haya completado el intercambio del certificado HTTPS).
4. Espere 72 horas como mínimo a que sus dispositivos reciban la nueva política. Cuando todos los dispositivos hayan recibido la nueva política (la alerta del núcleo MDM "El cambio de certificado HTTPS está en curso. Todavía se está utilizando el certificado antiguo" ya no aparece en la ficha Alertas), puede eliminar la política anterior.

Este es un ejemplo de cómo crear una nueva política para que el Conector de dispositivo móvil de ESET active APNS (Apple Push Notification Services) y la función Programa de inscripción de dispositivos iOS. Es una acción obligatoria para inscribir dispositivos iOS. Antes de configurar esta directiva, cree un nuevo certificado APN y obtenga la firma de Apple en el Portal de certificados push de Apple para que se convierta en un certificado

firmado o en un **Certificado de APNS**. Para instrucciones detalladas, consulte la sección Certificado de APN.

Básico

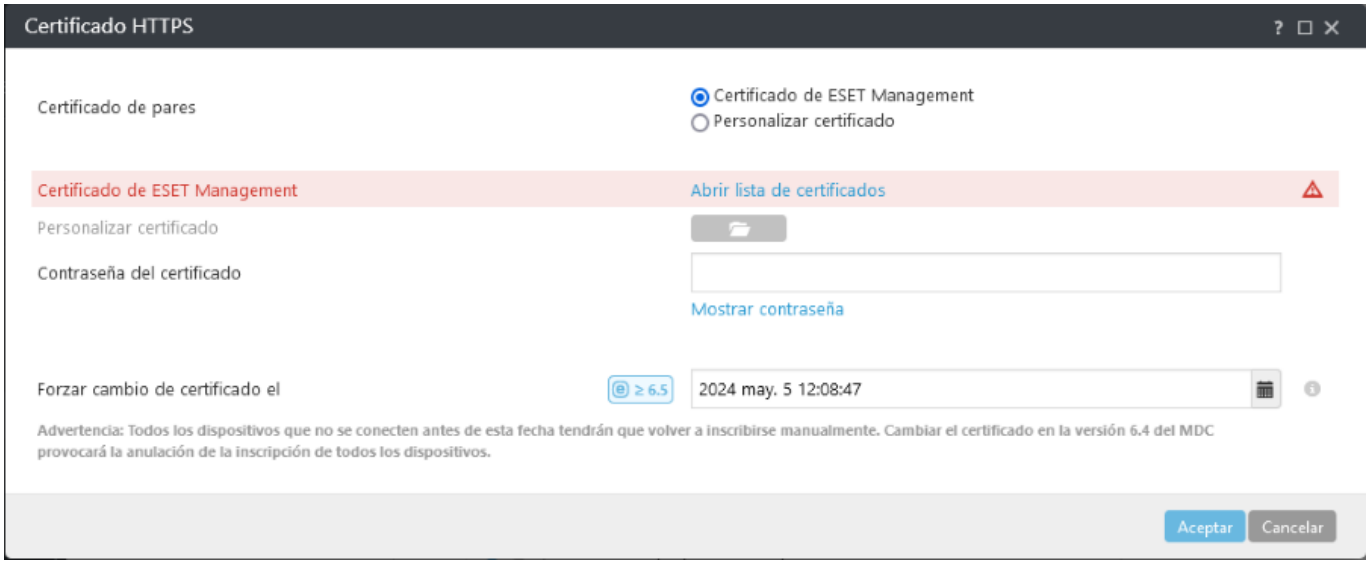
Escriba el **Nombre** de esta política. El campo **Descripción** es opcional.

Configuración

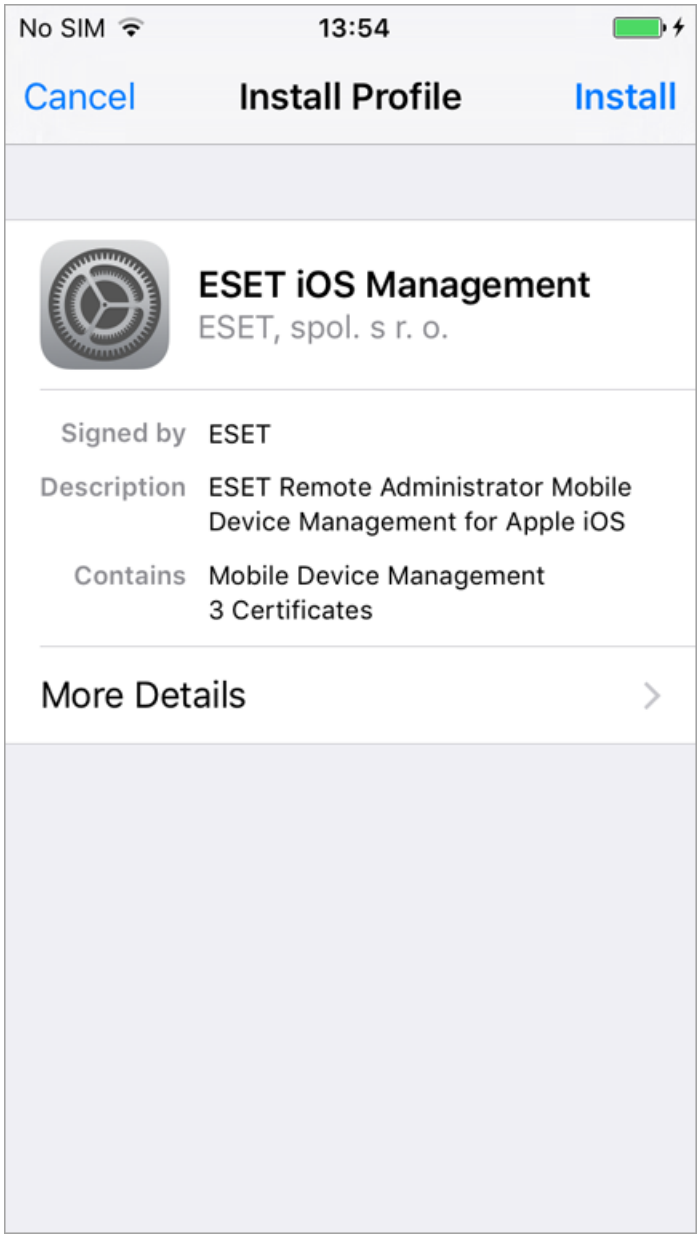
Seleccione **Conector de dispositivo móvil de ESET** en la lista desplegable.

Si instaló el servidor MDM con el instalador todo en uno (no de forma independiente y no como componente), el certificado HTTPS se generó automáticamente durante la instalación. En todos los demás casos, debe aplicar un certificado HTTPS personalizado. Puede consultar más información anotada tras el paso uno del tema Administración de dispositivos móviles.
Puede utilizar el certificado ESET PROTECT (firmado por la CA ESET PROTECT On-Prem) o su certificado personalizado. También puede especificar la fecha en la que **Forzar cambio de certificado**. Haga clic en la sugerencia situada junto a este ajuste para obtener más información.

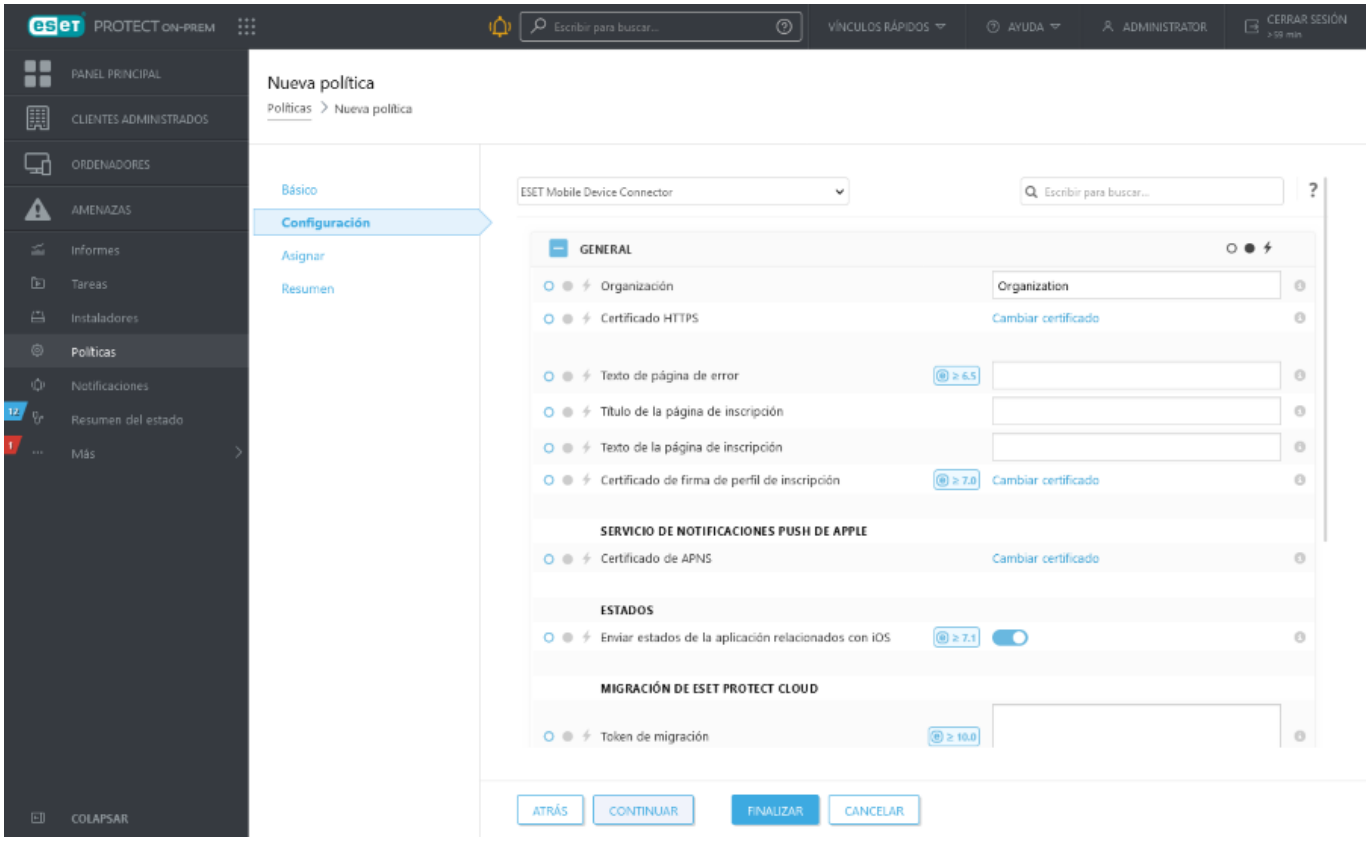
Escriba el nombre de su organización sobre la cadena **Organización**. El generador de perfiles de inscripción usa este dato para incluir esta información en el perfil.



En **General** puede cargar su certificado HTTPS de inscripción en el **Certificado de firma de perfil de inscripción** (esto solo afecta a la inscripción que no es ABM). Esto permitirá firmar la página de inscripción para dispositivos iOS que visitan durante el proceso de inscripción y que estén visibles en el campo **Firmado por** según el certificado.

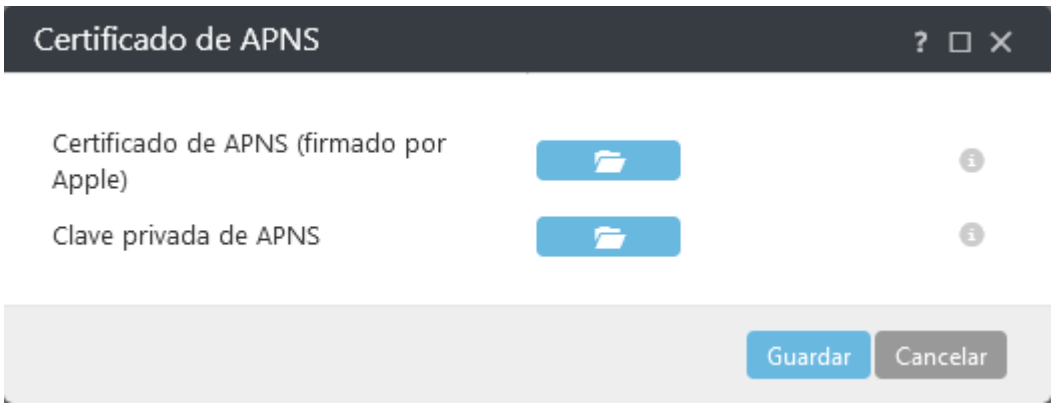


Cargar los certificados de Apple para la inscripción de iOS: vaya a Apple Push Notification Service y cargue el Certificado de APNS y una Clave privada de APNS.



Certificado de APNS (firmado por Apple): haga clic en el icono de la carpeta y busque el Certificado de 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 el icono de 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 de APN/ABM.



Programa para la mejora del producto: active o desactive la transmisión de informes de bloqueo y datos de telemetría anónimos a ESET.

Nivel de detalle de seguimiento de registros: establezca el nivel de detalle del registro para determinar la cantidad de información que se recogerá y registrará de **Trazar** (datos meramente informativos) a **Fatal** (la información más importante).

Si crea esta política para la inscripción de iOS con el ABM de Apple, desplácese hasta **Apple Business Manager (ABM)**.

Apple Business Manager (ABM): estos ajustes son exclusivos de ABM.

Si se cambia cualquiera de estos ajustes tras la configuración inicial, para aplicar los cambios tendrá que restablecer los valores predeterminados de fábrica de los dispositivos iOS afectados e inscribirlos de nuevo.

Cargar token de autorización: haga clic en el icono de la carpeta y busque el token del servidor ABM. El token del servidor ABM es el archivo que descargó al crear el servidor MDM virtual en el portal de ABM de Apple.

Instalación obligatoria: el usuario no podrá utilizar el dispositivo sin instalar el perfil de MDM.

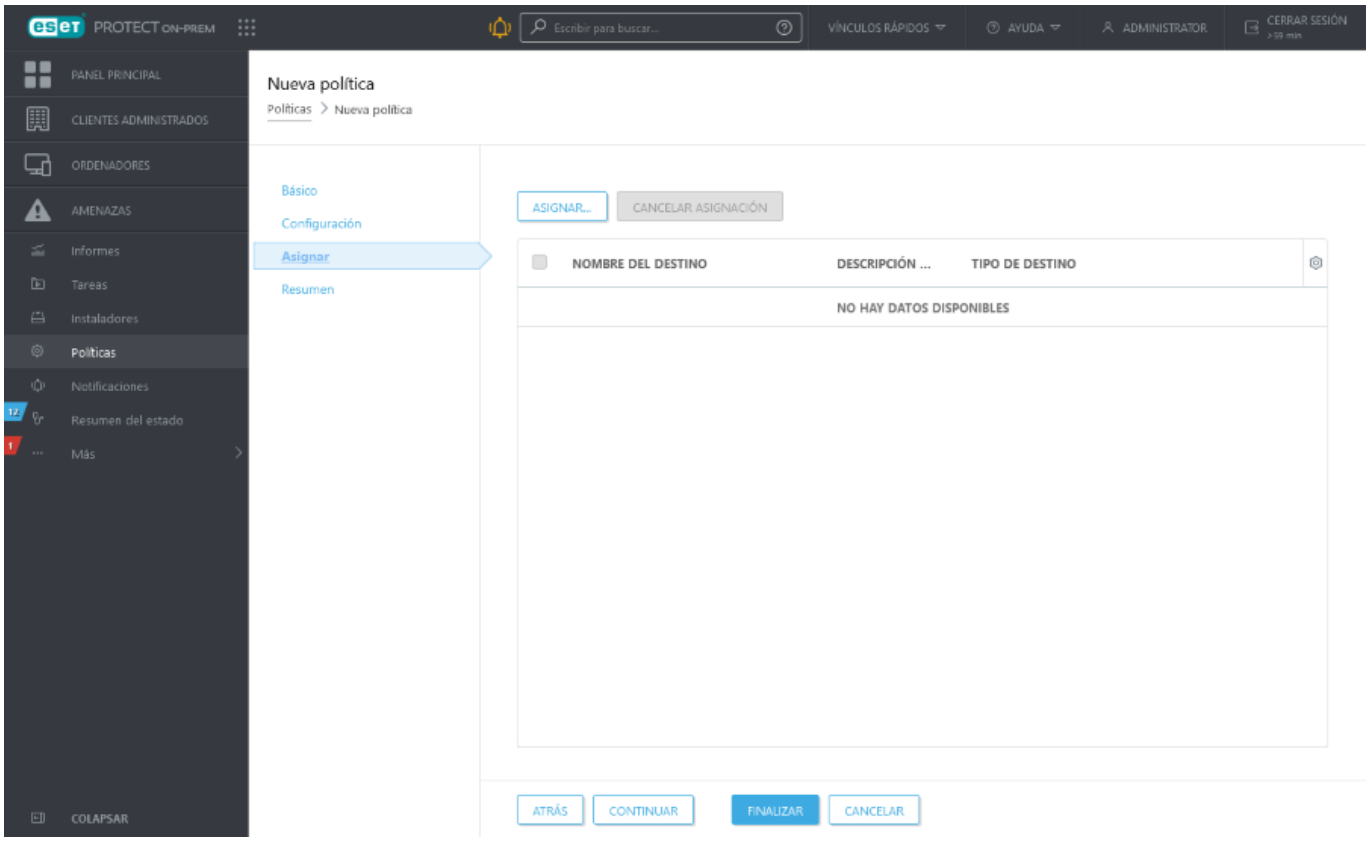
Permitir al usuario quitar el perfil de MDM: el dispositivo debe estar en modo supervisado para impedir que el usuario quite el perfil de MDM.

Requerir inicio de sesión en dominio: el usuario debe utilizar credenciales de dominio válidas en el asistente de configuración de dispositivos.

Omitir elementos de configuración: este ajuste le permite decidir qué pasos de la configuración inicial se omitirán durante la configuración inicial de iOS. Puede encontrar más información sobre cada uno de estos pasos en el artículo de la base de conocimiento de Apple.

Asignar

Seleccione el dispositivo que aloja el servidor MDM al que va dirigida la política.



Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione la instancia del Conector del dispositivo móvil a la que quiera aplicar la política y haga clic en **Aceptar**.

Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**.

Crear una directiva para aplicar restricciones a iOS y añadir conexión Wi-Fi

Puede crear una directiva para aplicar determinadas restricciones a dispositivos móviles con iOS. También puede definir varias conexiones Wi-Fi para que, por ejemplo, los usuarios se conecten automáticamente a la red Wi-Fi corporativa de distintas sucursales. Lo mismo se aplica a las conexiones VPN.

Las restricciones que puede aplicar al dispositivo móvil con iOS se clasifican en categorías. Por ejemplo, puede desactivar FaceTime y el uso de la cámara, desactivar determinadas funciones de iCloud, realizar un ajuste preciso de las opciones de seguridad y privacidad, o desactivar determinadas aplicaciones.

> Las restricciones que pueden o no aplicarse dependen de la versión de iOS utilizada por los dispositivos cliente. Se admiten las versiones iOS 8.x y más recientes.

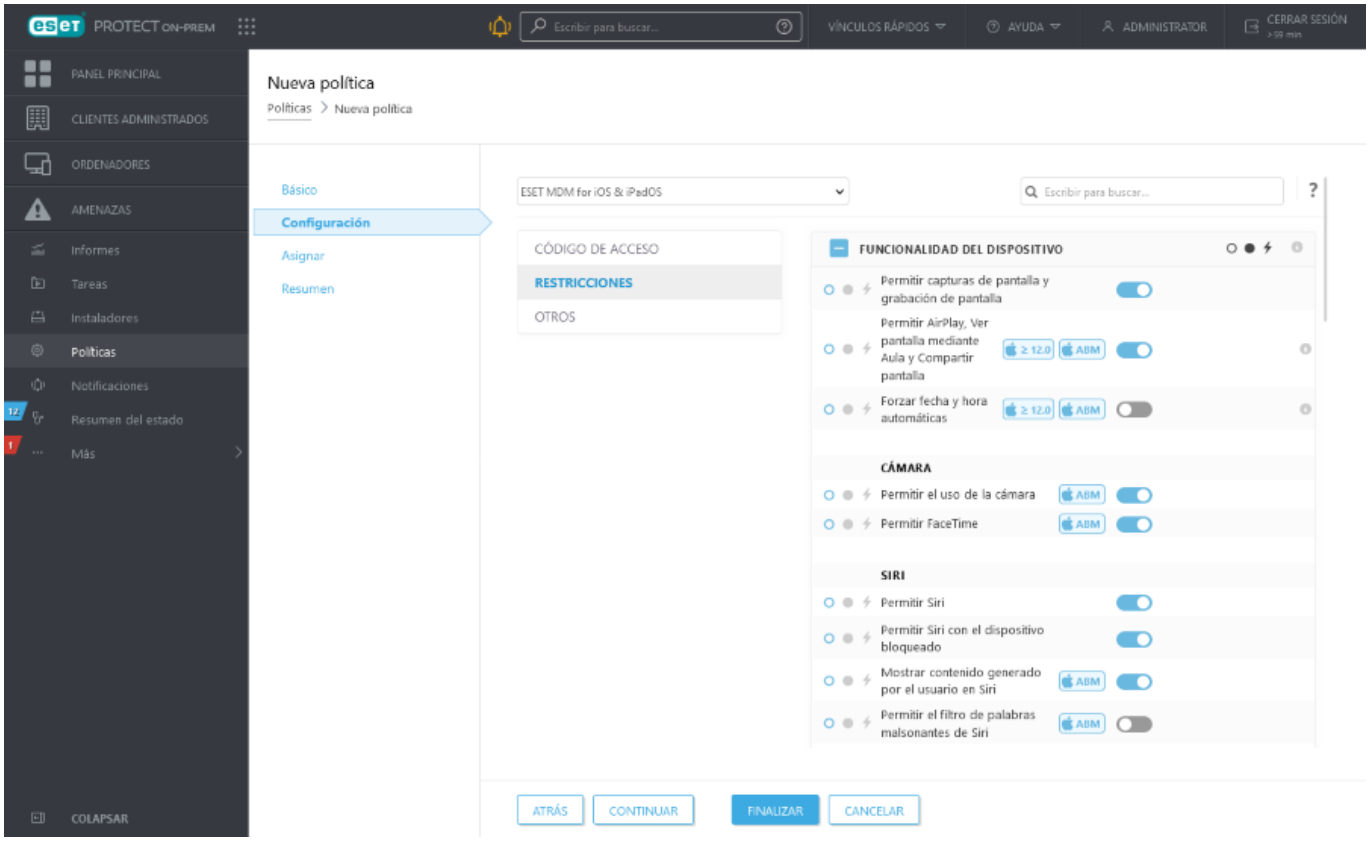
A continuación se muestra un ejemplo de cómo desactivar las aplicaciones **Cámara** y **FaceTime** y añadir los detalles de la conexión Wi-Fi para que el dispositivo móvil iOS se conecte a una red Wi-Fi siempre que la red se detecte. Si utiliza la opción Unirse automáticamente, los dispositivos móviles iOS se conectarán a esta red de forma predeterminada. La configuración de la directiva anulará la selección manual de una red Wi-Fi por parte del usuario.

Básico

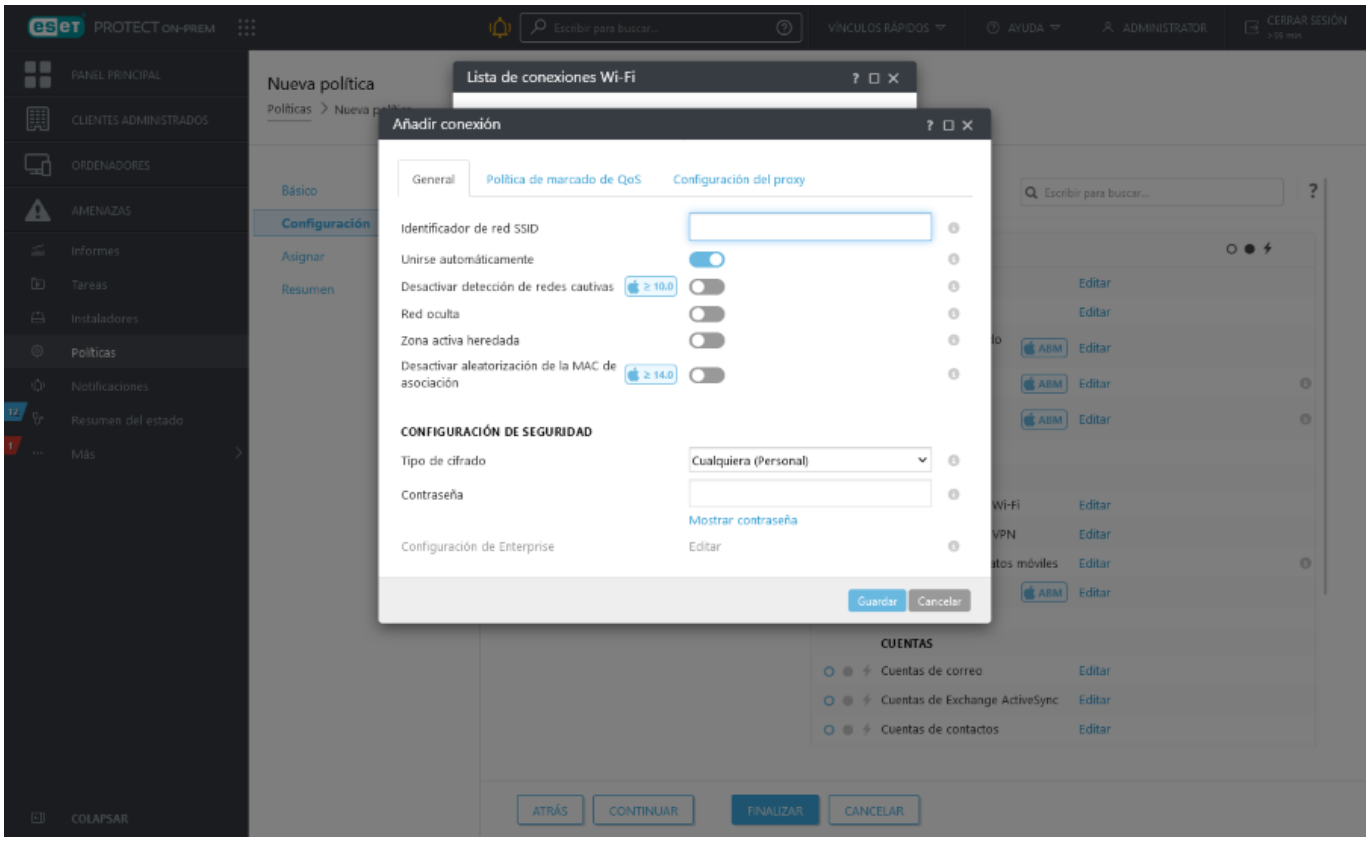
Escriba el **Nombre** de esta directiva. El campo **Descripción** es opcional.

Configuración

Seleccione **ESET MDM para iOS/iPadOS** y haga clic en **Restricciones** para ver las categorías. Utilice el conmutador de alternancia situado junto a **Permitir el uso de la cámara** para desactivar esta opción. Como la cámara está desactivada, FaceTime se desactivará automáticamente también. Si desea desactivar únicamente FaceTime, deje activada la cámara y utilice el conmutador de alternancia situado junto a **Permitir FaceTime** para desactivarlo.



Una vez configuradas las **Restricciones**, haga clic en **Otros** y, a continuación, en **Modificar** junto a **Lista de conexiones Wi-Fi**. Se abrirá una ventana con la lista de conexiones Wi-Fi. Haga clic en **Agregar** y especifique los detalles de conexión de la red Wi-Fi que quiera añadir. Haga clic en **Guardar**.



- **Identificador de red SSID**: SSID de la red Wi-Fi que se va a utilizar.
- **Unirse automáticamente**: opcional (activado de forma predeterminada), el dispositivo se une a esta red

automáticamente.

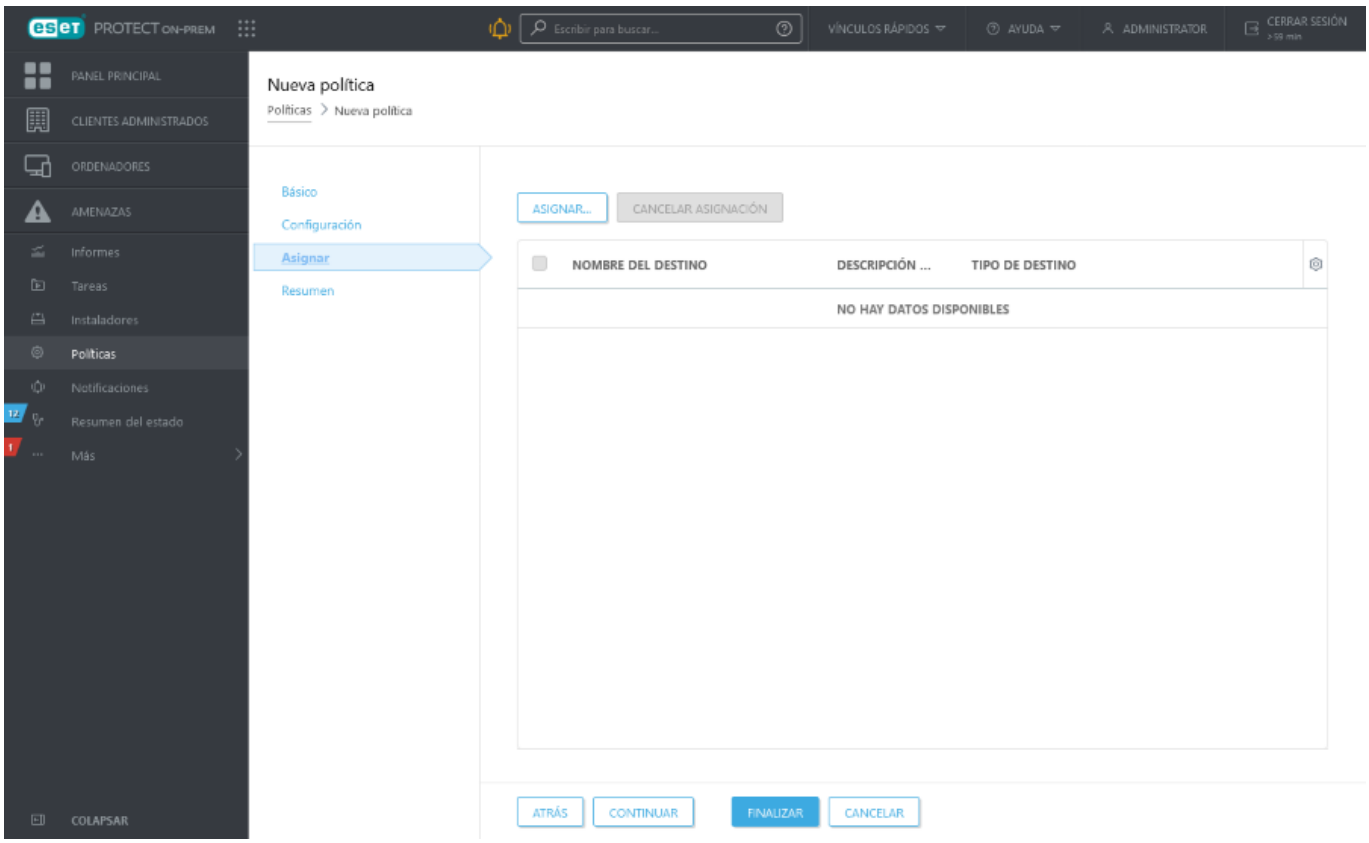
Configuración de seguridad

- **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 utilizará para la autenticación al conectarse a la red Wi-Fi.

Configuración de proxy: opcional. Si su red usa un proxy, especifique los valores correspondientes.

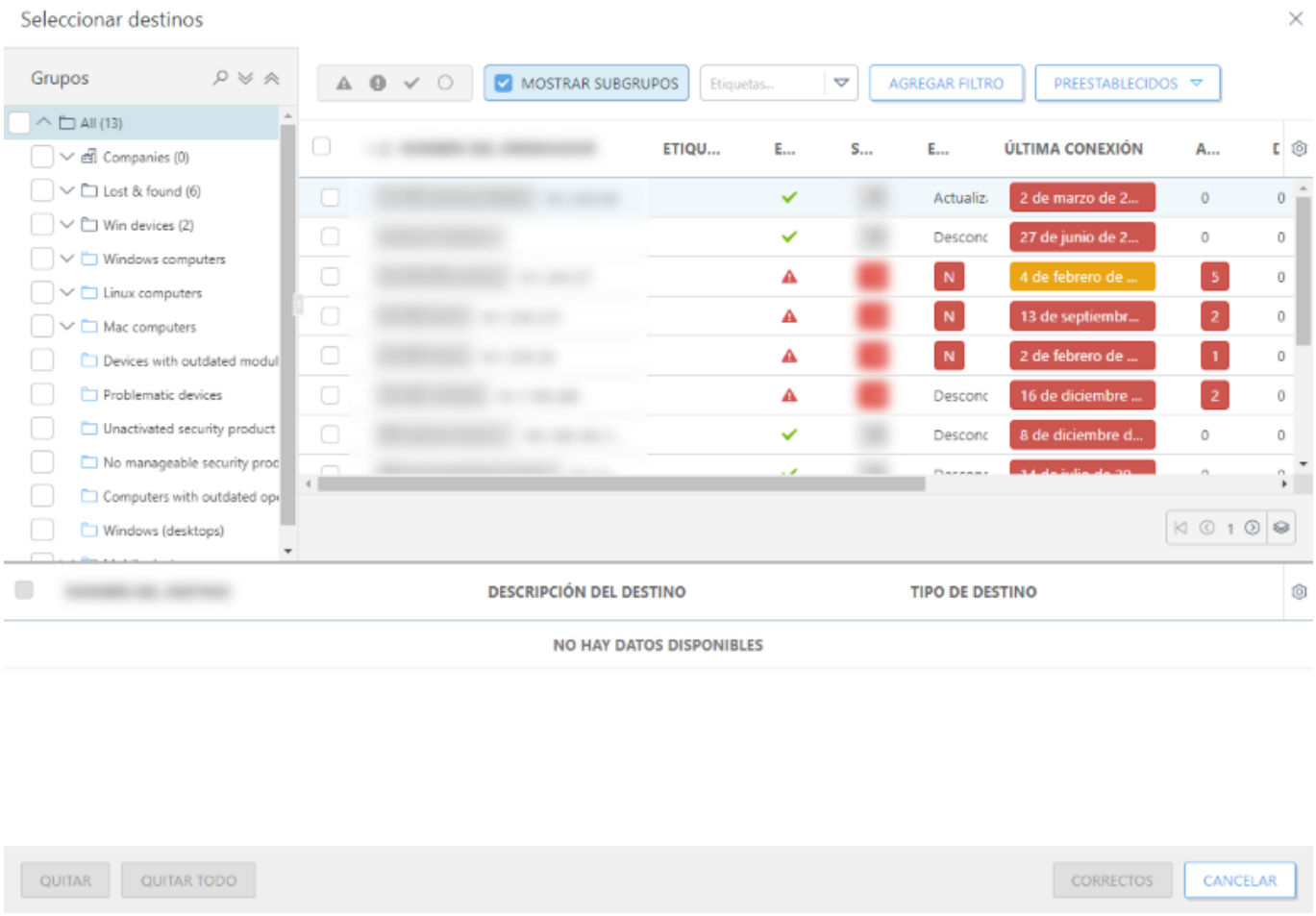
Asignar

Especifique los clientes (ordenadores individuales/dispositivos móviles o grupos enteros) que vayan a ser los destinatarios de esta política.



Haga clic en **Asignar** para mostrar todos los grupos estáticos y dinámicos así como sus miembros. Seleccione los ordenadores o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los ordenadores de un grupo, asigne el grupo en lugar de ordenadores individuales para evitar que Web Console se ralentice.
Web Console muestra una advertencia si selecciona un gran número de ordenadores.



Resumen

Revise las opciones de esta directiva y haga clic en **Finalizar**. La política se aplica a los destinos después de su siguiente conexión con ESET PROTECT Server (en función del intervalo de conexión del agente).

Perfiles de configuración del MDM

Puede configurar el perfil para imponer directivas y restricciones en el dispositivo móvil gestionado.

Nombre del perfil	Descripción breve
Código de acceso	Obliga a los usuarios finales a proteger sus dispositivos con códigos de acceso cada vez que quieren desactivar el estado de suspensión. Así, la información corporativa confidencial de los dispositivos gestionados permanecerá protegida. Si varios perfiles exigen códigos de acceso en un solo dispositivo, se aplicará la directiva más restrictiva.
Restricciones	Los perfiles de restricción limitan las funciones disponibles para los usuarios de los dispositivos gestionados mediante la restricción del uso de permisos específicos relacionados con la funcionalidad del dispositivo, las aplicaciones, iCloud, la seguridad y la privacidad.
Lista de conexiones Wi-Fi	Los perfiles Wi-Fi envían los ajustes Wi-Fi corporativos directamente a los dispositivos administrados para un acceso instantáneo.

Nombre del perfil	Descripción breve
Lista de conexiones VPN	Los perfiles de VPN envían la configuración de la red privada virtual corporativa a los dispositivos corporativos para que los usuarios puedan acceder a la infraestructura corporativa desde ubicaciones remotas de forma segura. **Nombre de la conexión**: permite ver el nombre de la conexión mostrado en el dispositivo. **Tipo de conexión**: seleccione el tipo de conexión que permite este perfil. Cada tipo de conexión permite funciones distintas. **Servidor**: introduzca el nombre de host o la dirección IP del servidor al que se está estableciendo conexión.
Cuentas de correo	Permite al administrador configurar las 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 push corporativa. Tenga en cuenta que hay campos con valores de consultas previamente cumplimentados y opciones que solo se aplican a iOS versión 5 y superiores.
CalDAV: cuentas de calendario	CalDAV ofrece opciones de configuración para permitir a los usuarios finales sincronizar inalámbricamente con el servidor CalDAV de la empresa.
CardDAV: cuentas de contactos	Esta sección permite la configuración concreta de los servicios de CardDAV.
Cuentas de calendario suscritas	Los calendarios suscritos proporcionan configuración de calendarios.

Control de acceso web para Android

Utilice ESET Endpoint Security for Android para regular el acceso a sitios web desde sus dispositivos Android administrados. El control de acceso 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 de acceso web para Android es compatible con ESET Endpoint Security para Android versión 3.0 y posteriores.

De forma predeterminada, el control de acceso web está desactivado. Para activarlo, tendrá que 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 de acceso web y active el botón de alternancia **Control de acceso web**.
4. Vínculos o categorías específicos de las listas blanca y negra.

Reglas del control de acceso web

Utilice la política Control de acceso web para especificar una lista de URL para tres categorías distintas:

- **Lista negra**: bloquear la URL sin opción ni acceso.
- **Lista blanca**: permitir acceso a la URL.
- **Advertencia**: advierte al usuario sobre la URL, pero ofrece una opción de acceso

Cada uno de estos apartados se puede administrar con las siguientes acciones:

- **Agregar**: agregar un registro nuevo con una dirección URL concreta.
- **Modificar**: editar una dirección URL existente.
- **Quitar**: eliminar un informe existente de una dirección URL.
- **Importar**: importar una lista de direcciones URL nuevas en la categoría.
- **Exportar**: exportar una lista de direcciones URL de la categoría seleccionada.

> En el caso de reglas que controlen el acceso a un sitio web determinado, introduzca la URL completa en el campo **URL**.
> Los símbolos especiales * (asterisco) y ? (signo de interrogación) se pueden usar en el campo de 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/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 de URL específica y especifique qué subcategoría se debe ver afectada:

- **Permitir**: permitir el acceso a la URL desde una categoría seleccionada.
- **Bloquear**: bloquear el acceso a la URL desde una categoría seleccionada.
- **Advertir**: advertir al usuario sobre la URL de una categoría seleccionada.

Administración de actualizaciones del sistema operativo

ESET Endpoint Security para Android permite a un administrador gestionar las actualizaciones del sistema operativo Android en dispositivos Android administrados.

> Esta funcionalidad requiere ESET Endpoint Security for Android versión 3.0 y Android versión 8.x o posteriores, y el dispositivo Android debe estar inscrito en un 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 el ajuste **Activar la 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 este apartado 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 periodo de tiempo**: 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 durante los que los dispositivos no se puedan actualizar.

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 el ajuste de cualquier política (y se puede utilizar en aquellos casos en los que la política no se pueda entregar). Si se reconoce, se genera la línea "Setting log level from loggerLevel.cfg override file to XYZ"en el registro de seguimiento (nivel de información). Valores reconocidos: all, trace, debug, information, warning, error, critical, fatal. Cuando está configurado 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*	Registros de bloqueos que aún no se han enviado al servicio ESET CrashReporting.
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 gzipped numerados 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 gzipped numerados 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.
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 se está utilizando o no es válido.

Es probable que esté intentando repetir la inscripción con un token de inscripción antiguo. Cree un nuevo token de repetición de la inscripción en la Consola web y utilícelo. También es posible que esté intentado una segunda repetición de la inscripción demasiado pronto después de la primera. Compruebe que el token de repetición de la inscripción sea diferente del primero. Si no lo es, espere unos minutos e intente otra vez generar un nuevo token de repetición de la inscripción.

Ha fallado la validación del certificado del servicio

En este mensaje de error se indica que hay un problema con su certificado de servidor APNS o FCM. Esto se anuncia en la Consola web de ESET PROTECT como una de las siguientes advertencias en las alertas del núcleo de MDM:

- **Ha fallado la validación del certificado del servicio FCM** (0x0000000100001002)
- **Ha fallado la validación del certificado del servicio APNS** (0x0000000100001000)
- **Ha fallado la validación del certificado del servicio de respuesta de APNS** (0x0000000100001004)

Asegúrese de contar con la autoridad de certificado correcta disponible en el sistema:

- Autoridad certificadora APNS: **Autoridad certificadora Entrust**, necesaria para validar certificados de gateway.push.apple.com:2195;
- Autoridad certificadora de respuesta de APNS: **Autoridad certificadora Entrust**, necesaria para validar certificados de feedback.push.apple.com:2196;
- Autoridad certificadora FCM: **GeoTrust Global CA**, necesaria para validar certificados de android.googleapis.com:443.

La autoridad certificadora deseada se debe incluir en el almacén de certificados de la máquina host de MDM. Si se trata de un sistema Windows, puede buscar "Administrar certificados raíz de confianza". Si se trata de un sistema Linux, la ubicación del certificado depende de la distribución utilizada. Algunos ejemplos de destinos de almacenes de certificados:

- en Debian, CentOS: */usr/lib/ssl/cert.pem*, */usr/lib/ssl/certs*;
- en Red Hat: */usr/share/ssl/cert.pem*, */usr/share/ssl/certs*;
- el comando `openssl version -d` suele devolver la ruta deseada.

Si la autoridad certificadora deseada no se encuentra instalada en el sistema en el que se está ejecutando el núcleo MDM, instálela. Tras la instalación, reinicie el servicio ESET PROTECT MDC.

Tenga cuidado, ya que la validación del certificado es una función de seguridad. Si la advertencia se da en Web Console, también puede indicar una amenaza para la seguridad.

Herramienta de migración de MDM

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 ESET PROTECT funcional
- Cuenta de ESET PROTECT con privilegios de **Superusuario**

Limitaciones

- Esta migración está disponible solo 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 ESET PROTECT Web Console.

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 de tokens**: puede limitar el número de dispositivos que se pueden migrar con el token de migración.

Si administra un gran número de dispositivos móviles, le recomendamos intentar en primer lugar el proceso de migración con un número reducido de dispositivos para comprobar que la migración no tenga ningún problema. Después podrá continuar con la migración de los restantes dispositivos móviles administrados.

6. Seleccione **Generar token** para generar un token de migración con parámetros establecidos para el proceso de migración.

El token generado es válido durante 14 días y solo está disponible mientras usted permanece en la página. No cierre ni actualice la página antes de copiar el token.

7. El token de migración aparece como una cadena de caracteres en el siguiente campo. 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**, introduzca 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 a partir de este momento. Asegúrese de que todos sus dispositivos móviles administrados puedan conectarse al servidor mientras el token de migración sea válido (durante los 14 días siguientes). Si un dispositivo móvil administrado no se conecta al servidor durante este periodo, no se migrará, y usted tendrá que repetir el procedimiento de migración.

15. Puede supervisar el proceso de migración en ESET PROTECT Web Console. Una vez migrado el dispositivo móvil, se conectará a ESET PROTECT, y será visible en la sección **Ordenadores** de ESET PROTECT Web Console.

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 del servicio el componente MDM.

ESET PROTECT On-Prem para proveedores de servicios administrados (MSP)

¿Qué es un MSP?

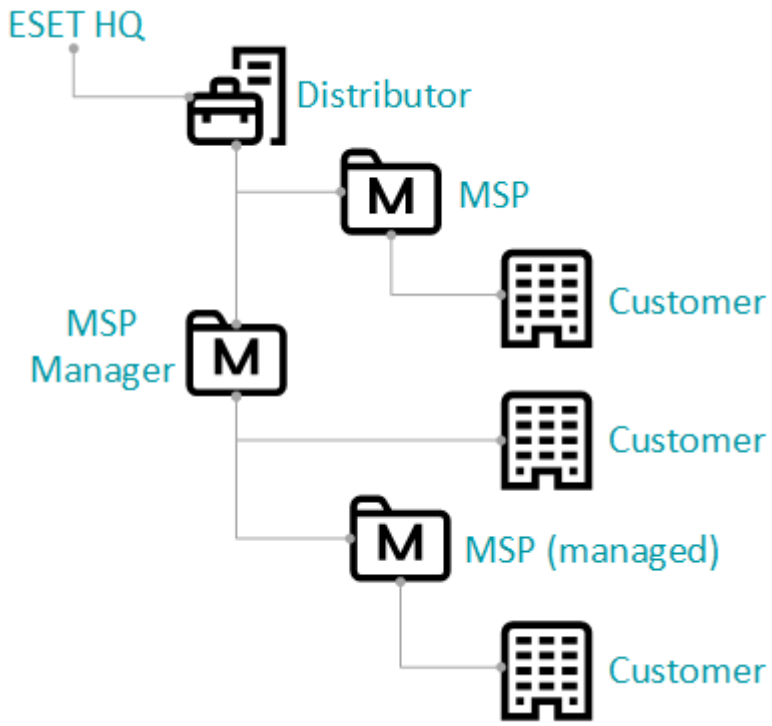
La abreviatura MSP hace referencia a "Proveedor de servicios administrados". Los usuarios MSP ofrecen servicios de TI a sus clientes, por ejemplo, la administración de sus productos de seguridad (como ESET Endpoint Antivirus).

- Los usuarios MSP tienen distintos requisitos y distintas formas de usar ESET PROTECT On-Prem que, por ejemplo, los usuarios de grandes empresas o de pymes (pequeñas y medianas empresas). Consulte las situaciones de implementación para MSP recomendadas.

- 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 Managed Service Provider de ESET.

La estructura de las entidades en los MSP

ESET PROTECT On-Prem sincroniza su estructura de ESET MSP Administrator con el árbol de grupos estáticos de **Ordenadores** en Web Console.



- **Distribuidor**: un distribuidor es un socio de ESET y un socio de un MSP o responsable de MSP.
- **Responsable de MSP**: administra las distintas empresas MSP. Un responsable de MSP también puede tener clientes directos.
- **MSP**: los destinatarios de esta guía. Un MSP proporciona servicios a sus clientes. Por ejemplo, MSP: administra los ordenadores de sus clientes de forma remota e instala y administra productos de ESET.
- **MSP administrado**: es similar a un MSP, pero está administrado por un responsable de MSP.
- **Cliente**: el usuario final de las licencias de productos de ESET. El cliente no debe interactuar con los productos de ESET. El cliente puede tener diferentes estados marcados con un icono:
  - 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 de Clientes administrados del menú principal de ESET PROTECT On-Prem.

Características específicas de los entornos MSP

En el modelo de negocio de los MSP se usa una configuración de infraestructura distinta de la que se utiliza en una empresa o una pyme. En el entorno MSP, los clientes suelen ubicarse fuera de la red de la empresa MSP. El propio ESET PROTECT Server puede alojarse también fuera de la empresa MSP. Las instancias de ESET Management Agent deben tener conectividad directa con ESET PROTECT Server mediante una red pública de Internet. Las configuraciones recomendadas del servidor ESET PROTECT para MSP son:

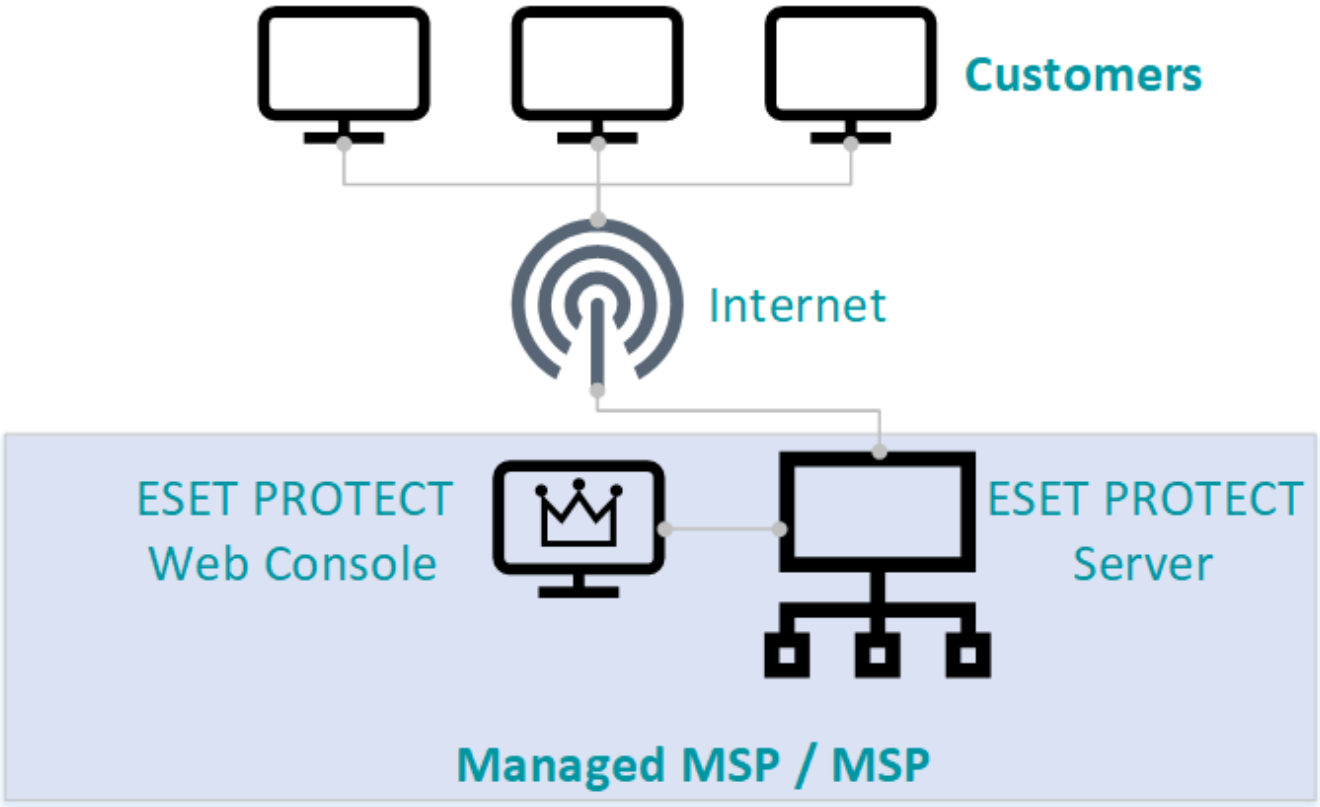
- Alojado en una nube pública.

- Alojado en la nube privada de un MSP (tendrá que abrir algunos puertos para que ESET PROTECT On-Prem sea visible desde Internet).

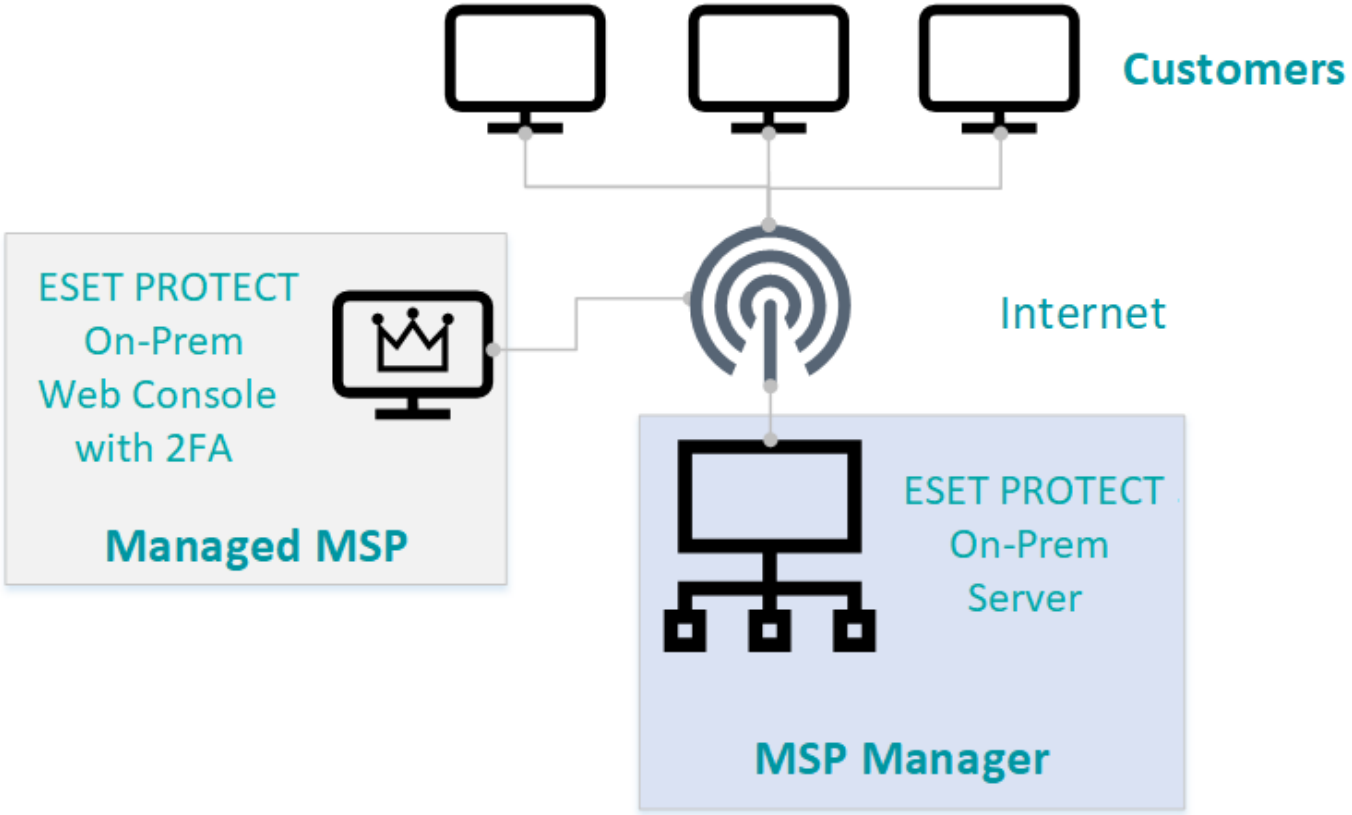
- Alojado en la red privada de un MSP (use el proxy HTTP para reenviar las conexiones de Internet si el servidor no está visible de forma directa.)

Configuración básica

- **Configuración centralizada**: los clientes acceden a ESET PROTECT Server desde Internet. Es posible que solo se pueda acceder a ESET PROTECT Web Console desde la red de la empresa MSP.



- **Configuración distribuida**: los clientes acceden a ESET PROTECT Server desde Internet. El MSP puede acceder a ESET PROTECT Web Console desde 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 MSP

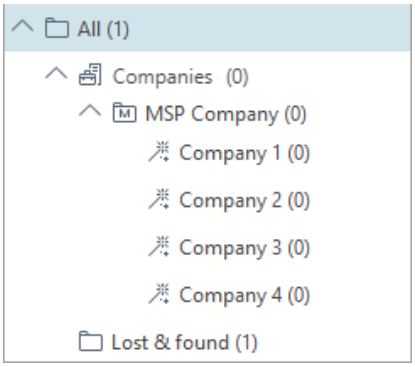
ESET PROTECT On-Prem ofrece un conjunto de funciones centradas en los usuarios MSP. Todas las funciones relacionadas con MSP se activan después de importar una cuenta de EMA 2 en ESET PROTECT On-Prem.

Asistente de instalación de clientes

La función MSP principal en ESET PROTECT On-Prem . es la configuración de clientes MSP. Esta función le ayuda a crear usuarios y un instalador personalizado de ESET Management Agent para su cliente.

Árbol MSP

Después de importar la cuenta de EMA 2, ESET PROTECT On-Prem se sincroniza con el Portal de ESET MSP (EMA 2) y crea el árbol MSP. El árbol MSP es una estructura del menú Ordenadores que representa la estructura de las empresas de su cuenta de EMA 2. Los elementos de los árboles MSP usan iconos diferentes a los iconos estándar de los dispositivos y grupos de ESET PROTECT On-Prem. No puede modificar la estructura del árbol MSP en Web Console. Solo podrá empezar a modificar y quitar clientes del árbol cuando haya quitado la cuenta de EMA 2 de la Administración de licencias. Si se suspende una empresa en EMA 2, no se quita la empresa del árbol MSP en ESET PROTECT On-Prem.

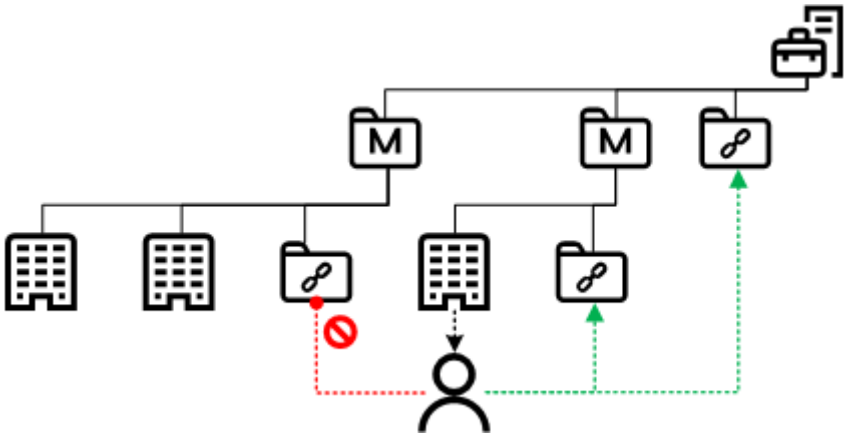


Grupo Objetos compartidos

Tras la sincronización de la cuenta MSP, ESET PROTECT On-Prem crea el árbol MSP. Hay un grupo de acceso de **Objetos compartidos** para cada MSP y cada responsable 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

ordenadores en **Objetos compartidos**. Los **Objetos compartidos** no están visibles en **Grupos** en **Ordenadores**. Los MSP pueden compartir objetos, como políticas y tareas, desde el grupo de acceso **Objetos compartidos**.

Todos los usuarios MSP creados mediante el asistente de instalación para empresas tienen acceso de lectura y uso a todos los grupos de **Objetos compartidos** por encima del usuario. Puede inspeccionar los Conjuntos de permisos asignados al usuario para ver la lista de grupos de acceso. Los usuarios solo pueden acceder a grupos ascendentes de Objetos compartidos, y no a grupos de responsables de MSP paralelos.



Clientes administrados

Después de sincronizar la cuenta MSP, el usuario MSP puede ver la lista de clientes administrados en la sección de Clientes administrados del menú principal de ESET PROTECT On-Prem.

ESET PROTECT certificados y MSP

Cuando importa la cuenta de EMA 2 en ESET PROTECT On-Prem, ESET PROTECT Server crea una nueva autoridad certificadora (CA) de MSP. La autoridad certificadora de MSP se almacena en el grupo estático **Objetos compartidos**, en el grupo raíz de MSP. Solo hay una autoridad certificadora de MSP, aunque importe varias cuentas. Si quita la autoridad certificadora de MSP, ESET PROTECT On-Prem creará una nueva autoridad certificadora de MSP tras la próxima sincronización con los servidores de la licencia. La sincronización se produce de forma automática una vez al día.

ESET PROTECT On-Prem crea un nuevo certificado de igual para Agent después de configurar una empresa con el asistente de instalación de clientes. La autoridad certificadora de MSP firma estos certificados de iguales. Cada certificado se etiqueta con el nombre de la empresa. La creación de certificados independientes para cada empresa mejora la seguridad global.

Si quita una autoridad certificadora, todos los ordenadores que usen certificados firmados por dicha autoridad dejarán de conectarse a ESET PROTECT Server. Sería necesario volver a implementar ESET Management Agent de forma manual.

MSP en Resumen del estado

Podrá acceder a la nueva ventana dinámica de MSP en Resumen del estado después de importar la cuenta de EMA 2. La ventana dinámica de MSP muestra información básica sobre su cuenta.

Proceso de implementación para MSP

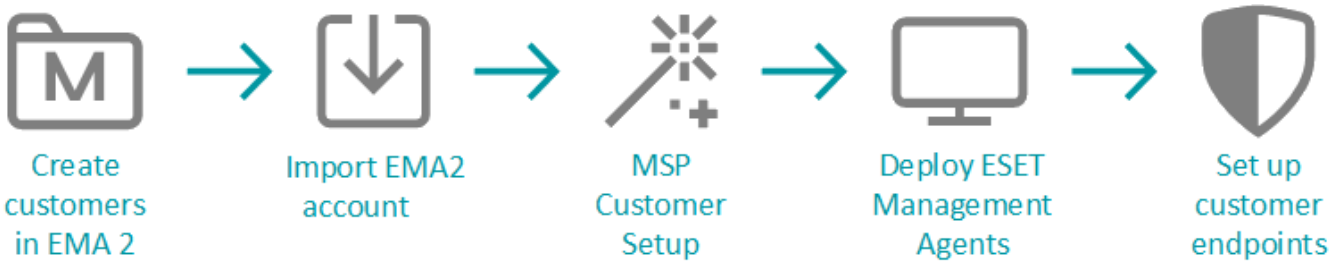
Si no tiene ESET PROTECT On-Prem instalado, le recomendamos usar el instalador todo en uno de Windows y seguir los pasos de la guía de instalación. Tenga en cuenta estas recomendaciones:

- No elija la opción para instalar **ESET Bridge** (proxy HTTP). Sus clientes establecerán conexión directa con los servidores de ESET (para descargas, activaciones, actualizaciones). Los clientes más grandes pueden tener su propia solución local de proxy HTTP. Puede configurarse más tarde.
- ESET PROTECT Server también debe tener conectividad con el servidor de ESET (para sincronizarse con EMA 2, descargar actualizaciones y otras acciones).

Después de instalar ESET PROTECT Server, siga este proceso:

1. Asegúrese de tener una cuenta EMA 2 elegible.
2. Prepare un cliente con al menos una licencia. También puede utilizar un cliente existente.
3. Importe su cuenta de EMA 2 en ESET PROTECT On-Prem.
4. Complete la configuración de clientes MSP. Cuando se le solicite, seleccione el instalador **Solo agente**.
5. Distribuya e instale el instalador de ESET Management de forma local o remota.
6. Instale los productos de ESET Security y configure políticas.

El siguiente esquema es una descripción de alto nivel del proceso de inscripción de clientes MSP.



Implementación local del agente

Implementación local del instalador solo del agente

El **instalador solo del agente** es un script (*.bat* para Windows y *.sh* para Linux y macOS) que contiene toda la información necesaria para que un equipo cliente descargue e instale ESET Management Agent. Si instala en un equipo Linux, asegúrese de que este cumpla con los requisitos previos.

Puede ejecutar el instalador de forma local o desde un medio extraíble (una unidad de memoria USB, por ejemplo).

El ordenador cliente debe tener conexión a Internet para descargar el paquete de instalación del agente y conectarse a ESET PROTECT On-Prem.

Puede modificar el script de forma manual para ajustar algunos parámetros si lo considera necesario. Esta opción solo es recomendable para usuarios avanzados.

Implementación local del instalador todo en uno

El instalador todo en uno contiene el producto de seguridad de ESET que elija y un instalador de ESET Management Agent preconfigurado.

Consulte el manual del instalador para ver instrucciones detalladas.

Implementación remota del agente

Implementación remota del instalador solo del agente

El **instalador solo del agente** es un script (*.bat* para Windows y *.sh* para Linux y macOS) que contiene toda la información necesaria para que un equipo cliente descargue e instale ESET Management Agent. 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 implemente. Si está disponible, utilice una herramienta de administración remota de terceros para distribuir y ejecutar el script.

El ordenador cliente debe tener conexión a Internet para descargar el paquete de instalación del agente y conectarse a ESET PROTECT On-Prem.

Implementación remota del instalador todo en uno

El instalador todo en un no puede instalarse de forma remota en una red local con ESET Remote Deployment Tool. Consulte la documentación de ESET Remote Deployment Tool para ver instrucciones detalladas.

Licencias MSP

Cuentas válidas

Para activar las funciones MSP en ESET PROTECT On-Prem deberá importar su cuenta MSP en la Administración de licencias de ESET PROTECT On-Prem.

- Puede importar estos tipos de cuentas de EMA 2: MSP, MSP administrado y Responsable de MSP.
- Cualquier cuenta debe tener al menos un permiso de lectura para una empresa, que puede ser la empresa principal o un cliente.
- No es necesario tener acceso a la empresa principal.
- No se puede importar la cuenta de distribuidor.

Información sobre licencias y empresas

- Las licencias importadas desde su cuenta MSP se etiquetan con el nombre de la empresa. Si se cambia el nombre de la empresa más tarde, el nombre de las etiquetas no cambia automáticamente. Puede editarlos

de forma manual.

• Todas las licencias se importan con un método que sea compatible con el modelo de seguridad de ESET PROTECT On-Prem. Los usuarios que se crean con la configuración de clientes MSP solo pueden ver y usar sus licencias.

• Si hay una empresa en su estructura MSP que no tenga licencias cuando llegue el momento de la sincronización, esa empresa se sincronizará únicamente en el árbol MSP del ordenador, y no en el árbol MSP de la Administración de licencias.

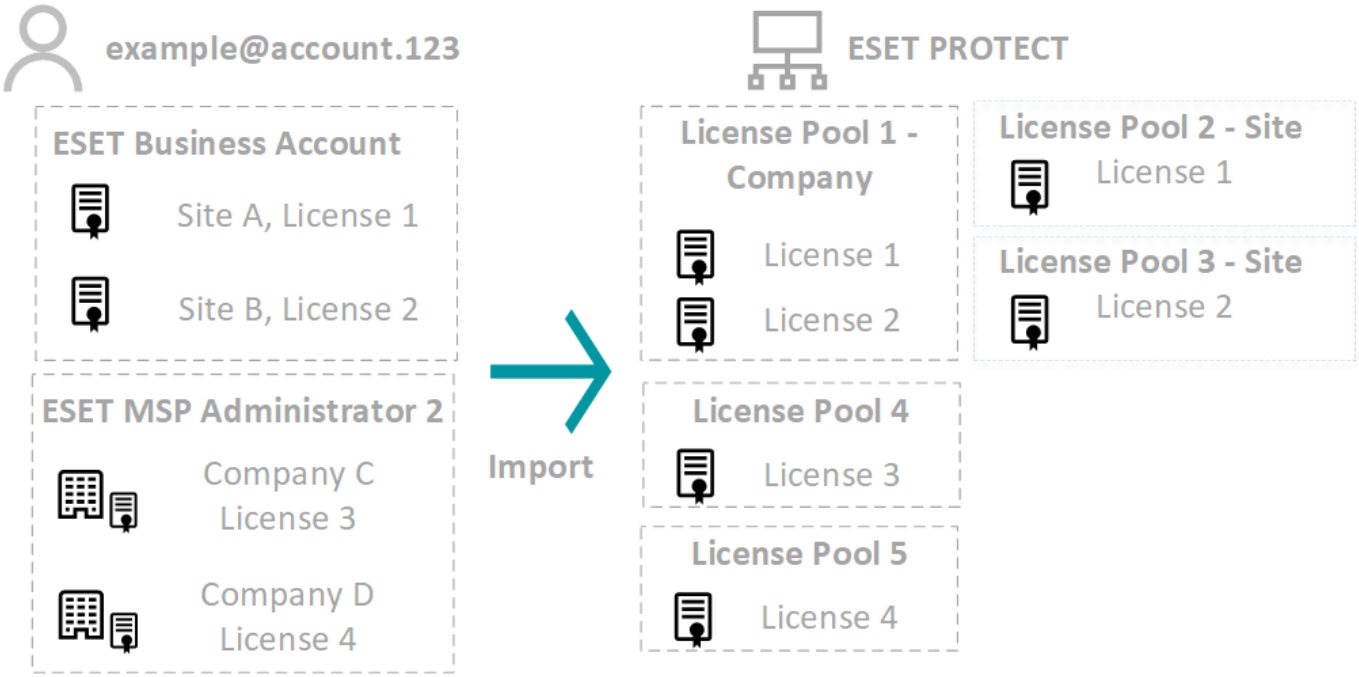
• Si agrega una nueva empresa en ESET MSP Administrator 2, ESET PROTECT On-Prem agregará la empresa al árbol MSP tras la próxima sincronización de licencias.

• Las licencias de ESET MSP Administrator 2 se dividen en un grupo para cada empresa. No puede extraer una licencia del grupo.

• Puede encontrar nombres de empresas y sitios en la columna **Usuario de la licencia** de Administración de licencias. Puede utilizar los datos del **Usuario de la licencia** al crear un informe.

• Si tiene licencias en ESET Business Account y ESET MSP Administrator 2 con las mismas credenciales, ESET PROTECT On-Prem sincroniza todas las licencias de ambas cuentas. Todas las licencias de ESET Business Account se guardan en varios grupos de licencias. Las licencias de ESET MSP Administrator 2 se dividen en un grupo para cada empresa. Desde la versión 8.0, ESET PROTECT On-Prem es compatible con Sitios de ESET Business Account para la división de licencias.

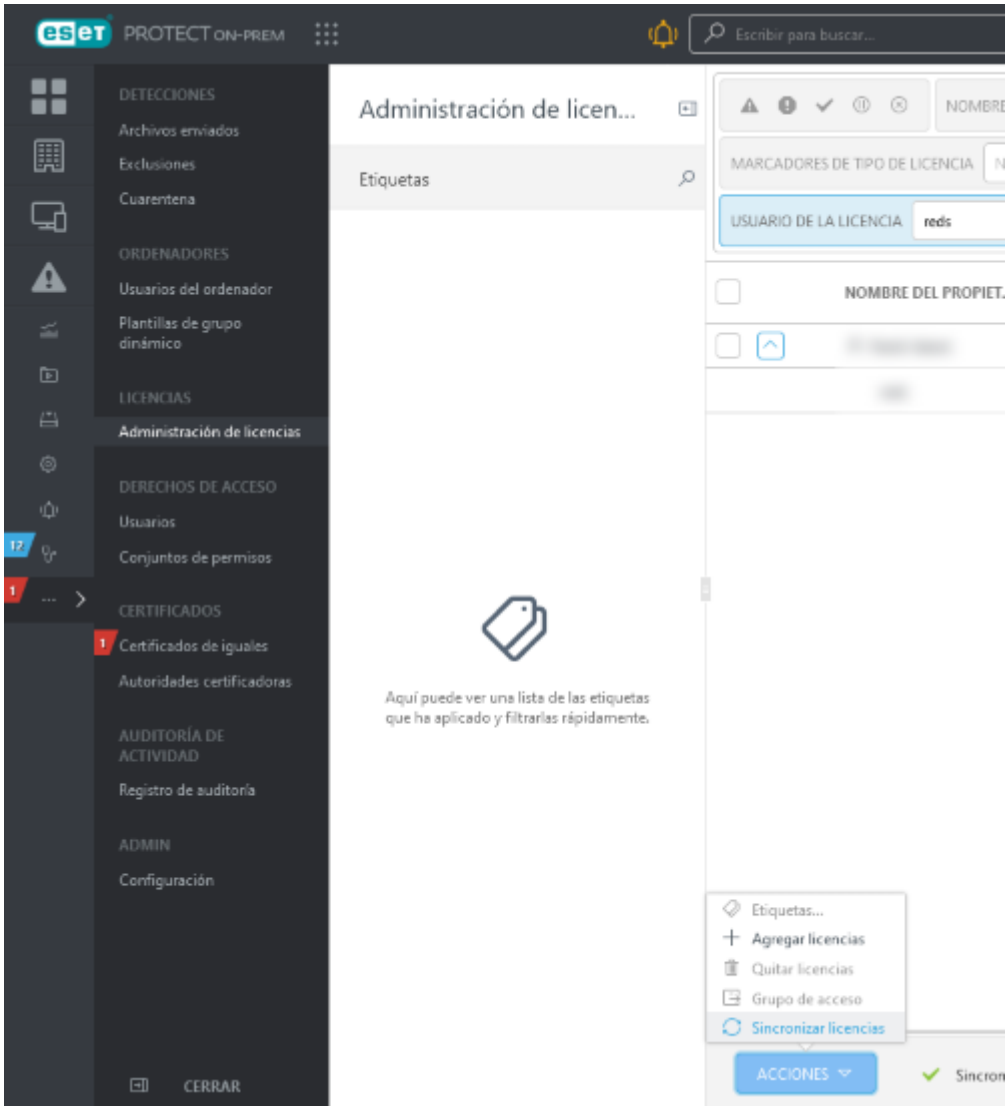
• Al quitar un grupo de licencias, se quitan automáticamente el resto de grupos de licencias asociados a la misma cuenta. Lea más información sobre cómo quitar una empresa.



Sincronización a petición

ESET PROTECT On-Prem se sincroniza con los servidores de licencias una vez al día. Si ha realizado cambios en su cuenta MSP y desea actualizar la pantalla de licencias y el árbol MSP, vaya a **Administración de licencias** >

Acciones y haga clic en **Sincronizar licencias**.

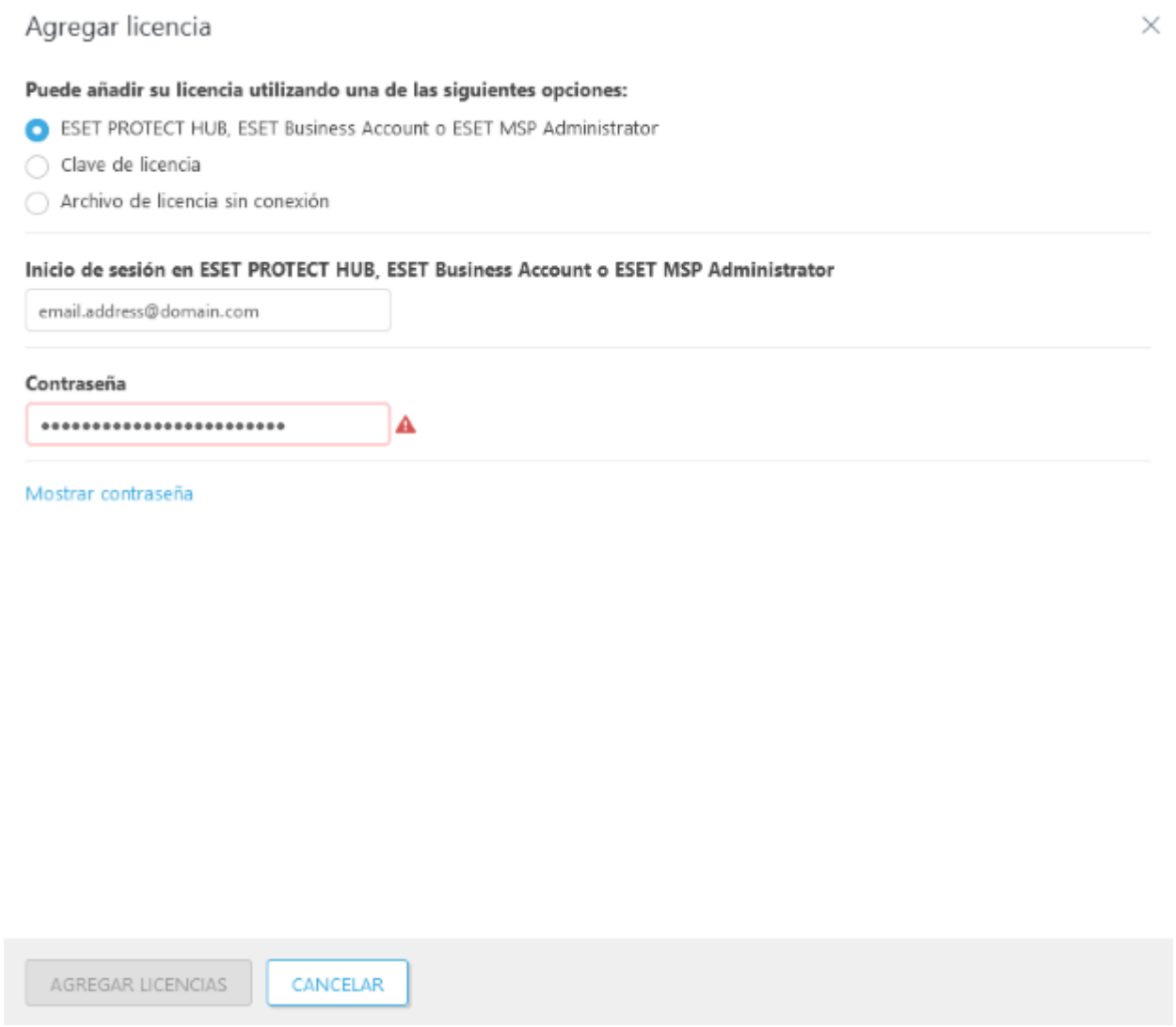


Importación de una cuenta MSP

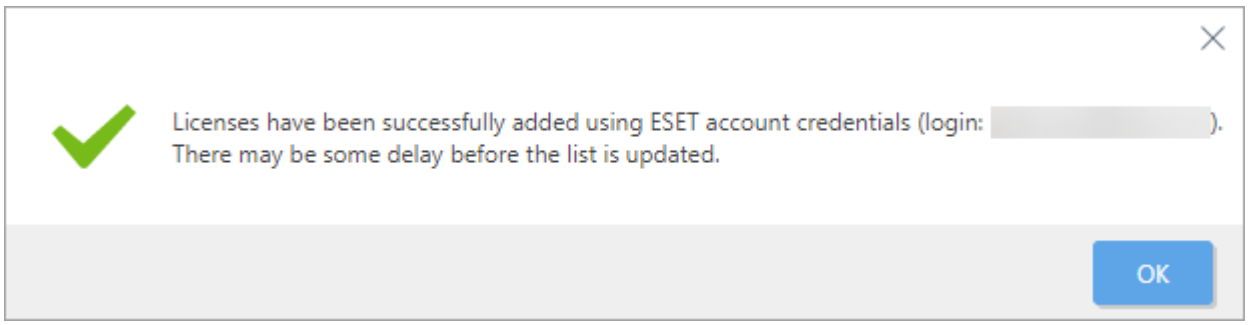
1. Inicie sesión en Web Console y vaya a **Más** > **Administración de licencias**.

2. Haga clic en **Acciones** > **Agregar licencias**.

3. Seleccione la opción **ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**. Introduzca sus credenciales de MSP (inicio de sesión de EMA 2) en los siguientes campos **Iniciar sesión** y **Contraseña**.



4. Haga clic en **Agregar licencias** para confirmar.



5. ESET PROTECT On-Prem sincronizará su estructura del portal MSP con el árbol de grupos estáticos del menú **Ordenadores** en Web Console. La estructura sincronizada recibe el nombre de *árbol MSP*.

> Importar una cuenta MSP con un elevado número de clientes (miles) puede tardar mucho tiempo, incluso horas.

Iniciar configuración de cliente MSP

Después de importar su cuenta MSP y sincronizar el árbol MSP, puede comenzar a configurar empresas. La configuración de clientes MSP crea:

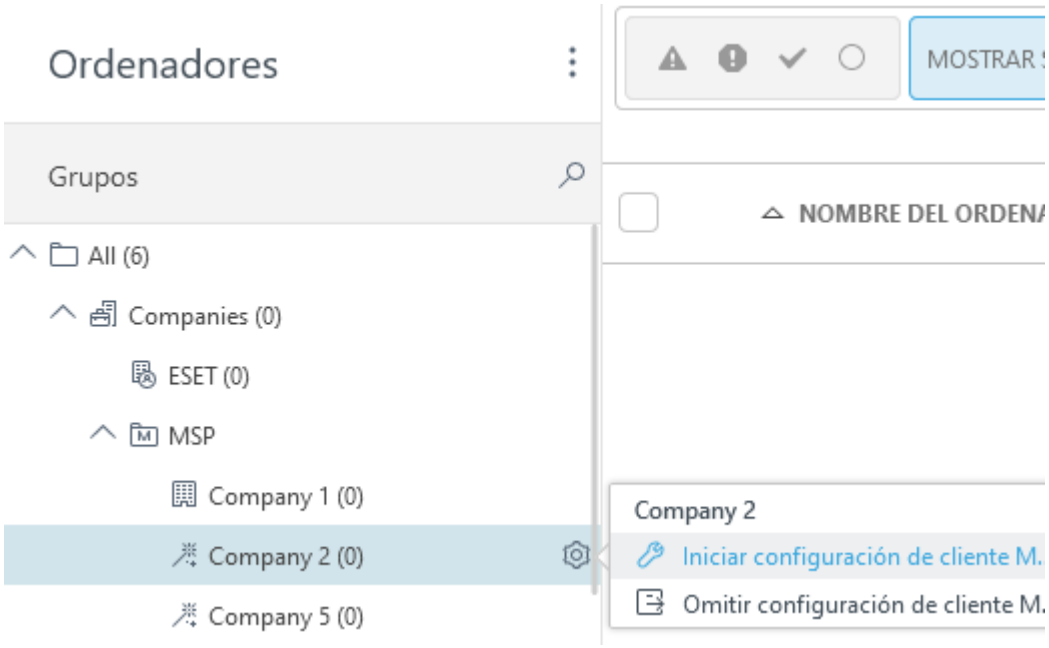
• Un instalador de una instancia de ESET Management Agent personalizada o integrada y un producto de seguridad de ESET. La configuración de clientes MSP no es compatible con la creación de instaladores de ESET Full Disk Encryption o ESET Inspect Connector.

• Un usuario MSP, que puede administrar ordenadores de la empresa desde Web Console.

También puede omitir la configuración de clientes MSP, pero le recomendamos que la complete.

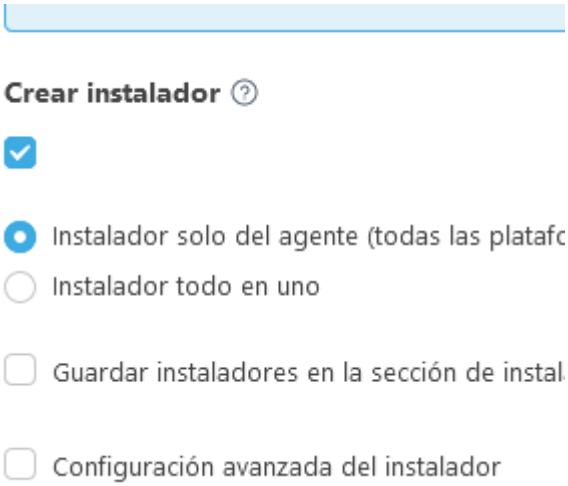
Solo puede configurar una empresa que tenga al menos 1 puesto de licencia válido.

1. En la ventana **Ordenadores**, haga clic en el icono del engranaje junto a la empresa que desee configurar y seleccione **Iniciar configuración de cliente MSP**.



2. Si desea guardar esta configuración como la predeterminada, marque la casilla de verificación de **Recordar configuración**. Haga clic en **Continuar**.

3. Si desea crear un instalador personalizado durante la configuración (recomendado), marque la casilla de verificación de **Crear instalador**.



4. Puede crear dos tipos de instaladores:

• **Instalador solo del agente (todas las plataformas)**: puede instalar este instalador de scripts del agente en ordenadores Windows, macOS y Linux.

• **Instalador todo en uno**: el instalador contiene ESET Management Agent 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 Instalador todo en uno

Producto o versión: seleccione el producto de seguridad de ESET que se instalará junto con ESET Management Agent. De forma predeterminada, se selecciona previamente la versión más reciente (recomendado). Puede seleccionar una versión anterior.
Seleccione el idioma en el menú desplegable **Idioma**.
Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

Si desea guardar el instalador en los instaladores para utilizarlo más adelante, marque la casilla de verificación situada junto a **Guardar instaladores en la sección de instaladores**.

^ Configuración avanzada del instalador (recomendada)

Nombre de host del servidor: es la dirección en la que las instancias de ESET Management Agent se conectan a ESET PROTECT Server. Seleccione un puerto distinto para la comunicación entre Agent y Server si es necesario. Si cambia el puerto, tendrá que cambiarlo para todos los agentes conectados y también 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 para entornos MSP.

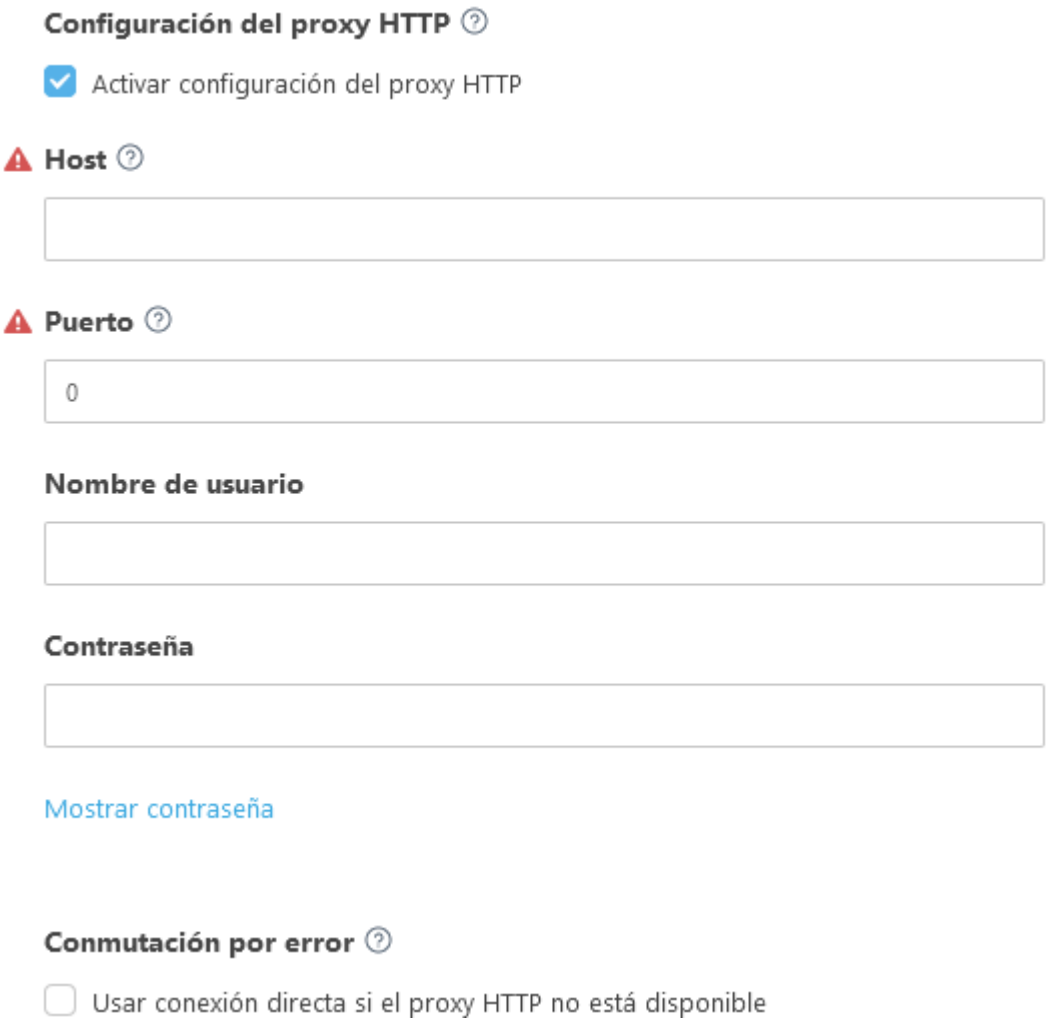
Activar configuración del proxy HTTP

Si utiliza un proxy HTTP (recomendamos utilizar ESET Bridge), marque la casilla **Activar configuración del proxy HTTP** y especifique la configuración del proxy (**Cliente**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador desde el proxy y establezca la conexión de ESET Management Agent con el proxy para activar el reenvío de comunicación entre ESET Management Agent y ESET PROTECT Server. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge utiliza el puerto 3128 de forma predeterminada. Puede establecer un puerto distinto si lo necesita. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

> El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

La casilla **Usar conexión directa si el proxy HTTP no está disponible** está marcada de forma predeterminada. El asistente aplica el ajuste como reserva para el instalador: no puede desmarcar la casilla. Puede deshabilitar la configuración mediante una política de ESET Management Agent:

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

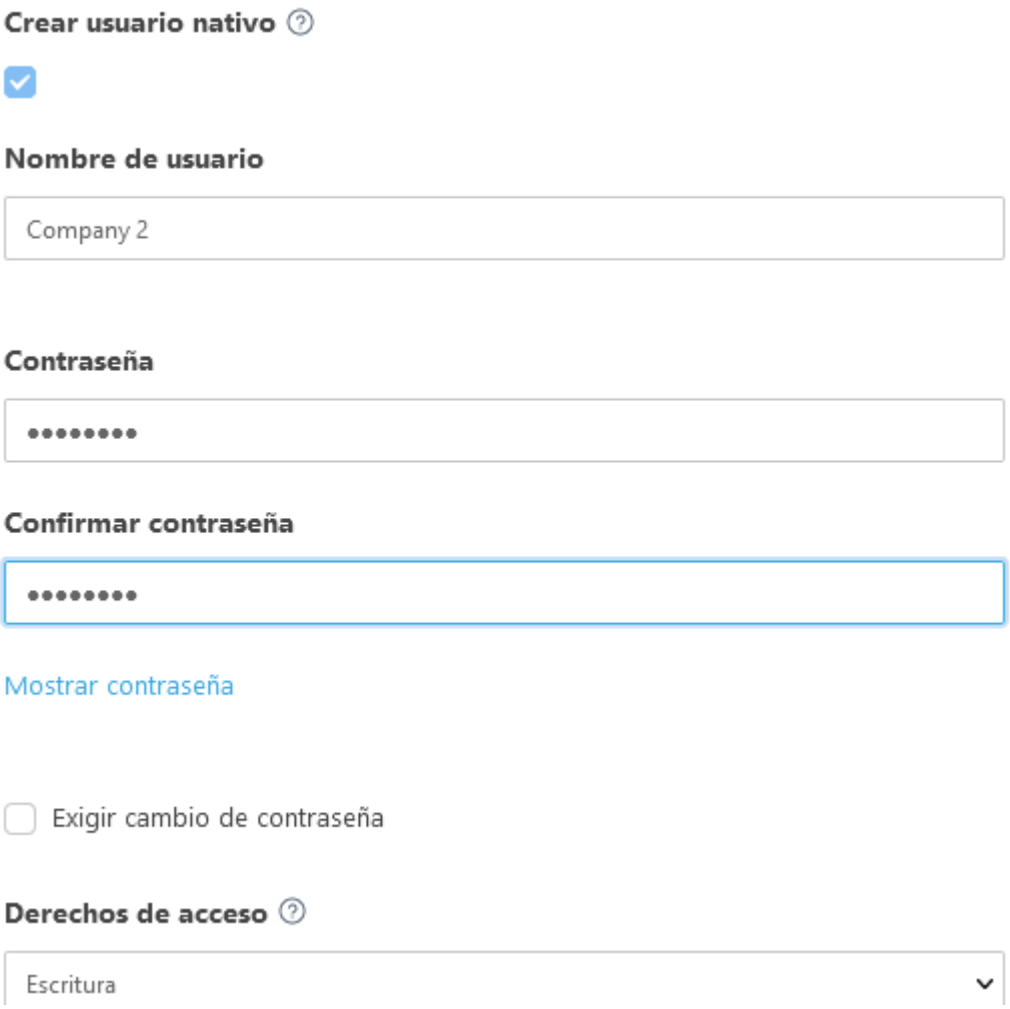


5. Haga clic en **Continuar** para ir a la sección **Usuario**.

6. Si desea crear un nuevo usuario para la empresa (recomendado), marque la casilla de verificación junto a **Crear usuario nativo**. El usuario puede iniciar sesión en Web Console y administrar los dispositivos de la empresa. Introduzca un nombre de usuario válido (que no contenga los caracteres , ; ") y una contraseña para el usuario nuevo.

a.**Exigir cambio de contraseña**: el usuario tiene que cambiar su contraseña después de iniciar sesión por primera vez.

b.**Derechos de acceso**: decida si el usuario tiene accesos de **Lectura y uso** o **Escritura** a los objetos de la empresa (ordenadores, políticas y tareas).



La sincronización con Active Directory no está disponible para usuarios creados mediante la configuración de empresas 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 vínculo y descargue el instalador que necesite. También puede volver a descargar el instalador desde el menú Instaladores si ha seleccionado guardar el instalador.

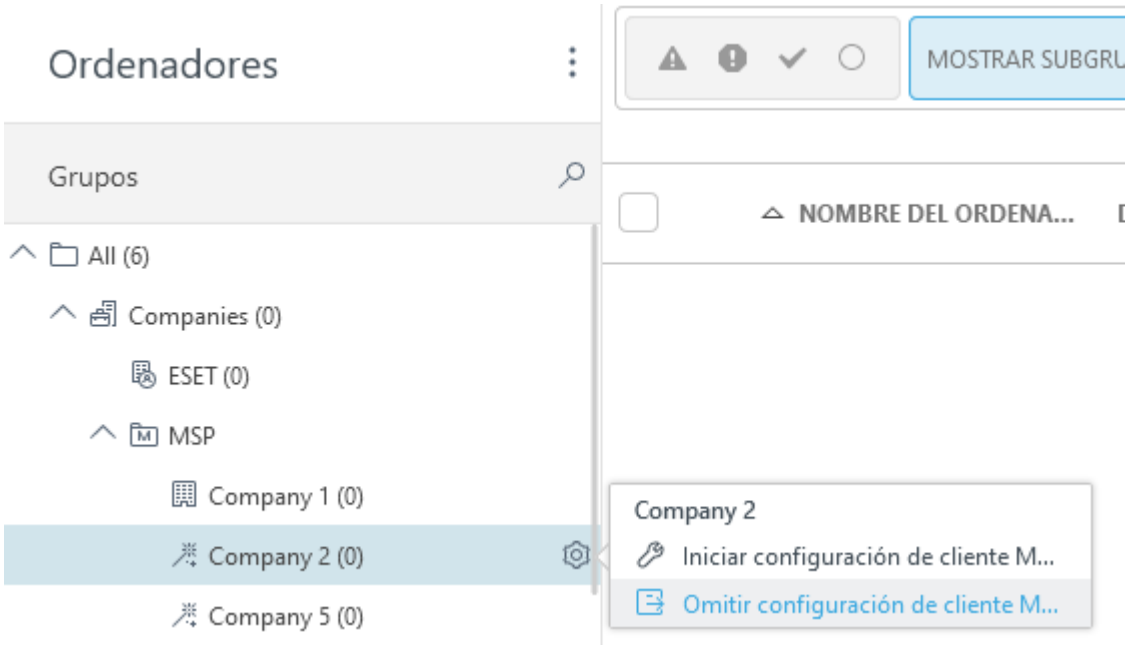
Consulte cómo implementar ESET Management Agent de forma local o remota.

Omitir configuración de cliente MSP

Puede **omitir la configuración de clientes MSP** si no desea configurarlo. También puede crear un instalador y un nuevo usuario más tarde. No le recomendamos omitir la configuración.

Después de omitir la configuración, el icono de la empresa cambia como si se hubiera configurado:

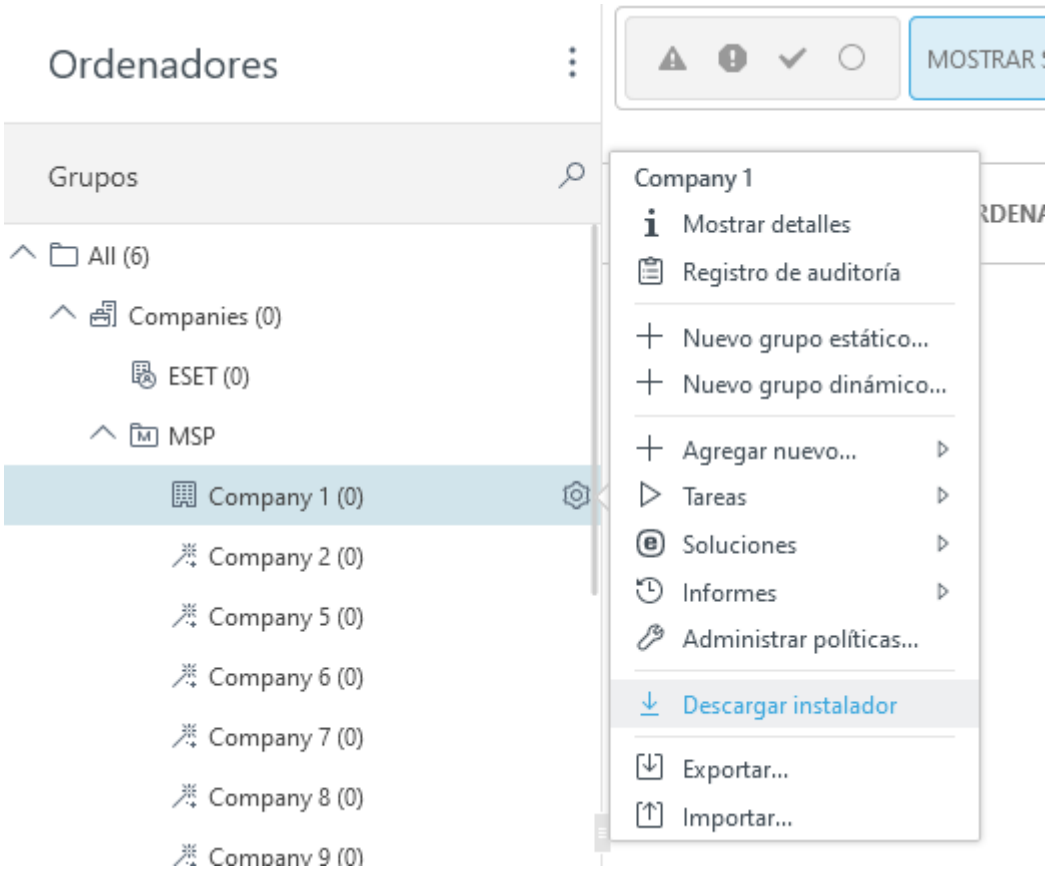
Si omite la configuración, no podrá volver a ejecutar el asistente de instalación para la empresa en la misma instancia de ESET PROTECT On-Prem.



Crear un instalador personalizado

1. En la consola web, vaya al menú **Equipos**.

2. Haga clic en el icono del engranaje junto a la empresa para la que desea 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 scripts del agente en ordenadores Windows, macOS y Linux.

• **Instalador todo en uno**: el instalador contiene ESET Management Agent 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 Instalador todo en uno

Producto o versión: seleccione el producto de seguridad de ESET que se instalará junto con ESET Management Agent. De forma predeterminada, se selecciona previamente la versión más reciente (recomendado). Puede seleccionar una versión anterior.
Seleccione el idioma en el menú desplegable **Idioma**.
Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

Si desea guardar el instalador en los instaladores para utilizarlo más adelante, marque la casilla de verificación situada junto a **Guardar instaladores en la sección de instaladores**.

^ Configuración avanzada del instalador (recomendada)

Nombre de host del servidor: es la dirección en la que las instancias de ESET Management Agent se conectan a ESET PROTECT Server. Seleccione un puerto distinto para la comunicación entre Agent y Server si es necesario. Si cambia el puerto, tendrá que cambiarlo para todos los agentes conectados y también 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 para entornos MSP.

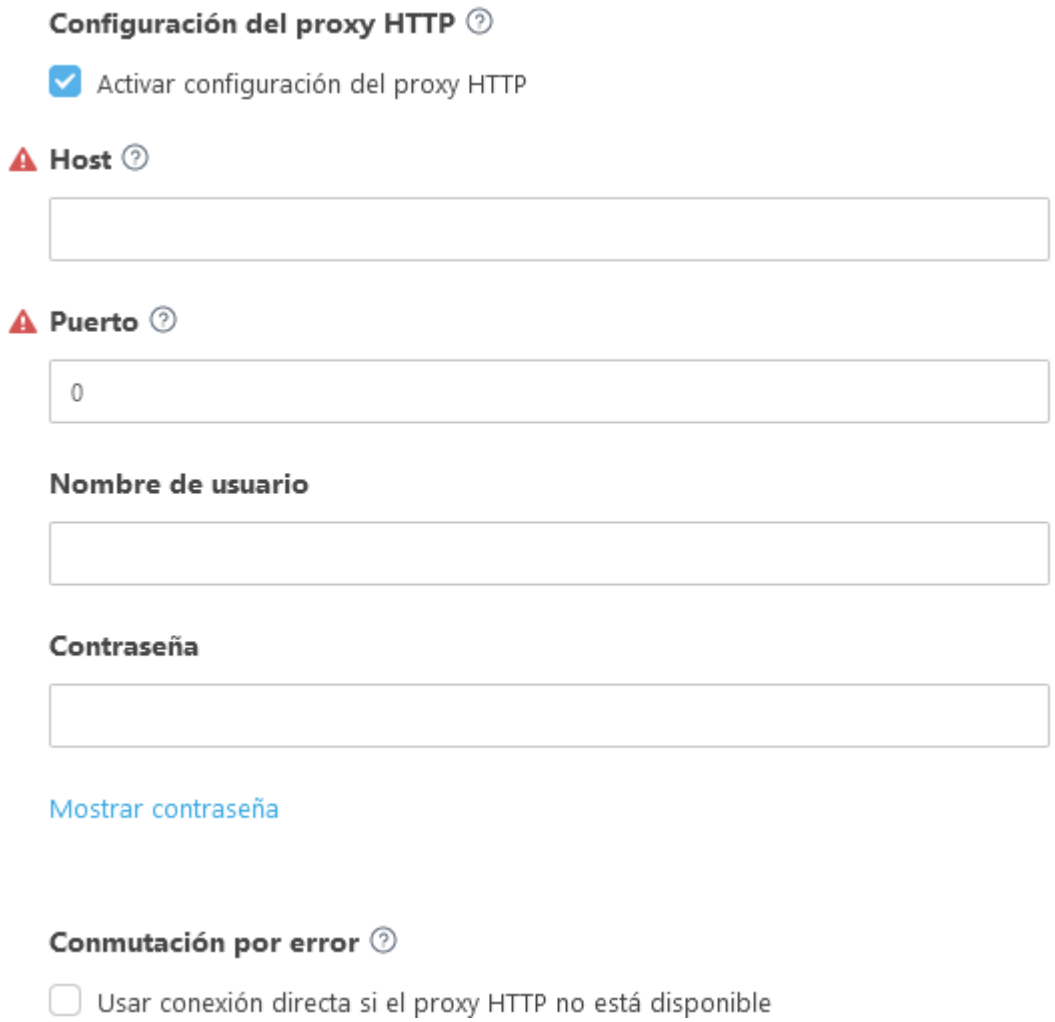
Activar configuración del proxy HTTP

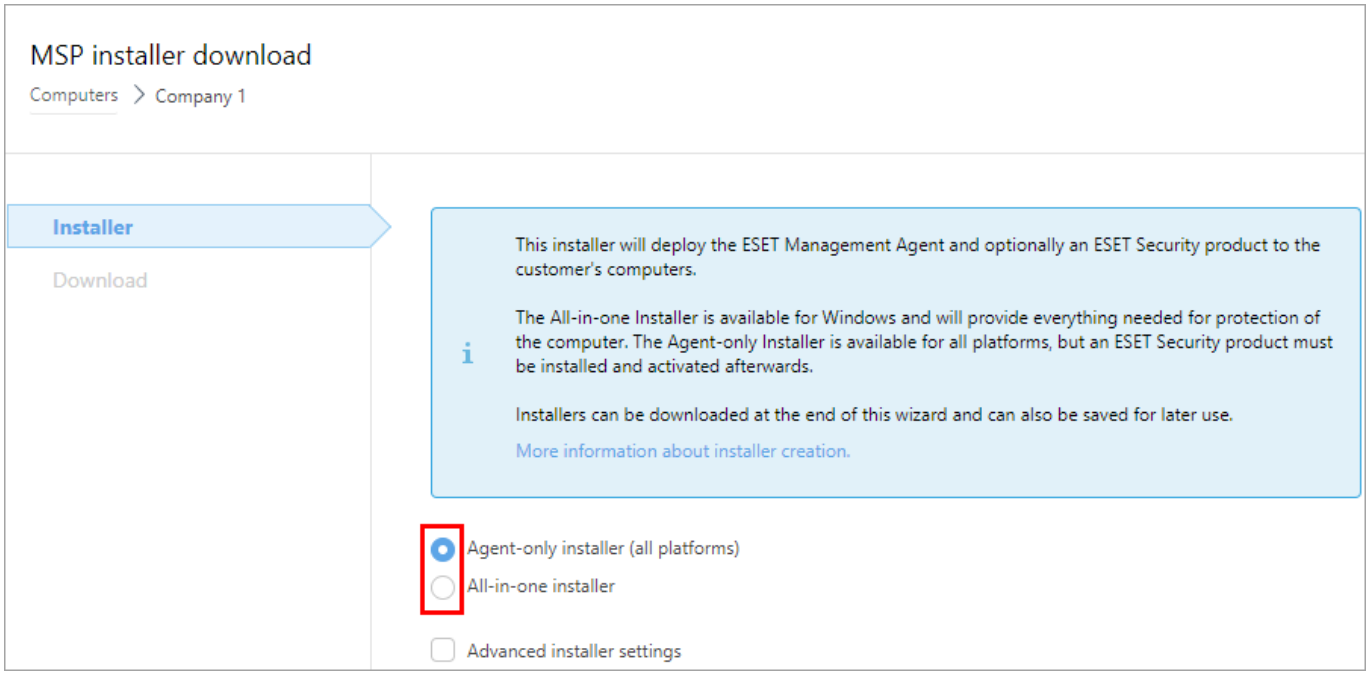
Si utiliza un proxy HTTP (recomendamos utilizar ESET Bridge), marque la casilla **Activar configuración del proxy HTTP** y especifique la configuración del proxy (**Cliente**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador desde el proxy y establezca la conexión de ESET Management Agent con el proxy para activar el reenvío de comunicación entre ESET Management Agent y ESET PROTECT Server. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge utiliza el puerto 3128 de forma predeterminada. Puede establecer un puerto distinto si lo necesita. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

> El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.

La casilla **Usar conexión directa si el proxy HTTP no está disponible** está marcada de forma predeterminada. El asistente aplica el ajuste como reserva para el instalador: no puede desmarcar la casilla. Puede deshabilitar la configuración mediante una política de ESET Management Agent:

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





4. Haga clic en **Crear** para crear el instalador.

5. Haga clic en el vínculo y descargue el instalador que necesite.

Usuarios MSP

Si configura su empresa mediante la configuración de clientes MSP, puede crear un tipo especial de usuario nativo (usuario MSP). Para revisar y editar el usuario, vaya al menú **Más** > **Derechos de acceso** > **Usuarios**.

También puede crear un usuario MSP personalizado, por ejemplo, para un MSP o un distribuidor.

Permisos necesarios

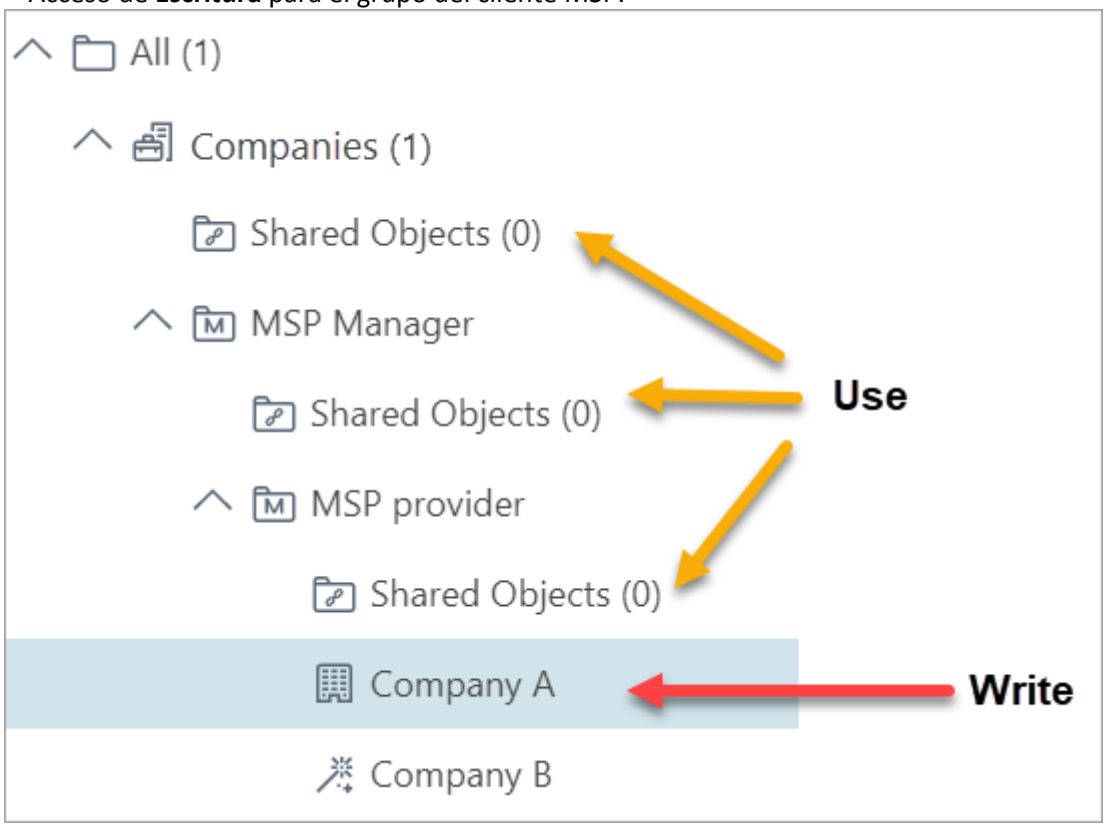
Para crear el nuevo usuario en la configuración de clientes MSP, necesita los derechos de acceso a la empresa que ha configurado y los grupos de **Objetos compartidos**.

Esquema de permisos detallado

Configurar una sola empresa

Derechos de acceso necesarios para crear un usuario durante la configuración de la *Empresa A*:

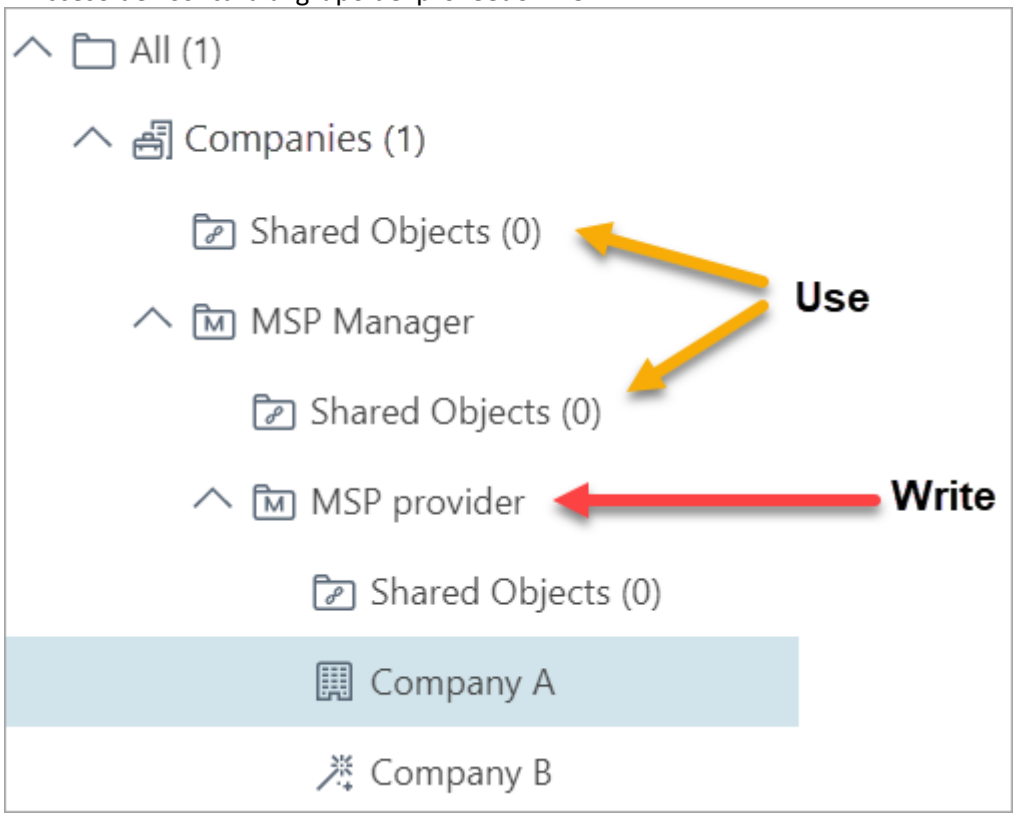
- Acceso de **Uso** para todos los grupos de **Objetos compartidos**.
- Acceso de **Escritura** para el grupo del cliente MSP.



Configurar todas las empresas de un MSP

Derechos de acceso necesarios para crear usuarios para todas las empresas que pertenezcan al *proveedor MSP*:

- Acceso de **Uso** para todos los grupos de **Objetos compartidos**.
- Acceso de **Escritura** al grupo del proveedor MSP.



Tener derechos de acceso significa que el usuario actual (activo) tiene conjuntos de permisos asignados con acceso a los grupos como se menciona anteriormente. Si no tiene los derechos de acceso necesarios, la configuración de clientes MSP termina con un error.

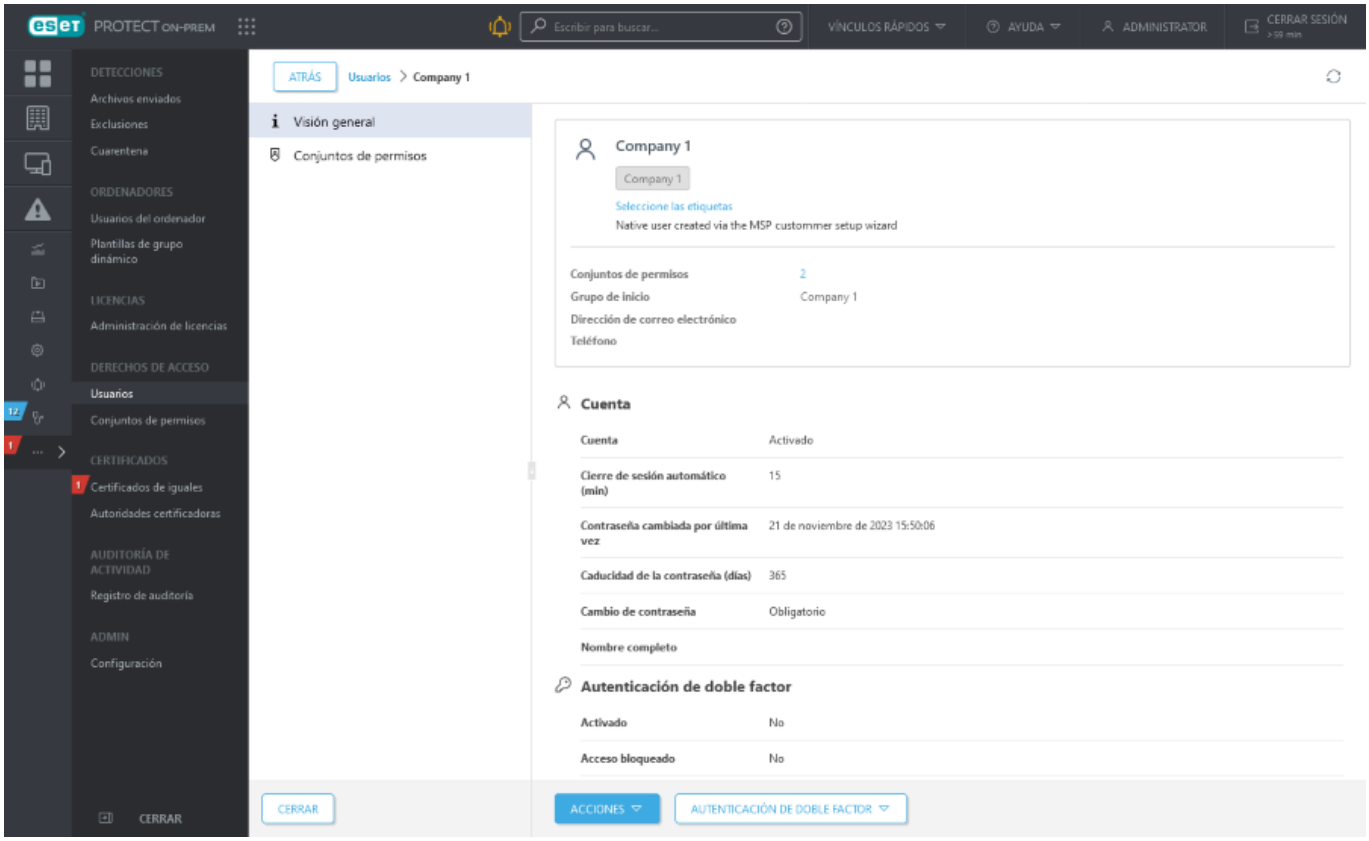
Características de los usuarios MSP

- Pueden iniciar sesión en ESET PROTECT Web Console y administrar dispositivos y otros objetos para los que tengan derechos de acceso.
- Pueden crear otro usuario nativo con los mismos permisos o menos.
- No pueden crear Usuarios del ordenador. Si es necesario crear un usuario del ordenador, deberá hacerlo un administrador.

La sincronización con Active Directory no está disponible para usuarios creados mediante la configuración de empresas MSP.

ESET PROTECT On-Prem tiene la siguiente configuración para cada nuevo usuario MSP:

- **Descripción**: usuario nativo creado en el asistente de instalación de clientes MSP
- **Etiquetas**: el usuario se etiqueta con el nombre de la empresa
- **Grupo de inicio**: grupo estático de la empresa
- **Cierre de sesión automático**: 15 minutos
- La cuenta está activada y no es necesario cambiar la contraseña
- **Conjuntos de permisos**: cada usuario MSP tiene dos conjuntos de permisos. Uno para su grupo de inicio y otro para los grupos de **Objetos compartidos**.

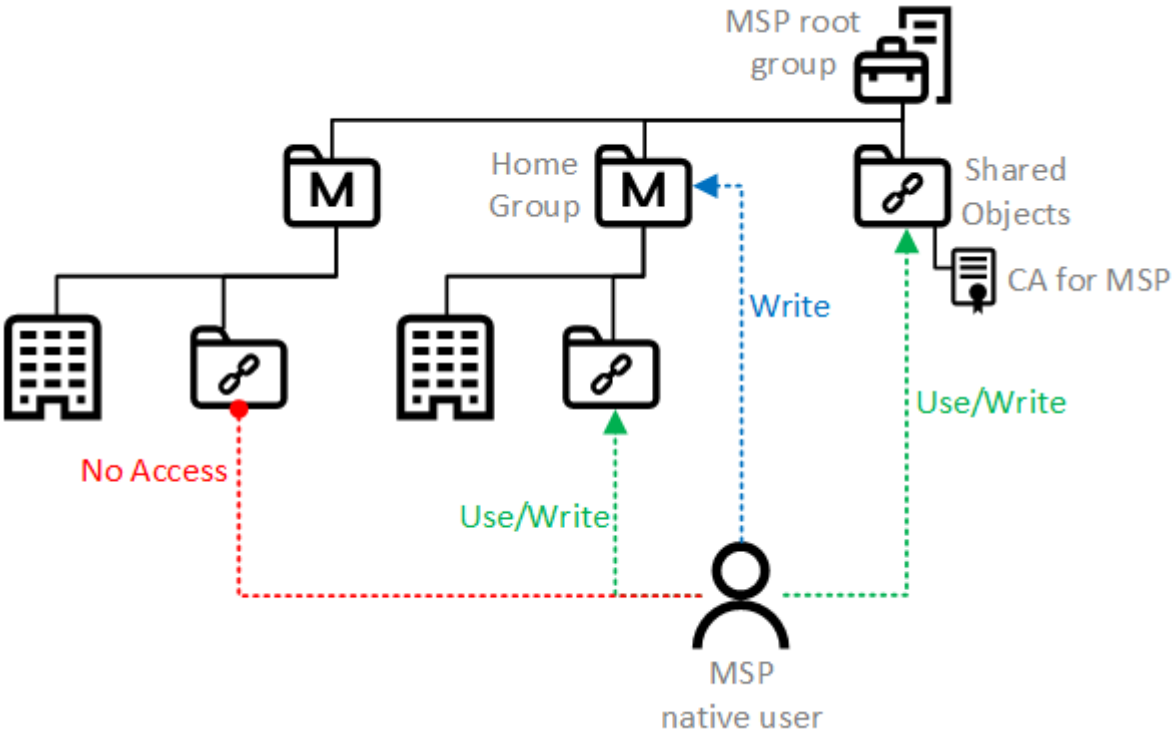


Crear un usuario MSP personalizado

Puede crear usuarios nativos de Web Console para administrar clientes, por ejemplo, para un MSP o un distribuidor.

1. Debe haberse creado la empresa MSP en EMA 2.
2. Compruebe que la empresa MSP se sincroniza en el árbol MSP.
3. Crear un usuario nativo. Configuración importante para usuarios MSP personalizados:
    a. El grupo de inicio del usuario se establece como el grupo estático MSP correspondiente.
    b. Cree y asigne los siguientes conjuntos de permisos al usuario:
        i. Permisos de **Escritura** para el grupo de inicio.
        ii. Permisos de **Uso** o **Escritura** para los grupos de **Objetos compartidos**.

> El grupo superior de **Objetos compartidos** contiene la autoridad certificadora de MSP. El acceso a la autoridad certificadora de MSP es necesario para que el usuario pueda crear un instalador.



El esquema de acceso de un usuario MSP personalizado.

Los usuarios MSP personalizados que se hayan creado siguiendo estos pasos podrán administrar dispositivos de clientes y crear instaladores. Sin embargo, no podrán administrar ESET PROTECT Server ni importar licencias.

Etiquetado de objetos MSP

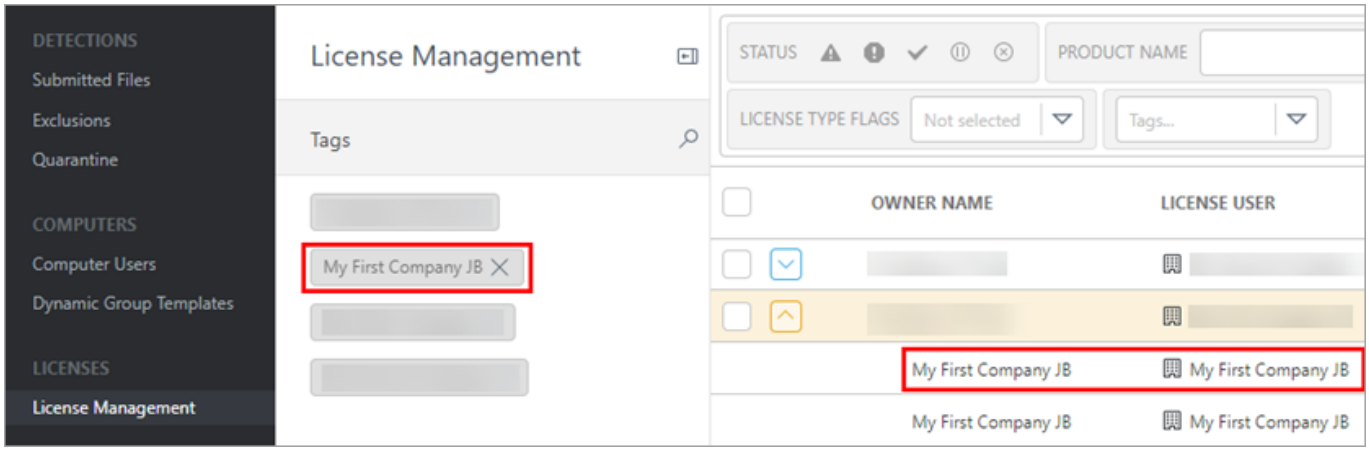
Si importa una cuenta MSP válida a ESET PROTECT On-Prem, activará el etiquetado automático de objetos MSP. Los siguientes objetos se etiquetan de forma automática:

- Licencias importadas desde una cuenta MSP
- Instaladores
- Usuarios y sus conjuntos de permisos creados con la configuración de clientes MSP

Las etiquetas son un tipo de marcas que se usan para mejorar el filtrado de objetos.

- El nombre de etiqueta automático es el mismo que el **Usuario de la licencia** (nombre de la empresa en EMA 2, excepto los caracteres , " que ESET PROTECT On-Prem elimina de la etiqueta).
- Si cambia el nombre del cliente en EMA 2 después de la sincronización, las etiquetas no se actualizan.
- Si lo desea, puede agregar más etiquetas personalizadas a cualquier objeto.
- Puede quitar las etiquetas sin afectar a los objetos etiquetados.

Haga clic en el icono para desplegar para ver la pestaña **Etiquetas**.



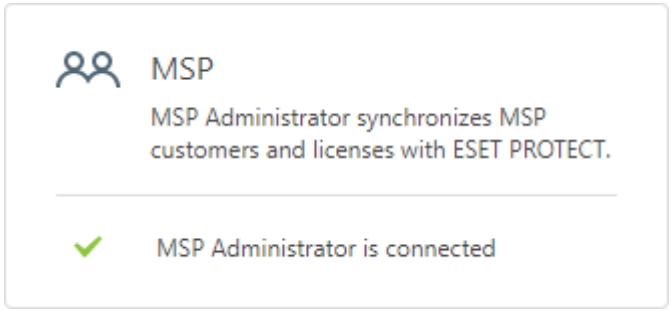
Resumen del estado de MSP

La sección Resumen del estado ofrece información detallada sobre el estado de ESET PROTECT On-Prem. Si importa una cuenta MSP, hay una ventana dinámica de MSP con información relacionada con MSP.

Estados de MSP

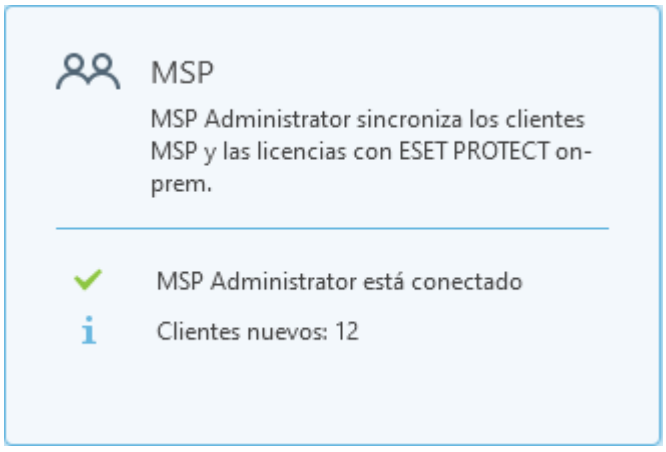
Cuenta sincronizada

Su cuenta está sincronizada y no tiene que hacer nada.



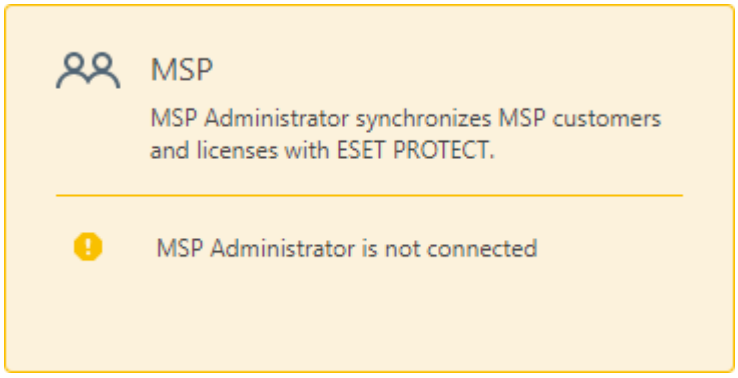
Sincronización en curso

Se está ejecutando la sincronización de una cuenta MSP en segundo plano. Si las cuentas contienen muchos datos, la sincronización puede tardar varias horas. La ventana dinámica se vuelve blanca después de la sincronización.



Cuenta desconectada

Hay varios grupos MSP (partes de árboles MSP) en su estructura de grupos estáticos, pero la cuenta MSP correspondiente no está importada. Esto puede ocurrir si quita su cuenta MSP de Administración de licencias.

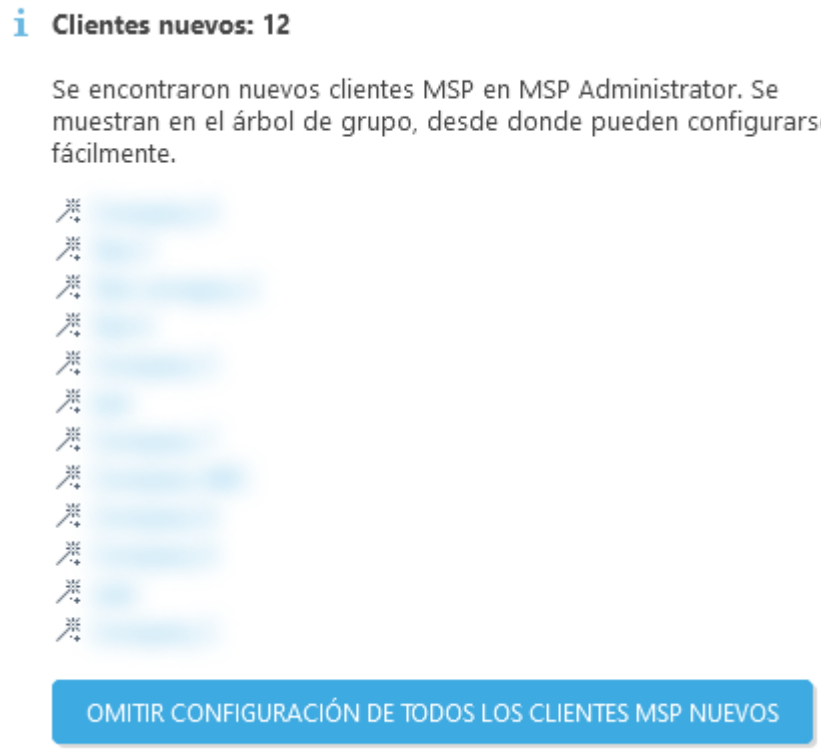


Acciones disponibles

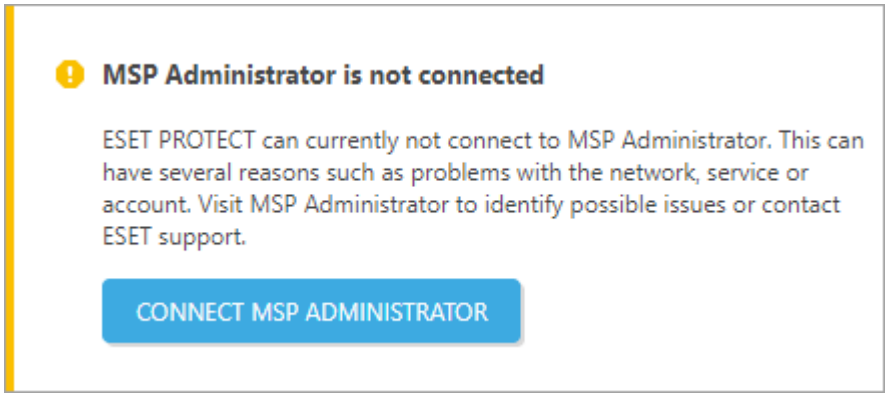
Haga clic en la ventana dinámica de MSP para ver más información.

- **Buscar nuevos clientes MSP**: ejecuta una sincronización de licencias a petición (se actualiza el árbol MSP).

- **Clientes nuevos**: si no ha configurado algunas empresas, puede hacer clic en ellas y seguir los pasos del asistente de instalación de clientes.
- **Omitir configuración de todos los clientes MSP nuevos**: omita los asistentes de instalación de todas las empresas que no se hayan configurado.



- **Conectar MSP Administrator**: puede agregar su cuenta MSP para importar sus licencias y su estructura de MSP.



Eliminación de una empresa

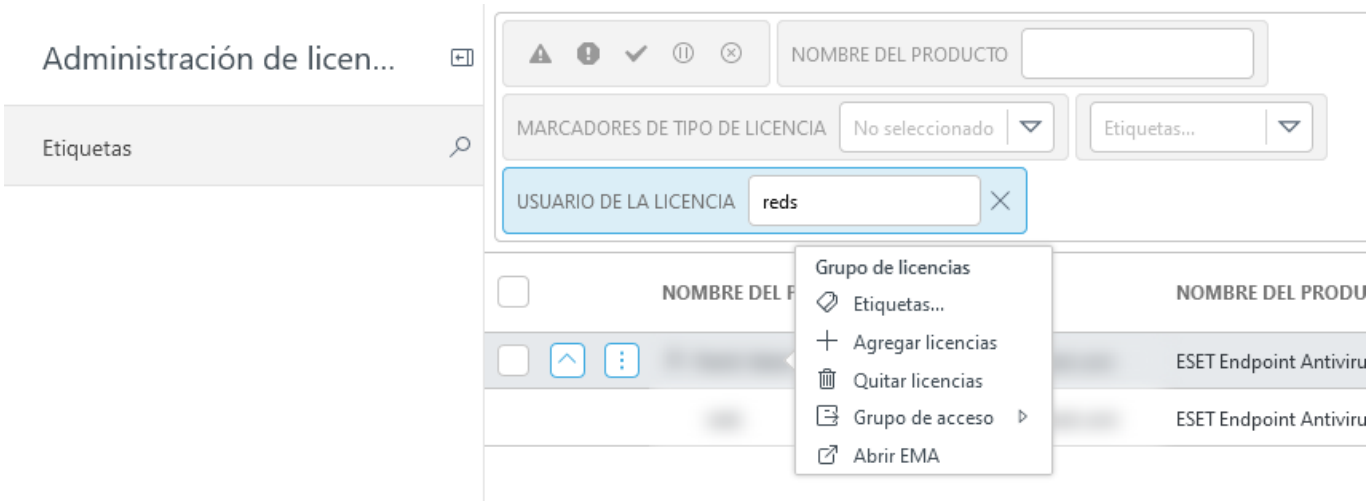
El árbol MSP se sincroniza con la cuenta MSP. Debe quitar la cuenta MSP de la Administración de licencias para desbloquear el árbol MSP. Una vez eliminada la cuenta, todas las empresas administradas por dicha cuenta se desvincularán del árbol MSP.

Si deja de administrar una empresa, quite las instancias de ESET Management Agent de los ordenadores de esa empresa. No puede quitar la empresa del árbol MSP sin quitar la cuenta MSP completa de su administración de licencias.
El grupo estático MSP es persistente. Una vez que sincronice el árbol MSP, no podrá eliminar nunca el grupo MSP raíz, solo sus grupos secundarios.

Eliminación de la cuenta MSP y las empresas del árbol MSP

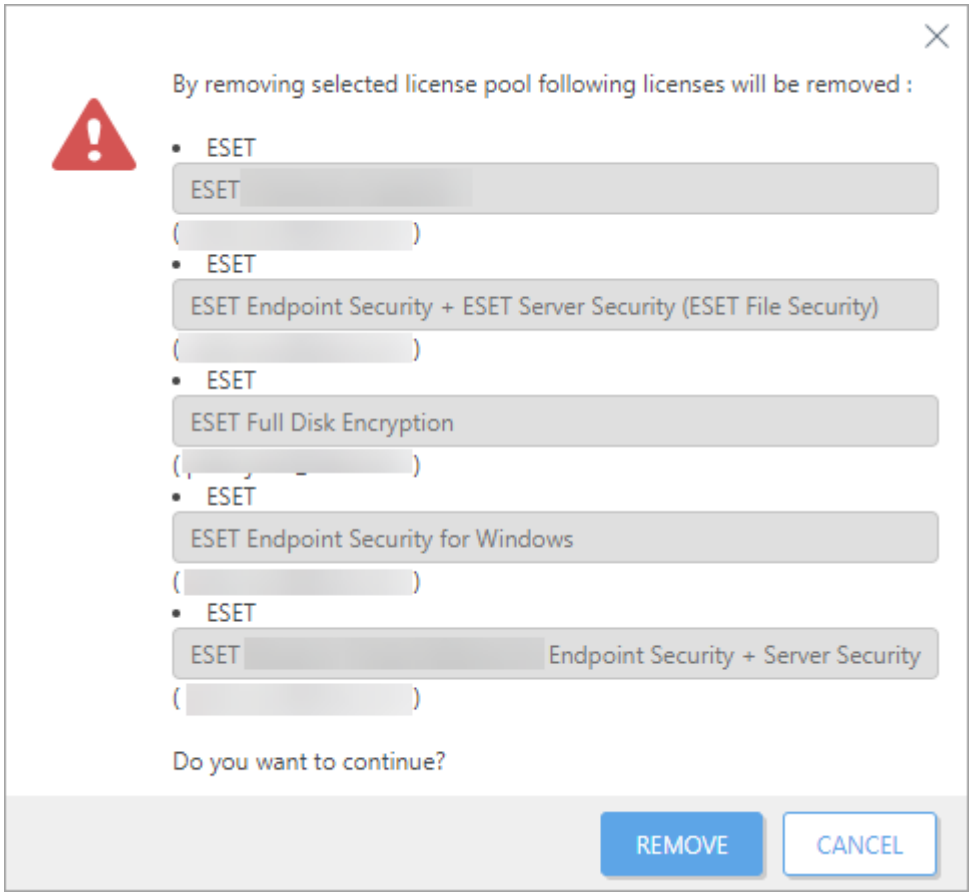
1. Inicie sesión en ESET PROTECT Web Console y vaya a **Más** > **Administración de licencias**.

2. Haga clic en la licencia que desee quitar > **Quitar licencias**. Recuerde que, si quita una licencia que esté vinculada a una cuenta MSP, toda la cuenta y sus licencias vinculadas desaparecerán de ESET PROTECT On-Prem.



3. Confirme que desea quitar (desvincular) las licencias mostradas de la Administración de licencias.

Al quitar un grupo de licencias, se quitan automáticamente el resto de grupos de licencias asociados a la misma cuenta.
Por ejemplo, las licencias de la *empresa X* se importaron usando credenciales de joe@test.me de EMA 2. Si un usuario quita licencias de la *empresa X*, todas las licencias importadas desde las cuentas de EBA y EMA 2 de joe@test.me se eliminarán de la Administración de licencias.



4. Espere unos minutos después de realizar la acción y vaya al menú **Ordenadores**.

5. Los iconos de todas las empresas eliminadas cambian a . Ya puede hacer clic y **eliminar** cualquier empresa que formara parte del árbol MSP anteriormente. Solo puede quitar una empresa (su grupo estático) si está vacía.

Después de quitar la cuenta MSP de la Administración de licencias, aparece el estado **MSP Administrator no está conectado** en el Resumen del estado. Debe quitar todos los grupos del árbol MSP anterior (en el menú **Ordenadores**) para desactivar ese estado.

Actualizaciones automáticas

Hay distintos tipos de actualizaciones automáticas de los productos de ESET:

- Actualización automática de ESET Management Agent
- 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 la vida útil 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 utiliza un repositorio sin conexión que no contiene los metadatos (por ejemplo, si ha copiado instaladores en una unidad de red compartida). Utilice la Mirror Tool para crear un repositorio sin conexión que admita actualizaciones automáticas. El repositorio sin conexión de la herramienta Mirror distribuye las actualizaciones automáticas simultáneamente por toda la red (un repositorio en línea distribuye las actualizaciones automáticas de forma gradual).

Actualización automática de ESET Management Agent

ESET PROTECT On-Prem ofrece una actualización automática de ESET Management Agent en ordenadores administrados.

Cómo funciona la actualización automática de ESET Management Agent

- El agente se actualiza a la versión más reciente que sea compatible con la instancia de ESET PROTECT Server instalada. Esta versión suele ser la versión de la instancia de ESET PROTECT Server instalada (por ejemplo, la 11.0).

- La actualización automática del agente está activada de forma predeterminada. Puede desactivarla en la política de ESET Management Agent > **Actualizaciones** > desactive el conmutador de alternancia **Activar actualización automática**.

- La actualización automática de ESET Management Agent se activa unas dos semanas después de la publicación de la versión más reciente de ESET Management Agent en el repositorio.

Cuando haya una versión de ESET Management Agent más reciente disponible y la actualización automática aún no se haya producido, puede iniciar la actualización del agente manualmente desde **Panel** > Estado de la versión del componente.
También puede usar la tarea del cliente Actualización de componentes de ESET PROTECT.

- El diseño de la actualización automática garantiza que el proceso de actualización se escalone y distribuya durante un periodo más largo, con el fin de evitar un mayor impacto en la red y en los ordenadores administrados.

- Las actualizaciones automáticas no funcionan si utiliza un repositorio sin conexión que no contiene los metadatos (por ejemplo, si ha copiado instaladores en una unidad de red compartida). Utilice la Mirror Tool para crear un repositorio sin conexión que admita actualizaciones automáticas. El repositorio sin conexión de la herramienta Mirror 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

Las versión 9.0 de ESET PROTECT On-Prem y posteriores incluyen una función para mantener los productos de seguridad de ESET actualizados a la versión más reciente en sus ordenadores administrados.

Las actualizaciones automáticas de productos se activan 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 empresariales de ESET compatibles con las actualizaciones automáticas. Otros productos de seguridad de ESET no admiten las actualizaciones automáticas y ESET incorporará esta función en ellos más adelante.
- Puede configurar las actualizaciones automáticas mediante una política.
- Consulte también las preguntas frecuentes sobre las actualizaciones automáticas. La primera actualización automática se realizará cuando se publique una versión futura de la compilación 9.x publicada inicialmente (por ejemplo, 9.1 o 9.0.xxxx.y, cuando xxxx sea 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, Web Console puede informar de 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 utiliza un repositorio sin conexión que no contiene los metadatos (por ejemplo, si ha copiado instaladores en una unidad de red compartida). Utilice la Mirror Tool para crear un repositorio sin conexión que admita actualizaciones automáticas. El repositorio sin conexión de la herramienta Mirror 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:

- Utilice la acción con un clic en **Panel** > **Resumen del estado** > **Estado de la versión del componente** > haga clic en el gráfico de barras y seleccione **Actualizar componentes de ESET instalados**.
- En **Ordenadores**, haga clic en el icono del engranaje situado junto a **Todo el grupo estático** y seleccione **Tareas** > **Actualización** > **Actualizar productos de ESET**.
- Utilice la Tarea del cliente Instalación de software.

Hay dos formas de actualizar los productos de seguridad de ESET a la versión más reciente:

- Tarea del cliente Instalación de software
- Función de actualizaciones automáticas

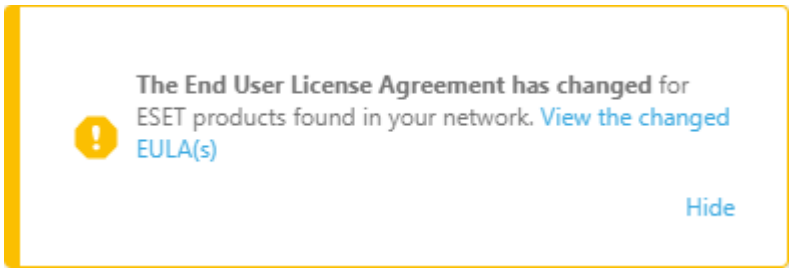
Diferencias entre la tarea del cliente Instalación de software y la función Actualizaciones automáticas:

	Proceso de actualización	Reiniciar tras la actualización	Futuras actualizaciones
Tarea del 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 ordenador 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 del cliente Instalación de software. Consulte las opciones disponibles más arriba.

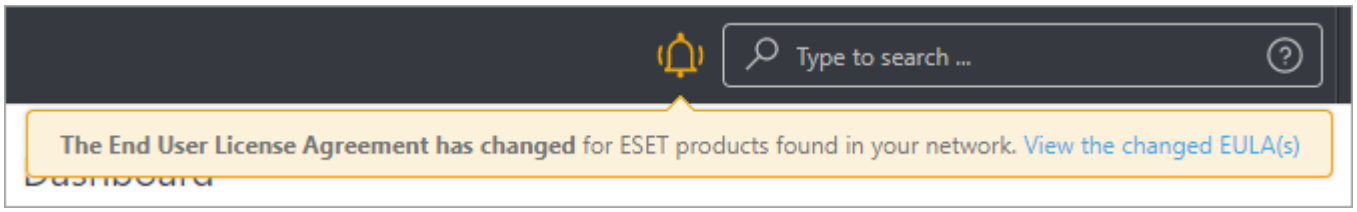
	Proceso de actualización	Reiniciar tras la actualización	Futuras actualizaciones
Actualizaciones automáticas	El proceso de actualización no incluye la reinstalación del producto de seguridad de ESET.	Para actualizar el producto de seguridad de ESET hay que reiniciar el ordenador, pero no inmediatamente (el reinicio no se fuerza). El administrador de ESET PROTECT On-Prem puede forzar la actualización y el reinicio del ordenador de forma remota desde la consola web mediante la tarea del cliente Apagar el ordenador con la casilla de verificación **Reiniciar ordenadores** seleccionada.	Automática: actualizaciones automáticas de los productos de seguridad de ESET compatibles cuando se lanza una nueva versión (la actualización se retrasa por motivos de estabilidad). Puede activar manualmente la búsqueda de actualizaciones de productos de seguridad de ESET mediante la tarea Buscar actualizaciones del producto.

Acuerdos de licencia para el usuario final actualizados de productos de seguridad de ESET administrados

ESET PROTECT Web Console notifica al administrador si está disponible un acuerdo de licencia para el usuario final (EULA) actualizado de un producto de seguridad de ESET administrado.

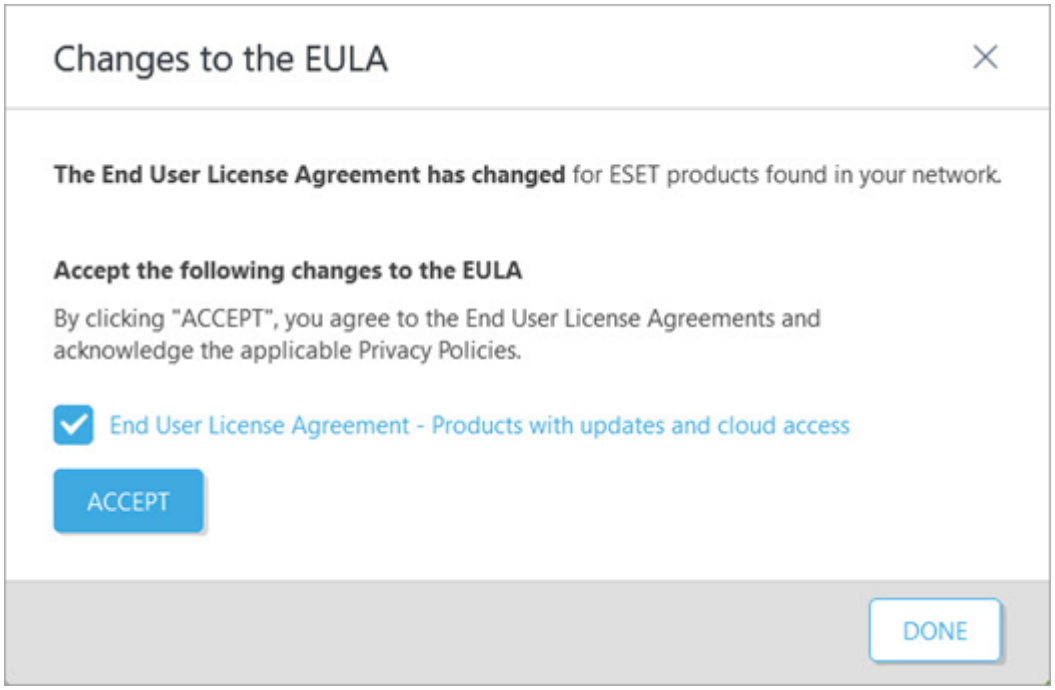


Haga clic en **Ver los EULA modificados** para ver los detalles o en **Ocultar** para mover la notificación situada bajo un icono de campana amarillo en la barra de herramientas superior.

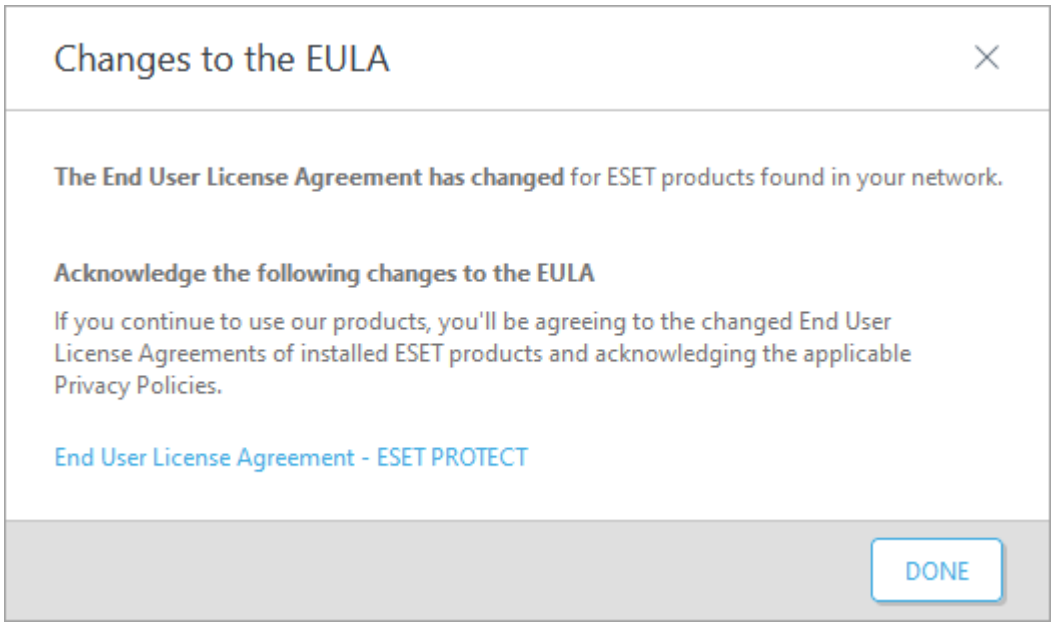


Cuando hace clic en **Ver los EULA modificados**, aparece una nueva ventana con detalles sobre el producto de seguridad de ESET y los cambios de su EULA:

- 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 **Acepto** para aceptar el EULA actualizado y permitir la actualización a una versión que admita actualizaciones automáticas.



- Si tiene productos empresariales de ESET que admiten actualizaciones automáticas (por ejemplo, ESET endpoint versión 9 y posteriores), recibe una notificación sobre el EULA actualizado, pero no tiene que aceptarlo (el botón **Acepto** 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 el grupo estático **Todos** como destino predeterminado.

Cambie los destinos de la política de actualizaciones automáticas

integrada.

En ESET PROTECT Web Console, haga clic en **Políticas** > despliegue **Políticas integradas** > haga clic en la política > seleccione **Cambiar asignaciones** > ajuste los destinos > haga clic en **Finalizar**.

Configurar las actualizaciones automáticas

Cree una nueva política de **Actualizaciones automáticas** para configurar las actualizaciones automáticas.

1. En ESET PROTECT Web Console, haga clic en **Políticas** > **Nueva política Configuración**.
2. Seleccione **Funciones comunes** > **Actualización** en el menú desplegable y configure los ajustes de la política:
   - **Cambio automático de perfil**: haga clic en **Editar** y asigne un perfil de actualización según los perfiles de conexión de red.
   - **Actualizaciones automáticas**: las actualizaciones automáticas están activadas de forma predeterminada.

> Para desactivar las actualizaciones automáticas, desactive el conmutador de alternancia **Actualizaciones automáticas**. Consulte también Exclusión de las actualizaciones automáticas.

   - **Detener actualizaciones en** > **Seleccionar versión**: también puede configurar, si lo desea, la versión del producto de seguridad de ESET que dejará de actualizarse automáticamente:
     - Haga clic en **Seleccionar del repositorio** y seleccione la versión.
     - Escriba la versión; puede utilizar * como comodín; por ejemplo, 9.*/9.0.*/9.0.2028.*.

> Por ejemplo, si escribe 9.0.*, se instalarán todas las correcciones de errores 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 establecida 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 política (grupos u ordenadores individuales).

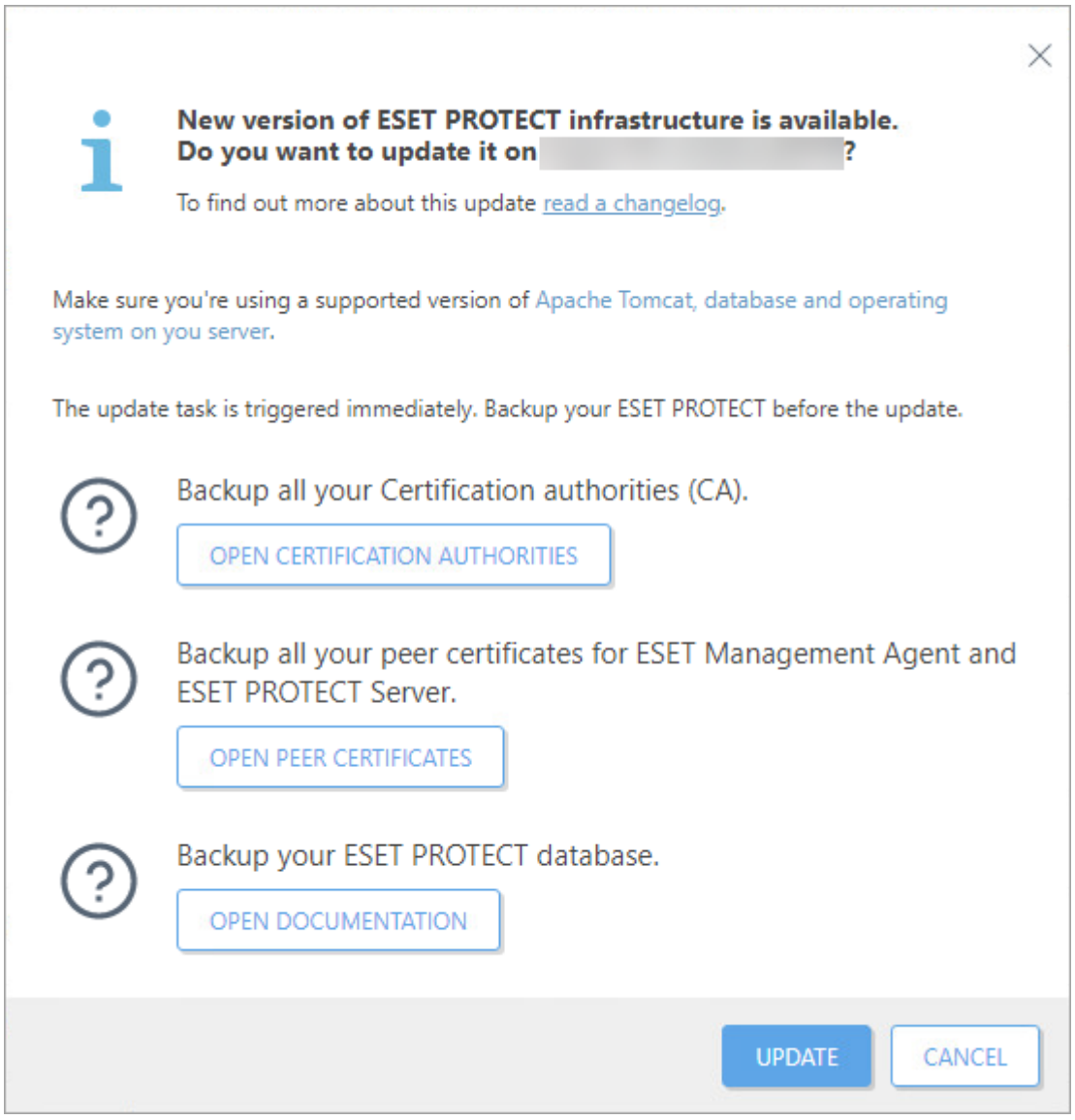
> Asegúrese de que la política de actualizaciones automáticas integrada no sobrescribe la configuración de la política de actualizaciones automáticas que ha creado. Obtenga más información sobre la aplicación de las políticas en los clientes.

4. Haga clic en **Finalizar**.

Actualización ESET PROTECT On-Prem

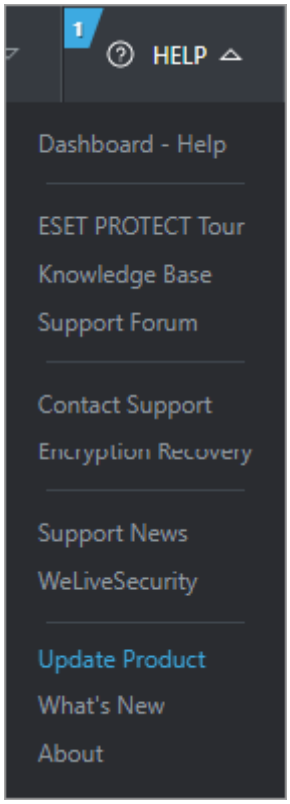
ESET PROTECT Server busca regularmente las actualizaciones disponibles para la infraestructura de ESET PROTECT.

Cuando hay una actualización disponible, aparece una ventana:



Puede obtener información sobre la actualización de ESET PROTECT On-Prem disponible si hace clic en **leer un registro de cambios**.

Si no selecciona la opción de actualizar, puede ver la ventana de actualización haciendo clic en **Ayuda** > **Actualizar el producto**:



Solo los usuarios que pueden ejecutar la tarea del cliente ESET PROTECT Actualización de componentes pueden ver la notificación de la actualización.

Asegúrese de ejecutar una versión compatible de Apache Tomcat, base de datos y sistema operativo en su servidor.

1. Haga clic en el botón **Abrir autoridades certificadoras** y haga una copia de seguridad de todas sus autoridades certificadoras.

2. Haga clic en el botón **Abrir certificados de iguales** y haga una copia de seguridad de todos sus certificados.

3. Haga clic en el botón **Abrir documentación** y haga una copia de seguridad de la base de datos de ESET PROTECT.

4. Haga clic en el botón **Actualizar**.

5. Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

6. Haga clic en el botón **Actualizar**. Hay una actualización de ESET PROTECT Server programada: en **Tareas** encontrará una nueva tarea del cliente que actualiza los componentes de ESET PROTECT en el ordenador en el que está instalado ESET PROTECT Server. Se cerrará sesión en Web Console cuando se inicie la actualización. Puede iniciar sesión una vez completada la actualización. Puede comprobar la versión de ESET PROTECT On-Prem en **Ayuda** > Acerca de.

Para actualizar a la versión más reciente componentes de ESET PROTECT en los dispositivos conectados a ESET PROTECT Server, puede activar la tarea ESET PROTECT Actualización de componentes directamente desde la ventana de actualización.

No todos los componentes de ESET PROTECT se actualizan automáticamente; algunos requieren una actualización manual.

ESET PROTECT On-Prem admite la actualización automática de las instancias de ESET Management Agent en ordenadores administrados.

Actualizar componentes de terceros

Además de componentes de ESET, ESET PROTECT On-Prem utiliza componentes de terceros que requieren una actualización manual.

En ESET PROTECT Web Console, haga clic en **Vínculos rápidos** > **Componentes del servidor** para ver componentes de terceros con una versión más reciente disponible.

- Recomendamos 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 utilizado para ejecutar ESET PROTECT Server.
- El dispositivo virtual de ESET PROTECT no informa de las actualizaciones disponibles para componentes de terceros.

ESET PROTECT Web Console recomienda una actualización de las versiones anteriores a las indicadas a continuación:

Componente de terceros:	Versión:	Notas:	Actualizar instrucciones
Microsoft SQL Server	2019 (compilación 15.0.4335.1)	Determine su versión y su edición de SQL Server Database Engine e instale la actualización acumulativa más reciente.	Servidor de base de datos
MySQL	8.0.0.0	Haga clic en **Ayuda** > **Acerca de** en ESET PROTECT Web Console 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 de 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 para consultar 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:	Actualizar instrucciones
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 ha alcanzado el soporte limitado. Si utiliza Apache HTTP Proxy, le recomendamos migrar a ESET Bridge.	Migrar a ESET Bridge

El componente ESET PROTECT Mobile Device Management/Connector (MDM/MDC) (solo local) llega al fin de la vida útil en enero de 2024. Más información. Le recomendamos migrar a Cloud MDM.

Preguntas frecuentes

Lista de preguntas

17. ¿Cómo puedo actualizar mi producto de seguridad de ESET?

18. Cómo puedo cambiar el sufijo en la dirección de la Consola web

---

¿Cómo resolver el error **No se pudo iniciar sesión: la conexión ha fallado con el estado "No conectado"**?

Verifique si el servicio del servidor ESET PROTECT o Microsoft SQL está funcionando. De no ser así, inícielos. De no ser así, inícielos. Si está en funcionamiento, reinicie el servicio, actualice Web Console e intente iniciar sesión de nuevo. Encontrará más información en Resolución de problemas de inicio de sesión.

¿Para qué se usa el grupo "**Perdidos y encontrados**"?

Cada ordenador que se conecta a ESET PROTECT Server y no es un miembro de ningún grupo estático se muestra automáticamente en este grupo. Puede trabajar con el grupo y los ordenadores incluidos en el mismo y con ordenadores en cualquier otro grupo estático. Es posible cambiar el nombre del grupo o moverlo a otro grupo, pero no se puede eliminar.

¿Cómo se puede crear un perfil de actualización dual?

Consulte nuestro artículo de la base de conocimiento de ESET para obtener instrucciones paso a paso.

¿Cómo puede actualizarse la información en una página o en una sección de la página sin actualizar la ventana completa del navegador?

Haga clic en **Actualizar** en el menú contextual en la parte superior derecha de una sección de la página.

¿Cómo puede realizarse una instalación silenciosa de ESET Management Agent?

Los siguientes métodos le permiten realizar una instalación silenciosa:

- Script de GPO o SCCM
- Tarea Implementación de agente
- ESET Remote Deployment Tool

RD Sensor no detecta todos los clientes de la red.

El RD Sensor detecta la comunicación de red de forma pasiva en la red. RD Sensor no muestra los PC que no se comunican. Verifique la configuración de DNS para asegurarse de que los problemas con la búsqueda de DNS no

están evitando la comunicación.

¿Cómo puede restablecerse el contador de detecciones activas que se muestra en ESET PROTECT On-Prem después de la desinfección de detecciones?

Para restablecer el número de detecciones activas, debe iniciarse un análisis exhaustivo a través de ESET PROTECT On-Prem en los ordenadores de destino. Si ha desinfectado una detección manualmente, puede marcarla como resuelta.

¿Cómo puede configurarse la expresión CRON para el intervalo de conexión de ESET Management Agent?

P_REPLICATION_INTERVAL acepta una expresión CRON.

El valor predeterminado es "R R/20 * * * ? *" que implica conectar en un segundo aleatorio (R=0-60) cada 20 minutos aleatorios (por ejemplo,3, 23, 43 o 17,37,57). Deben emplearse valores aleatorios para equilibrar la carga en el tiempo. Por lo tanto, cada ESET Management Agent se conecta en un momento aleatorio 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 más información, consulte Intervalo de la expresión CRON.

¿Cómo puede crearse un grupo dinámico para implementación automática?

Consulte nuestro artículo de la base de conocimiento para obtener instrucciones paso a paso.

¿Cuál es el formato de archivo requerido al importar un archivo con una lista de ordenadores para añadirlos a ESET PROTECT On-Prem?

Archivo con las líneas siguientes:

All\Grupo1\GrupoN\Ordenador1
All\Grupo1\GrupoM\OrdenadorX

All es el nombre necesario del grupo raíz.

¿Qué certificados de terceros se pueden usar para firmar certificados de ESET PROTECT?

El certificado debe ser un certificado de CA (o de CA intermedia) con el indicador 'keyCertSign' de la restricción 'keyUsage'. Esto implica que puede usarse para firmar otros certificados.

¿Cómo puedo restablecer la contraseña de administrador para Web Console (introducida durante la configuración en sistemas operativos Windows)?

Es posible restablecer la contraseña mediante la ejecución del instalador del servidor y, después, eligiendo

Reparar. Tenga en cuenta que puede necesitar la contraseña de la base de datos de ESET PROTECT si no usó la autenticación de Windows durante la creación de la base de datos. Consulte el artículo de la base de conocimiento sobre este tema.

- Tenga cuidado, algunas opciones de reparación pueden eliminar datos almacenados.
- El restablecimiento de la contraseña desactiva la autenticación de doble factor.

¿Cómo puedo **restablecer** la **contraseña de administrador** de Web Console (Linux, introducida durante la configuración)?

Si tiene otro usuario en ESET PROTECT On-Prem con suficientes derechos, debe tener la capacidad de restablecer la contraseña de la cuenta de administrador. Sin embargo, si la cuenta de administrador es la única cuenta (puesto que se crea en la instalación) del sistema, no se puede restablecer esta contraseña. Consulte el artículo de la base de conocimiento sobre este tema.

¿Cómo puedo solucionar problemas si **RD Sensor** no detecta nada?

Si se detecta su sistema operativo como un dispositivo de red, no se enviará a ESET PROTECT On-Prem como un ordenador. Los dispositivos de red (impresoras, routers) son filtrados. RD Sensor se compiló con *libpcap version 1.3.0*, verifique que tiene esta versión instalada en su sistema. El segundo requisito es una red puente desde su máquina virtual en la que RD Sensor está instalado. Si se cumplen estos requisitos, ejecute nmap con detección de sistema operativo (http://nmap.org/book/osdetect-usage.html) para comprobar si puede detectar el sistema operativo de su sistema.

No veo elementos en la ventana Plantillas de grupos dinámicos. ¿Por qué?

Lo más probable es que sus usuarios no tengan permisos suficientes. 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 Panel principal. ¿Por qué?

Lo más probable es que sus usuarios no tengan permisos suficientes. 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 de ESET?

Utilice la tarea Instalación del software y seleccione el producto que quiera 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 desea cambiar el sufijo *era*, no cambie nunca el nombre de la carpeta en sí. No se recomienda modificar la dirección pero, si lo necesita, cree un vínculo en la carpeta *webapps* con un nombre distinto.

Por ejemplo, en Linux o en un dispositivo virtual, puede usar el siguiente comando:
`ln -sf /var/lib/tomcat/webapps/era/ /var/lib/tomcat/webapps/protect`

Tras ejecutar este comando en el terminal, se puede acceder a la Consola web también desde 10.1.0.5/protect (cambie la dirección IP a la que desee).

Acerca de ESET PROTECT On-Prem

Para abrir la ventana **Acerca de**, desplácese hasta **Ayuda** > **Acerca de**. Esta ventana contiene detalles acerca de la versión de ESET PROTECT On-Prem. En la parte superior de la ventana se muestra información sobre el número de dispositivos cliente conectados y el número de licencias activas. Además, se mostrará la lista de módulos del programa instalados, su sistema operativo y la licencia que utiliza ESET PROTECT On-Prem para descargar las actualizaciones de los módulos (la misma licencia utilizada para activar ESET PROTECT On-Prem). En esta ventana se muestra información sobre su base de datos, como el nombre, la versión, el tamaño, el nombre de host y los usuarios.

Para obtener instrucciones para identificar la versión de un componente de ESET PROTECT, consulte el artículo de nuestra Base de conocimiento.

Acuerdo de licencia para el usuario final

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

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

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

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

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

documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos

como persona interesada. También puede visitarla desde la sección de ayuda del Software.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS, CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

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

15. **Soporte técnico**. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

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

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

ANEXO AL ACUERDO

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

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

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

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Política de privacidad

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

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

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

- La administración de los productos de seguridad de ESET requiere y almacena de manera local información como el ID y el nombre del puesto, el nombre del producto, información sobre la licencia, información de activación y caducidad, información de hardware y software relativa al ordenador administrado con el producto

de seguridad de ESET instalado. Se recopilan registros relacionados con las actividades de los productos y de seguridad de ESET y los dispositivos administrados, y están disponibles para facilitar las funciones y los servicios de administración sin envío automatizado a ESET.

• Información relativa al proceso de instalación, incluida la plataforma en la que se instala nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como la huella digital de hardware, los ID de instalación, los volcados de bloqueo, los ID de licencia, la dirección IP, la dirección MAC, los ajustes de configuración del producto, lo que también podría incluir los dispositivos administrados.

• La información sobre licencias, como el ID de licencia, y datos personales como el nombre, los apellidos, la dirección y la dirección de correo electrónico son necesarios para la facturación, la verificación de la autenticidad de las licencias y la prestación de nuestros servicios.

• La información de contacto y los datos contenidos en sus solicitudes de soporte pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Es posible que le pidamos que nos facilite otra información para prestar el servicio de asistencia técnica, como los archivos de registro generados.

• Los datos relativos al uso de nuestros servicios son totalmente anónimos al finalizar la sesión. Una vez concluida la sesión, no se guarda ningún tipo de información personal.

Confidencialidad de los datos

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

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

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

Derechos del titular de los datos.

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

• derecho a solicitar a ESET acceso a sus datos personales;

• derecho de rectificación de sus datos personales en caso de que sean incorrectos (también tiene derecho a

completarlos en caso de que estén incompletos);

- derecho a solicitar la eliminación de sus datos personales;
- derecho a solicitar la restricción del procesamiento de sus datos personales;
- derecho a oponerse al procesamiento;
- derecho a presentar una reclamación y
- derecho a la portabilidad de datos.

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

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