ESET PROTECT

Manual de usuario

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

Digital Security
Progress. Protected.

Copyright ©2024 de ESET, spol. s r.o.

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

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

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación ni transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de aplicación descrito sin previo aviso.

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

REV. 17/04/2024

1 Introducción a ESET PROTECT 1
1.1 Acerca de la ayuda 3
1.1 Leyenda de los iconos 4
1.2 Nuevas funciones de ESET PROTECT 5
1.3 Notas de la versión 6
1.4 Navegadores web, productos de seguridad de ESET e idiomas compatibles 30
1.5 Sistemas operativos compatibles 32
1.6 Requisitos previos de la red 33
1.7 Disponibilidad del servicio 34
1.8 Diferencias entre la consola de administración local y la de la nube 35
2 Introducción a ESET PROTECT 36
2.1 Crear una nueva instancia de ESET PROTECT con ESET Business Account 37
2.2 Crear un nuevoESET PROTECT usuario en ESET Business Account 40
2.3 ESET PROTECT Web Console 43
2.3 Pantalla de inicio de sesión 47
2.3 Recorrido por ESET PROTECT 48
2.3 Configurar protección 49
2.3 Configuración del usuario 52
2.3 Filtros y personalización del diseño 54
2.3 Etiquetas 57
2.3 Importar CSV 60
2.3 Solución de problemas: Web Console 61
2.3 Funciones de vista previa 63
2.4 Sincronizar ESET PROTECT con Active Directory 64
2.5 Cómo administrar productos Endpoint desde ESET PROTECT 68
2.6 ESET Push Notification Service 69
3 VDI, clonación y detección de hardware 70
3.1 Resolución de preguntas de clonación 74
3.2 Identificación de hardware 76
3.3 Maestro para clonación 77
4 ESET BridgeProxy HTTP - 79
5 ESET Management Implementación de agente 79
5.1 Agregar ordenadores con RD Sensor 80
5.1 Instalación de RD Sensor 81
5.1 Configuración de políticas de ESET Rogue Detection Sensor 83
5.2 Implementación local 84
5.2 Crear instalador del agente y el producto de seguridad de ESET 84
5.2 comportamiento Live Installer 89
5.2 Crear instalador de scripts del agente 90
5.2 Implementación del agente: Linux 91
5.2 Implementación del agente: macOS 93
5.3 Implementación remota 94
5.3 Implementación del agente con GPO o SCCM 95
5.3 Pasos de implementación - SCCM 96
5.3 ESET Remote Deployment Tool 113
5.3 Requisitos previos de la Herramienta de implementación remota de ESET 114
5.3 Seleccionar ordenadores en Active Directory 114
5.3 Analizar la red local en busca de ordenadores 117
5.3 Importar una lista de ordenadores 119
5.3 Agregar ordenadores manualmente 121

5.3 ESET Remote Deployment Tool: resolución de problemas 123
5.4 Protección del agente 123
5.5 Configuración de ESET Management Agent 124
5.5 Crear una directiva para activar la protección por contraseña de ESET Management Agent 125
5.6 Resolución de problemas - Conexión con el agente 127
6 ESET PROTECT Menú principal 128
6.1 Consola 129
6.1 Profundizar 135
6.2 Clientes administrados 137
6.3 Ordenadores 138
6.3 Detalles del ordenador 140
6.3 Vista previa del ordenador 147
6.3 Quitar ordenador de administración 148
6.3 Tráfico inusualmente elevado desde ordenadores administrados 150
6.3 Grupos 150
6.3 Acciones de grupo 151
6.3 Detalles de grupo 152
6.3 Grupos estáticos 152
6.3 Cree un grupo estático nuevo 153
6.3 Exportar grupos estáticos 155
6.3 Importar grupos estáticos 156
6.3 Árbol de grupos estáticos para ESET Business Account/ESET MSP Administrator 158
6.3 Grupos dinámicos 160
6.3 Crear un grupo dinámico nuevo 161
6.3 Mover grupo estático o dinámico 163
6.3 Asignar una tarea del cliente a un grupo 165
6.3 Asignar una política a un grupo 166
6.4 Detecciones 167
6.4 Administrar detecciones 170
6.4 Vista previa de la detección 171
6.4 Crear exclusión 172
6.4 Productos de seguridad de ESET compatibles con las exclusiones 175
6.4 Protección contra ransomware 175
6.4 ESET Inspect 176
6.5 Vulnerabilidades 177
6.5 Aplicaciones cubiertas por Vulnerabilidades 181
6.6 Administración de revisiones 181
6.6 Aplicaciones cubiertas por Administración de revisiones 185
6.7 Informes 185
6.7 Crear una nueva plantilla de informe 188
6.7 Generar informes 191
6.7 Planificar un informe 192
6.7 ESET MDR 193
6.7 Archivo de informe MDR 195
6.7 Aplicaciones obsoletas 197
6.7 Visor de registros de SysInspector 198
6.7 Inventario de hardware 199
6.7 Informe de registros de auditoría 201
6.8 Tareas 201
6.8 Información general de las tareas 204
6.8 Indicador de progreso 205

6.8 Icono de estado ... 206
6.8 Detalles de la tarea ... 206
6.8 Tareas del cliente ... 209
6.8 Desencadenadores de la tarea del cliente ... 211
6.8 Asignar una tarea del cliente a grupos u ordenadores ... 213
6.8 Acciones Anti-Theft ... 214
6.8 Buscar actualizaciones del producto ... 216
6.8 Diagnóstico ... 217
6.8 Mensaje de visualización ... 219
6.8 Finalizar aislamiento del ordenador de la red ... 220
6.8 Exportar configuración de productos administrados ... 221
6.8 Aislar ordenador de la red ... 222
6.8 Cerrar sesión ... 224
6.8 Actualización de módulos ... 225
6.8 Reversión de la actualización de módulos ... 226
6.8 Análisis a petición ... 227
6.8 Actualización del sistema operativo ... 229
6.8 Administración de la cuarentena ... 231
6.8 Activación del producto ... 233
6.8 Reiniciar agente clonado ... 234
6.8 Restablecimiento de la base de datos de Rogue Detection Sensor ... 235
6.8 Ejecutar comando ... 236
6.8 Ejecutar script de SysInspector ... 238
6.8 Enviar archivo a ESET LiveGuard ... 239
6.8 Análisis del servidor ... 239
6.8 Apagar el ordenador ... 241
6.8 Instalación del software ... 242
6.8 Software de Safetica ... 245
6.8 Desinstalación del software ... 246
6.8 Detener administración (desinstalar ESET Management Agent) ... 248
6.8 Solicitud de registro de SysInspector (solo Windows) ... 250
6.8 Actualizar agente ... 251
6.8 Cargar archivo en cuarentena ... 252
6.8 Tareas del servidor ... 254
6.8 Eliminar ordenadores que no se conecten ... 255
6.8 Generar informe ... 257
6.8 Cambiar nombre de los ordenadores ... 258
6.8 Tipos de desencadenadores de tarea ... 260
6.8 Intervalo de la expresión CRON ... 262
6.8 Configuración avanzada: Límites ... 264
6.8 Ejemplos de aceleración ... 268
6.9 Instaladores ... 270
6.10 Políticas ... 273
6.10 Asistente para políticas ... 275
6.10 Indicadores ... 277
6.10 Administrar políticas ... 279
6.10 Cómo se aplican las políticas a los clientes ... 279
6.10 Orden de los grupos ... 280
6.10 Enumeración de políticas ... 281
6.10 Fusión de políticas ... 282
6.10 Situación hipotética de fusión de políticas ... 283

6.10 Configuración de un producto desde ESET PROTECT 287
6.10 Asignar una directiva a un grupo 288
6.10 Asignar una política a un cliente 289
6.10 Cómo utilizar el modo de anulación 291
6.11 Notificaciones 293
6.11 Administrar notificaciones 294
6.11 Sucesos en ordenadores o grupos administrados 296
6.11 Cambios de estado del servidor 297
6.11 Cambios en el grupo dinámico 298
6.11 Distribución 298
6.12 Resumen del estado 301
6.13 Soluciones ESET 302
6.13 Activar ESET LiveGuard Advanced 303
6.13 Activar ESET Full Disk Encryption 306
6.14 Más 307
6.14 Archivos enviados 307
6.14 Exclusiones 309
6.14 Cuarentena 311
6.14 Usuarios del ordenador 313
6.14 Agregar nuevos usuarios 314
6.14 Modificar usuarios 316
6.14 Crear un nuevo grupo de usuarios 318
6.14 Plantillas de grupos dinámicos 319
6.14 Nueva plantilla de grupo dinámico 320
6.14 Reglas de una plantilla de grupo dinámico 321
6.14 Operaciones 322
6.14 Reglas y conectores lógicos 322
6.14 Evaluación de las reglas de una plantilla 324
6.14 Plantilla de grupo dinámico - ejemplos 326
6.14 Grupo dinámico - hay un producto de seguridad instalado 327
6.14 Grupo dinámico - hay una versión de software concreta instalada 328
6.14 Grupo dinámico - no está instalada una versión concreta de una software 329
6.14 Grupo dinámico - no está instalada una versión concreta de una software, pero sí otra 330
6.14 Grupo dinámico - un ordenador está en una subred concreta 331
6.14 Grupo dinámico - versión instalada pero no activada de producto de seguridad para servidor 331
6.14 Cómo automatizar ESET PROTECT 332
6.14 Administración de licencias 334
6.14 Licencias válidas para nube 338
6.14 Derechos de acceso 338
6.14 Usuarios 339
6.14 Acciones y detalles del usuario 342
6.14 Usuarios asignados 343
6.14 Asignar un conjunto de permisos a un usuario 346
6.14 Conjuntos de permisos 348
6.14 Administrar conjuntos de permisos 350
6.14 Lista de permisos 352
6.14 Registro de auditoría 356
6.14 Configuración 358
6.14 Exportar registros a Syslog 359
6.14 Servidor de Syslog 360
6.14 Restricciones y límites de seguridad de syslog 361

6.14 Eventos exportados a formato JSON ... 362
6.14 Eventos exportados a formato LEEF ... 370
6.14 Eventos exportados a formato CEF ... 371
7 ESET PROTECT para proveedores de servicios administrados (MSP) ... 379
7.1 Funciones de ESET PROTECT para usuarios MSP ... 381
7.2 Crear un nuevoESET PROTECT usuario en ESET MSP Administrator ... 382
7.3 Proceso de implementación para MSP ... 384
7.3 Implementación local del agente ... 385
7.3 Implementación remota del agente ... 385
7.4 Licencias MSP ... 386
7.5 Iniciar configuración de cliente MSP ... 388
7.6 Omitir configuración de cliente MSP ... 392
7.7 Crear un instalador personalizado ... 393
7.8 Usuarios MSP ... 394
7.9 Etiquetado de objetos MSP ... 396
7.10 Resumen del estado de MSP ... 397
8 Cloud Mobile Device Management ... 398
8.1 Inscripción: agregar dispositivos móviles ... 399
8.1 Inscripción de dispositivo Android ... 404
8.1 Inscripción de Android: propietario del dispositivo ... 414
8.1 Inscripción de dispositivo iOS ... 420
8.1 Inscripción con Microsoft Entra ID (Android o iOS) ... 429
8.1 Sincronización con Microsoft Intune (Android) ... 431
8.1 Sincronización con VMware Workspace ONE (Android) ... 433
8.1 Sincronización de Apple Business Manager (ABM) (iOS) ... 437
8.2 Administrar dispositivos móviles ... 441
8.2 Control de acceso web para Android ... 442
8.2 Administración de actualizaciones del sistema operativo ... 443
8.2 Crear una directiva para el iOS: cuenta de Exchange ActiveSync ... 444
8.2 Crear una directiva para aplicar restricciones a iOS y añadir conexión Wi-Fi ... 449
8.2 Perfiles de configuración del Cloud MDM ... 453
8.3 Migración a Cloud MDM (desde ESET PROTECT on-prem) ... 454
9 Casos de migración ESET PROTECT ... 455
9.1 Migración parcial de ESET PROTECT on-prem a ESET PROTECT ... 457
9.2 Migración en la nube: de un ESET PROTECT a otro ESET PROTECT ... 471
10 Cómo eliminar ESET PROTECT de la red ... 475
10.1 Caducidad de la última licencia de ESET PROTECT ... 477
11 Actualizaciones automáticas ... 478
11.1 Actualización automática de ESET Management Agent ... 479
11.2 Actualización automática de los productos de seguridad de ESET ... 479
11.2 Configurar las actualizaciones automáticas del producto ... 482
12 Acerca de ESET PROTECT ... 484
13 ESET Connect (API) ... 484
14 Preguntas frecuentes sobre Administración de revisiones y vulnerabilidades ... 484
15 Seguridad para ESET PROTECT ... 487
16 Términos de uso ... 491
16.1 Acuerdo de licencia para el usuario final de ESET Management Agent ... 496
16.2 Acuerdo de procesamiento de datos ... 503
16.3 Cláusulas contractuales tipo ... 505
17 Política de privacidad ... 530

Introducción a ESET PROTECT

Le damos la bienvenida a ESET PROTECT. ESET PROTECT le permite administrar productos de ESET en estaciones de trabajo y servidores en un entorno de red con hasta 50.000 dispositivos 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 amenazas 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.

Para empezar a utilizar ESET PROTECT, consulte Introducción a ESET PROTECT.

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 está compuesto por los siguientes componentes:

ESET PROTECT como servicio

ESET PROTECT Web Console

- La consola web interpreta los datos almacenados en la base de datos de ESET PROTECT. Muestra estas enormes cantidades de datos organizados en paneles principales e informes claros, y también aplica políticas y ejecuta tareas en agentes y otras aplicaciones de ESET.

Live Installer

- Es una pequeña aplicación que contiene ESET Management Agent y la opción de incluir un producto para punto de conexión empresarial en un paquete optimizado y fácil de usar.

- ESET Management Agent es una pequeña aplicación sin interfaz gráfica de usuario que ejecuta los comandos de ESET PROTECT en los clientes conectados. Ejecuta las tareas, recopila los registros de las aplicaciones de ESET, interpreta y aplica políticas y realiza otras tareas válidas, como la implementación de software y la supervisión general del ordenador.

- Es un paquete preconfigurado que se puede descargar fácilmente y contiene un agente y el producto de seguridad en forma de instalador optimizado que se conecta automáticamente a la instancia adecuada en la nube y se activa con una licencia válida mediante una interacción mínima del usuario. El instalador identificará la plataforma correcta y descargará el paquete del producto de seguridad adecuado.

- El agente es una aplicación ligera que facilita toda la comunicación entre el producto de seguridad de ESET del ordenador cliente y ESET PROTECT.

Productos de seguridad de ESET

- Los productos de seguridad de ESET protegen de amenazas los ordenadores cliente y los servidores.
- ESET PROTECT es compatible con los siguientes productos de seguridad de ESET.

ESET Business Account

- Puerta de entrada central para clientes empresariales o un proveedor de identidad para ESET PROTECT.
- Funciona como inicio de sesión único para que los clientes empresariales vean sus licencias y los servicios activados, ejecuten la administración de usuarios, etc.
- Es necesario ESET Business Account para activar la instancia de ESET PROTECT
- 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.

ESET Remote Deployment Tool

- Una herramienta que puede implementar Live Installer en la red de forma remota.
- Puede asignar la red y sincronizarse con Active Directory de forma remota o permitir la importación de destinos en los que se implementará el producto.

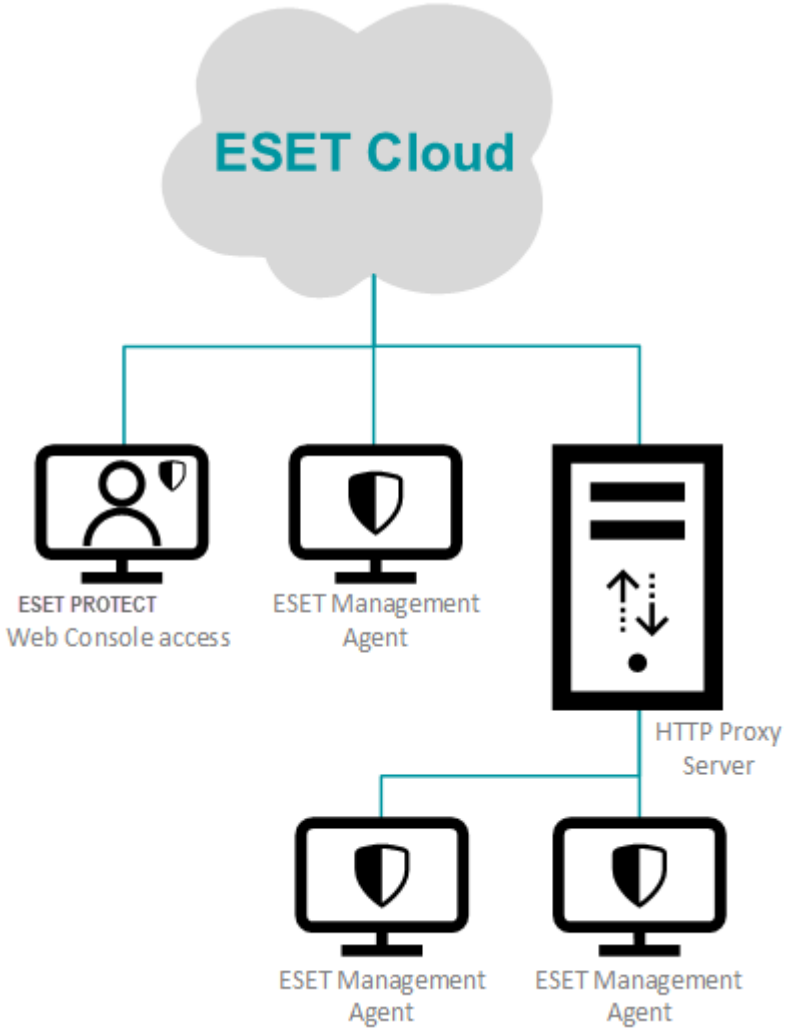
ESET Bridge (HTTP Proxy) –Puede utilizar ESET Bridge con ESET PROTECT como servicio proxy para:

- Descarga y almacena en caché: actualizaciones de los módulos de ESET, paquetes de instalación y actualización enviados por ESET PROTECT (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.

ESET Active Directory Scanner: sincronice ordenadores y usuarios de Active Directory con ESET PROTECT Web Console.

ESET Cloud Mobile Device Management (Cloud MDM) – ofrece administración de dispositivos móviles Android y iOS y administración de seguridad móvil.

En el siguiente diagrama se muestra la arquitectura de ESET PROTECT simplificada:



Acerca de la ayuda

La Guía de administración se escribió para ayudarle a familiarizarse con ESET PROTECT 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. 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.
- 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.
- 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.

Icono de estado	Descripciones
	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.
	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; 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 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 lo que desea importar.
	Exportar: seleccione en Informes/Políticas 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
	Servidor de correo
	Servidor de puerta de enlace
	Servidor de colaboración
	ESET Management Agent
	Conector del dispositivo móvil
	Rogue Detection Sensor
	ESET Bridge
	Tipo de detección de **antivirus**. Consulte todos los tipos de detección en Detecciones. Haga clic en un ordenador y seleccione **Soluciones** > **Activar producto de seguridad** para activar 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** para implementar ESET Inspect Connector en los ordenadores Windows/Linux/macOS administrados. El ESET Inspect solo está disponible cuando tiene la licencia de ESET Inspect y ESET Inspect está conectado a ESET PROTECT. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a 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.
	Vulnerabilidades
	Administración de revisiones

Nuevas funciones de ESET PROTECT

Panel de control de MDR e informe semanal

Para los clientes que utilizan el servicio de ESET MDR, presentamos el nuevo panel de MDR. Este panel recopila y muestra en tiempo real los datos importantes relacionados con el control y la búsqueda de amenazas 24 horas. Además, recibirá en su correo electrónico informes semanales periódicos con las instantáneas de datos más recientes. También se puede acceder a estos informes, que se archivan automáticamente para mayor comodidad, en la sección Informes. Obtener más información

Inscripción de dispositivos móviles con Microsoft Entra ID

Hemos agregado la opción de inscribir dispositivos móviles en ESET PROTECT a través de Microsoft Entra ID. Gracias a este método de inscripción simplificado, ya no hace falta generar códigos únicos por dispositivo. Ahora puede inscribir fácilmente todos sus dispositivos móviles con un solo enlace o código QR, que se envía por correo electrónico o a través del canal que desee. Obtener más información

Otras mejoras y correcciones de errores

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

Notas de la versión

Las notas de la versión solo están disponibles en inglés.

ESET PROTECT 5.2

Release date: April, 2024

- ADDED: MDR dashboard that displays real-time data for customers with the ESET MDR service
- ADDED: Weekly MDR report email sent automatically to customers with the ESET MDR service
- ADDED: Archive of MDR reports for customers with the ESET MDR service
- ADDED: Ability to enroll all mobile devices with one enrollment link or QR code via Microsoft Entra ID enrollment
- IMPROVED: Post-installation restart is not required for Linux products (ESET Endpoint Antivirus for Linux and ESET Server Security for Linux)
- IMPROVED: Using Google Play version of ESET Endpoint Security for Android instead of a web version when enrolling a mobile device in Device Owner mode
- FIXED: Error message displayed when opening the details or editing a server task with a trigger other than "Generate report"
- FIXED: Incorrect headline displayed in the webhook notifications sent to Microsoft Teams
- FIXED: Displaying "Product not installed" alert for "Common features" policies in some instances
- FIXED: No information about the mobile network is displayed when the device has multiple SIMs/eSIMs
- Other minor improvements and bug fixes

ESET PROTECT 5.1

Release date: February, 2024

- ADDED: Vulnerability & Patch Management for Windows servers (requires ESET Server Security for Microsoft Windows Server version 11.0 and later)
- ADDED: Enhanced ESET LiveGuard behavioral reports with detailed behavior of the sample (available for customers with ESET Inspect)
- IMPROVED: Migration of static group hierarchies from on-premises to cloud in large and MSP environments
- IMPROVED: Ability to send "ESET Inspect incidents" notification for all incident authors

- IMPROVED: Clarified wording related to Vulnerability & Patch Management
- FIXED: Incorrect installation date reported for Linux product
- FIXED: Table scrolling does not work after opening Details
- FIXED: Incorrect display of license time remaining before expiration next to the license end date in Computer Details
- Other minor improvements and bug fixes

ESET PROTECT 5.0

Release date: December, 2023

- ADDED: Name change for ESET PROTECT Cloud to ESET PROTECT
- ADDED: Enable automatic operating system updates (part of Vulnerability & Patch Management)
- ADDED: New preset policy with automatic operating system updates (part of Vulnerability & Patch Management)
- ADDED: Ability to download ESET LiveGuard behavioral reports
- ADDED: Option to send a notification to non-activated devices enrolled via Workspace ONE or Microsoft Intune (MDM)
- IMPROVED: Patch management restarts added to the Automatic problem resolving setting
- IMPROVED: Users with access to server settings can delegate access rights to other users for viewing and modifying the server settings
- IMPROVED: Devices API contains information about the BIOS serial number
- IMPROVED: New version of AV Remover in the Management Agent
- FIXED: Incorrect Dynamic Groups evaluation behavior on Agent startup
- FIXED: Devices API does not report installed security products
- REMOVED: Support for macOS Sierra (10.12), High Sierra (10.13) and Mojave (10.14)
- REMOVED: Support for Windows 7, 8 and 8.1
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.7

Release date: October, 2023

- ADDED: New REST API for ESET PROTECT Cloud
- IMPROVED: New information for MSP administrators about the MSP managing company in the All-in-one

installer

- FIXED: Agents lost connection after migration, followed by an upgrade
- FIXED: Agent service fails to stop in time, or system restart takes longer than expected in specific cases
- FIXED: Agent for macOS is not correctly reporting the system build number in specific cases
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.6

Release date: August, 2023

- ADDED: Setting time slots in Dynamic groups
- ADDED: Enrolling Android mobile devices from Workspace ONE
- IMPROVED: Added new setting in the ESET LiveGuard Basic built-in policy regarding the automatic document submissions (set to OFF by default)
- IMPROVED: Visual enhancements in the patches list in Patch Management
- IMPROVED: Added language settings for the mobile device enrollment email
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.5

Release date: July, 2023

- ADDED: ESET Vulnerability & Patch Management - a new protection layer monitoring vulnerabilities with the ability to patch all endpoints managed through our platform (requires ESET Endpoint Antivirus/Security for Windows version 10.1 and later)
- ADDED: New setting in "Set up your protection" wizard regarding ESET LiveGuard for new and existing customers
- ADDED: New Client task - Check for product update (requires ESET Endpoint Antivirus/Security for Windows version 10.1 and above)
- ADDED: The ability to test send email and webhook notifications
- ADDED: Webhook authentication to verify the credibility of the webhook notification
- IMPROVED: New version of the Log Collector in the Management Agent
- FIXED: Negative filter applied to the list of computers still visible after clearing the filters
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.4

Release date: June, 2023

- ADDED: New dashboard for customers using ESET Cloud Office Security
- ADDED: Data filter per customer for MSP administrators in the Dashboard section
- ADDED: New section for MSP administrators, "Managed Customers", offering an overview of all managed customers
- ADDED: Ability for MSP administrators to filter report templates per customer when creating scheduled reports
- ADDED: New delivery method for notifications - webhooks
- ADDED: New branding visuals within the console
- IMPROVED: Easier search within the console with no need to first choose a category
- IMPROVED: Ability to filter policies by name
- IMPROVED: Information about the creation and download of installers added to the Audit Log
- IMPROVED: MSP customers ready for a set up distinguished by an icon
- IMPROVED: Asynchronous sending of enrollment emails during the mobile device enrollment
- IMPROVED: Wi-fi settings available via QR code during Device owner enrollment (MDM)
- IMPROVED: New version of the AV Remover and Log Collector in the Management Agent
- CHANGED: The "Auto-updates" policy will become a part of the "Common features" policy when the new Configuration module is released (planned for July)
- FIXED: Creating a dynamic group template based on a value "LiveGuard is not working due to a license problem" not functioning properly
- FIXED: Dynamic group template based on a value "macOS is preventing the ESET security product from accessing some folders" not working properly
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.3

Release date: April, 2023

- ADDED: An MDR Report Template for offices and partners delivering ESET Services
- ADDED: A column for mobile device IMEIs in the device list and the possibility to filter the devices by IMEI
- ADDED: The ability to combine Computer name, Database version and Last connection in one report

- IMPROVED: Extended certificate validity for mobile devices - devices do not need to connect to an MDM server frequently to stay protected
- FIXED: Issues with displaying the Product Tour in the Safari browser
- FIXED: Various localization bugs
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.2

Release date: February, 2023

- ADDED: Detections are grouped by common attributes
- ADDED: Migration of mobile devices to cloud MDM
- ADDED: Syslog includes the operating system of a computer, and the full hierarchy and description of a static group
- ADDED: Product Navigator has a link to ESET Cloud Office Security (available later in April 2023)
- IMPROVED: Active Directory Synchronization (time of last sync, ability to deactivate and regenerate token)
- FIXED: Incorrect filter behavior when multiple license statuses are selected
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 4.1

Release date: January, 2023

- ADDED: Enrollment support for Android mobile devices via Microsoft Intune Management Console
- ADDED: Column "Investigated by ESET" in incident overview in the ESET Inspect dashboard
- ADDED: Ability to add column FQDN and Serial Number in the Computers section
- IMPROVED: Size values in Submitted Files
- FIXED: Inability to resolve/unresolve detections when the parent group is selected in the tree
- FIXED: Incorrect encryption process (EFDE) status in the ESET Solutions section
- FIXED: Wrong ESET LiveGuard license was shown while editing the existing software install task
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 4.0

Release date: November, 2022

- ADDED: Basic incident overview in the ESET Inspect dashboard

- ADDED: CEF format for Syslog
- ADDED: Reporting of absolute and relative free space for hard drives in HW inventory
- ADDED: Log out action in the Computer context menu (under Power)
- ADDED: Log out Client Task
- ADDED: Ability to filter Computers by FQDN
- ADDED: Ability to filter Computers by Serial Number
- ADDED: Last boot time in computer details
- ADDED: Ability to deploy LiveGuard on all devices in a static group via context menu action
- ADDED: Ability to reset default filters
- ADDED: Static Group name in Syslog events
- ADDED: Ability to see the progress of removing client tasks
- ADDED: Ability to filter unassigned policies in the Policies section
- ADDED: Ability to sort policies in the "Last Modified By" column
- ADDED: Support for time-elapsed (duration) filters in Dynamic Groups
- ADDED: Comma separator for thousands place in table numbers
- IMPROVED: Table numbers are now aligned right
- IMPROVED: Selecting a product from the repository in the Software Install task
- IMPROVED: "Deploy ESET LiveGuard" through the computer's or group's context menu now leverages a better mechanism that is used in the dedicated ESET Solutions section
- IMPROVED: Filtering by Detection Type
- IMPROVED: New version of Log Collector (version 4.6.0.0) in Management Agent
- IMPROVED: Solutions deployment supports computers in site/company location based on hierarchy
- IMPROVED: Example section in the "Select time interval" filter
- CHANGED: Limit from 100 to 1000 when opening selected objects
- CHANGED: Disabled optional use OPAL in built-in encryption policy "Encrypt all disks - Recommended"
- FIXED: The license list occasionally disappears when scrolling through a long License Management list
- FIXED: The date/time filter does not work correctly on the localized web console
- FIXED: All policies are hidden except auto-update when logging in to the console for the first time

- FIXED: Info message about default value for time-based criteria in Notifications is shown when it is not mandatory
- FIXED: Network adapter(s) screen informs that the latest version of an agent is required, even though the latest version is installed
- FIXED: Default presets for Computers/Detections sections are overwritten in a special scenario
- FIXED: Inaccurate problem count in License Management badge in specific scenarios
- FIXED: Missing limit for quarantine management actions, which causes an error message in some cases
- FIXED: HW inventory reports the TPM manufacturer version instead of the specification version
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.5

Release date: September, 2022

- ADDED: Initial configuration (Set up protection)
- ADDED: Dark theme
- ADDED: Ability to switch between Absolute and Relative time in tables
- ADDED: Ability to add column Hash in Detections section
- ADDED: Ability to search by Hash in the Detections section
- ADDED: Ability to search by Object in the Detections section
- ADDED: Ability to distinguish, whether BitLocker is activated on a particular machine
- ADDED: Filtering options in Computer details - Installed Applications screen
- ADDED: Computer preview - the ability to reset displayed sections into default
- ADDED: Ability to modify Computer name and Description directly from the Computer preview panel
- ADDED: Ability to mute/unmute Computer directly from the Computer preview panel
- ADDED: Section name as a prefix in the browser tab title
- IMPROVED: VDI support (mostly improvements around instant clones)
- IMPROVED: Network Adapters (part of Computer details - Details - Hardware) are more readable in the case of IPv4/IPv6
- IMPROVED: Multiplatform support when deploying or enabling features via Solutions in the Computer context menu
- IMPROVED: Displaying of Inspect button is now dependent on the permission set "Access to ESET Inspect"

- IMPROVED: Filter Advisor remembers item sorting
- IMPROVED: Information in the Detection type column was split into two separate columns Detection Category and Type
- IMPROVED: Creation of New Report Template for newly created Report category
- FIXED: Save filter set is not working correctly in all sections
- FIXED: Specific scenario causes license sync breakage (if static group below company has the same name as a site that is going to be created in EBA)
- FIXED: When you load a saved filter set, it is not applied unless you edit it (various sections)
- FIXED: Filter "≤ # OF ALERTS" is not working correctly (Computers section)
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.4

Release date: June, 2022

- ADDED: Advanced Filters in the Computers section
- ADDED: Native ARM64 support for ESET Management Agent for macOS
- ADDED: "Waiting" state in the Component version status section on Status Overview for better communication of auto-updates (available from ESET Endpoint Antivirus/Security for Windows version 9.1)
- ADDED: Site structure from ESET Business Account synchronizes in the static group tree
- ADDED: New rebooting option-administrator can set up reboots in a way that the end-users can postpone them (available from ESET Endpoint Antivirus/Security for Windows version 9.1)
- ADDED: Information on how many more devices can enable ESET LiveGuard on the ESET LiveGuard Dashboard
- ADDED: Dark Theme preview feature
- ADDED: Limited-input device-simple enrollment flow for Android-based devices that do not have access to emails or a camera for scanning QR codes
- ADDED: Support for deployment of the latest version in the software installation task (the latest version at the moment of task execution, it is not necessary to select a specific version anymore)
- ADDED: Creation date column in the Installers section
- ADDED: Reset functionality for columns in tables
- ADDED: Warning to Audit log access right
- ADDED: "Installation Date" column in Computer details - Installed Applications screen
- ADDED: Ability to select multiple monitored static groups in a single notification

- ADDED: Reporting human-readable Windows operating system version is displayed in the OS Service Pack column in the Computers section
- ADDED: OS build version collected from macOS is displayed in the OS Service Pack column in the Computers section
- ADDED: Agents tile in the Status Overview section for better identification of unmanaged computers
- ADDED: Instance ID is available in the console's About section (previously only available in ESET Business Account)
- ADDED: Console users can deploy ESET Full Disk Encryption (EFDE) on recommended (portable) devices in the ESET Solutions screen
- IMPROVED: EFDE does not deploy to devices using BitLocker for drive encryption
- IMPROVED: Reboot and shut down experience on macOS (user is notified about restart and can cancel it in 60 seconds)
- IMPROVED: Tasks planned ASAP are executed in the order in which they were created in the console
- IMPROVED: Admin password is not required when enrolling a new mobile device. However, ESET strongly recommends you use an admin password for the full functionality of certain features
- IMPROVED: Every ASAP trigger created by the user in the console must have an expiration set (less than six months)
- IMPROVED: HIPS detections now contain user and hash
- IMPROVED: New version of AVRemover and Log Collector in the Management Agent
- FIXED: Several functionality problems with the dynamic group template selector
- FIXED: Scheduled client tasks without "Invoke ASAP If Event Missed" pre-selected could be executed with the wrong timing if the computer woke up from sleep or hibernation
- FIXED: Tags assigned to a "Client Task" are automatically assigned to applicable computers
- FIXED: Unavailable EDR element in the Component version status section on the Status Overview screen
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.3

Release date: April, 2022

- ADDED: Manage up to 50,000 devices (according to purchased license)
- ADDED: Support for ESET Inspect Cloud (EDR solution)
- ADDED: Easy trial, deployment and purchase of ESET Full Disk Encryption (EFDE)
- ADDED: Preview feature - Advanced Filters in the Computers section

- ADDED: New buttons under the table in the Computers section and Detection section
- ADDED: Right-click tables to open the context menu
- ADDED: Enrollment link expiration and device certificate renewal information to the enrollment email
- ADDED: Built-in policies for V7 product for macOS and HTTP proxy
- ADDED: Ability to turn on the "Remote Host" column in the Computers section
- ADDED: Console users can configure (in Settings) the behavior of newly enrolled devices deduplication in the console
- ADDED: Console users receive an email notification that contains a link that redirects the user into the Computer details section in the console
- IMPROVED: Console users receive a notification about multiple detections occurring on managed computers aggregated in one email message
- IMPROVED: Remove button was moved behind the gear icon in the ESET Solutions section
- IMPROVED: Console users can click the chart in the ESET Solutions section and will be redirected to the Computers section
- IMPROVED: The latest versions of each product are prioritized in the product selection section of the software installation task
- IMPROVED: UI elements in tables
- CHANGED: ESET Dynamic Threat Defense to ESET LiveGuard in management consoles
- CHANGED: Remove tags icon in the Tags panel
- FIXED: Trigger for scheduled Reports cannot be edited
- FIXED: Exclusions table shows the "Occurred" column, but it is labeled as "Created on"
- FIXED: "Export table as" now exports all data, not just data on the page
- FIXED: Trigger via CRON shows different time after opening details of a specific trigger
- REMOVED: "Auto-loading" option in the Clients and Detections screen paging menu
- Various other minor bug fixes, security and performance improvements

ESET PROTECT Cloud 3.2

Release date: February, 2022

- ADDED: Easier enrollment for mobile devices
- ADDED: Easier deployment mechanism also extended for MSPs
- ADDED: New product tour

- ADDED: ESET Product Navigator to the header
- ADDED: New context menu action "Deploy ESET security product" (in Computers section)
- ADDED: AD user sync tool for ESET PROTECT Cloud
- ADDED: AD user sync-based features enabled for iOS devices
- IMPROVED: Context menu in Computers section
- IMPROVED: Installer creation Wizard
- IMPROVED: Email enrollment progress bar to indicate whether the task has been finished
- IMPROVED: Computer with IP column was divided into two columns in Submitted Files
- IMPROVED: Retention policy dialog is more user-friendly and upper limits are communicated in the Online Help guide
- FIXED: Last scan time in computer details
- FIXED: When "Module update failed" occurs, the computer is not moved to the related Dynamic Group, if the Dynamic Group was created
- FIXED: Policies under "Manage policies" over a group do not display for users with an administrator permission set
- FIXED: "Restart required" and "Inbound Communication" columns in the Detections list display incorrect values

ESET PROTECT Cloud 3.1.5

Release date: January, 2022

- ADDED: Easier deployment - the new simplified dialog for installer download, and reworked wizard for creation of the customized installer
- ADDED: Dynamic groups for mobile devices
- ADDED: Easy trial, deploy and purchase of ESET Dynamic Threat Defense (EDTD) also for MSP customers
- ADDED: Hide and Show action for EDTD Dashboard
- ADDED: Possibility to add Group Name column in the Detections section (not displayed by default)
- CHANGED: Default message contents (Computer first connected, Computer identity recovered, Computer cloning question created)
- IMPROVED: EDTD status (enabled/disabled) is reported properly to the console (requires ESET Endpoint Antivirus/Security for Windows version 9.0 and above) and leveraged in various sections (for example, action Enable is not offered for endpoint where the feature is already enabled)
- IMPROVED: Computer description can be multiline

- IMPROVED: User can define more than one naming pattern for VDI master image
- IMPROVED: Hover effect (Inverted color) on the cell with Computer name (in Computers section) and on the cell with Detection type (in Detections section)
- IMPROVED: Computer name and IP is now in separate columns in the Detection section
- FIXED: Multiple sorting does not work as expected when the top priority is assigned to the Alerts column
- FIXED: The overall status of the license might not be shown correctly in specific cases
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 3.0

Release date: October, 2021

- ADDED: Support for Automatic Product Updates (available from ESET Endpoint Antivirus/Security for Windows version 9.0)
- ADDED: Management for brute-force attack protection (available from ESET Endpoint Antivirus/Security for Windows version 9.0)
- ADDED: Easy trial, deploy and purchase of ESET Dynamic Threat Defense (EDTD)
- ADDED: Web control for Android devices
- ADDED: System updates management for Android
- ADDED: New column Logged users in Computers table
- ADDED: Windows OS build number is reported as a separate symbol (possibility to use it in Dynamic groups)
- ADDED: List of submitted files (EDTD) in Computer details, Detection and Quarantine section
- ADDED: New product categories in Component version status section on Status Overview
- ADDED: Full path to a computer in received notifications
- ADDED: Possibility disable the triggering of notifications for muted computers
- ADDED: Possibility to manage session protection (e.g., disable blocking requests from different IP addresses)
- CHANGED: Reducing and re-organizing columns in the Computers section
- IMPROVED: ESET Dynamic Threat Defense perception (added information of what was originally detected by EDTD)
- IMPROVED: Operating system update - allowing the user to postpone the required reboot
- IMPROVED: Operating system update task accessible not only from context menu over a group but also over a single device
- IMPROVED: Now is possible to visually distinguish locked policies in policies and computer details screens

(padlock icon)

- IMPROVED: When users create new permission sets, some checkboxes can grey out based on their permission (users can not give higher permission that they have)
- IMPROVED: Automatically selected newly created permission set when creating a new user
- IMPROVED: Basic support of installer file caching in script-based Agent Live Installers
- IMPROVED: Date and Time displayed in format according to language
- IMPROVED: Faster displaying of the planned flag on client tasks also after assigning to the significant amount of targets
- IMPROVED: The enrollment URL link is visible below the QR code, and the user can copy it in the enrollment wizard
- IMPROVED: New version of Log Collector in Management Agent
- FIXED: Idle session timeout was not matching settings in ESET Business Account
- FIXED: Triggers - infinite loading in some cases when the user changes trigger type
- FIXED: Unwanted machines moved during computers import
- FIXED: Missing notification about scheduled restart (macOS - osascript)
- FIXED: License is randomly changed when the software install task is edited
- FIXED: Notifications - Message preview is not displaying properly
- FIXED: macOS Big Sur, specific protections statuses are missing in dynamic groups and report templates
- FIXED: Users without access to an EDTD license cannot see the data on the EDTD Dashboard
- FIXED: Multiple sorting does not sort correctly
- FIXED: Performance issue when deleting a large number of exclusions
- FIXED: EDTD Deployment on Dynamic Group ends with error
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 2.4

Release date: August, 2021

- ADDED: Ability to manage up to 25,000 devices (according to purchased license)
- ADDED: New ESET Dynamic Threat Defense dashboard
- ADDED: Preview feature - Easy trial, deploy and purchase of ESET Dynamic Threat Defense
- ADDED: Ability to create a new trigger in client task details

- ADDED: Indicator of last connection status of managed computer (connected in last replication interval)
- ADDED: Computer preview - by clicking on computer name will be displayed side panel with the most important computer details
- ADDED: Detections preview - by clicking on detection type will be displayed side panel with the most important detection details
- CHANGED: Existing ESET Dynamic Threat Defense dashboard name change
- CHANGED: Triggers for server tasks and client tasks with frequencies lower than 15 minutes will not be allowed
- CHANGED: More granular communication of managed applications versions
- CHANGED: Automatic application of retention policy after the grace period
- CHANGED: After de-enrollment, ABM devices no longer offer the re-enroll task option
- IMPROVED: A user or a computer can only be assigned to 200 users or computers in one operation to retain adequate service responsiveness
- FIXED: Actions in the context menu for devices were disabled incorrectly (Enable ESET Dynamic Threat Defense, Network Isolation)
- FIXED: Licenses without an expiration date (for example, subscription licenses) were counted as expired in the Status Overview
- FIXED: Automatic update of company name in the console when changed in ESET Business Account or ESET MSP Administrator
- FIXED: Discrepancy in "Total number of devices" on the Dashboard compared to the total count of devices shown in the Computers tab
- FIXED: FaceID screen is now correctly skipped during ABM enrollment when selected in the wizard as one of the items to be skipped
- FIXED: "Title" in the properties of the exported PDF report

ESET PROTECT Cloud 2.3

Release date: June, 2021

- ADDED: Management of Apple devices running iOS and iPadOS, including Apple Business Manager
- ADDED: Native ARM64 support for ESET Management Agent for Windows
- ADDED: Support for VMWare Instant Clones
- ADDED: New audit information on the policy screen (Modification time, Last modified by, and Creation time)
- ADDED: Upgrade outdated operating systems in a computer group
- ADDED: Ability to copy a license Public ID to the clipboard via the context menu in license management

- ADDED: Ability to filter licenses on the license management screen based on the Public ID
- ADDED: Automatic resolution of HIPS logs
- ADDED: Computer description as a new attribute in Device Identifiers under computer details
- ADDED: Support for migration and backup of ESET Full Disk Encryption (EFDE) recovery data
- ADDED: New client task "Generate new FDE Recovery password" (available from EFDE client version 1.3 (EFDE - purchased separately))
- ADDED: Ability to retry encryption from the console if encryption fails (available from EFDE client version 1.3 (EFDE - purchased separately))
- IMPROVED: Preview feature – Computer preview (added new sections and the possibility to click on some elements and navigate to relevant details)
- IMPROVED: The Syslog export now also supports the information log level
- IMPROVED: The ESET Full Disk Encryption status now provides more details
- IMPROVED: Extended Hardware inventory details for the device with encryption-related fields
- IMPROVED: Disabled computers are not synced or deleted by the Active Directory scanner
- IMPROVED: Various UI and UX improvements
- CHANGED: Retention policy enforcement notification
- CHANGED: The CRON trigger can be planned for LOCAL or UTC time only
- CHANGED: The Wipe task has been dropped because it does not work properly in newer versions of Android. The Factory Reset task remains the only task for both Apple and Android devices
- CHANGED: Adjustments related to managed products name changes
- FIXED: Mobile device management allows manual selection of a suitable platform in case of unrecognized mobile devices
- FIXED: The License Owner name is not updated in License Management after changing it in ESET Business Account
- FIXED: A Client task cannot be scheduled for managed computer local time (only for browser time)
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 2.2

Release date: April, 2021

- NEW: New concept–Option to preview certain features
- NEW: Preview feature–Support for iOS / iPadOS (without ABM enrollment)

- NEW: Preview feature–Computer preview
- ADDED: Upgrade outdated products in a computer group
- ADDED: Default filter in the Detection screen (unresolved detections first)
- ADDED: Ability to use a second license to activate ESET Dynamic Threat Defense in a software installation task when an eligible endpoint product is selected
- ADDED: User management for users with global "write" access
- ADDED: Expiration time for client task triggers (Triggers tab)
- ADDED: New report–Computer Hardware Overview
- ADDED: Enabled non-root administration (other than the instance creator) to manage the security of other managed accounts (depends on the upcoming EBA release planned for April 2020)
- IMPROVED: Pause a task for ESET Full Disk Encryption (capability to select an exact date and time)
- IMPROVED: The encryption status tile is now more interactive
- IMPROVED: Extended information in detection details
- IMPROVED: A recommendation message is displayed when the Administrator tries to run a client task on more than 1,000 clients (using a group is recommended)
- IMPROVED: Assigning a policy to more than 200 individual devices is permitted (using a group is recommended)
- IMPROVED: Various performance improvements
- FIXED: Licenses with over 10,000 seats were displayed as infinite
- FIXED: In some cases, the "Planned" flag In a client task remained active after a task was executed
- FIXED: The license usage number did not display the correct number when a license was overused
- FIXED: Subunits were not used by percentage usage enumeration for mail security products
- FIXED: The operating system name (Big Sur) for macOS 11.1 and 11.2 was missing
- FIXED: Various other bug fixes and improvements

ESET PROTECT Cloud 2.1

Release date: February, 2021

- ADDED: Ability to look up specific computer based on the last logged user parameter
- ADDED: Support for policy-based migration from on-premises console to cloud console
- FIXED: Issue with opening/reading PDF reports sent by email (base64-encoded)

- FIXED: Non-root user with write permission rights for ESET PROTECT Cloud in ESET Business Account cannot import or create dynamic group templates
- FIXED: Device filters on Dashboards display different values than in tables
- FIXED: In some cases, Detail in the "Audit Log" overlapping other lines
- FIXED: Product deactivation fails with timeout (in certain cases) if started by "Delete not connected computers" server task
- FIXED: User cannot delete objects in some cases even with correct access rights
- FIXED: Name of the file is garbled when Japanese characters are used
- FIXED: Various other bug fixes and minor improvements

ESET PROTECT Cloud 2.0.148.0

Release date: December, 2020

- CHANGED: ESET Cloud Administrator renamed to ESET PROTECT Cloud
- ADDED: Ability to manage and protect Android mobile devices
- ADDED: Ability to manage FileVault (macOS) native encryption when an eligible license is present
- ADDED: Increased device management limit (up to 10,000 - dependent on purchased license size)
- ADDED: One-click deployment of ESET Dynamic Threat Defense if an eligible license is present
- ADDED: Ability to manage dynamic groups
- ADDED: Ability to manage notifications
- ADDED: Ability to define specific permission sets for selected users
- ADDED: Active Directory synchronization (Computers only)
- ADDED: Syslog log exporting
- ADDED: New “Audit log” section provides detailed information about specific actions
- ADDED: Ability to mass deploy the management agent to macOS devices
- ADDED: Second-level menu for advanced options
- ADDED: Secure Browser management
- ADDED: Support for sites (ESET Business Account) licenses including new "License user" column
- ADDED: Renew a license in the “License Management” screen
- ADDED: Ability to drill-down from expiring license issues in “Dashboards” and “Reports” to obtain more information in the “License Management” screen

- ADDED: New “Manage license” context menu
- ADDED: EULA update notifications that support auto-upgrade (uPCU) of endpoint products in managed environments
- ADDED: New ESET Full Disk Encryption (EFDE) management actions directly from “Computer details”
- ADDED: New EFDE Dynamic groups and Reports
- ADDED: Detection details (LiveGrid, Observed in organization, Virus Total)
- ADDED: One-click access to client task triggers
- ADDED: Unsupported browser warning
- ADDED: New "Seats allocated to sites" present in dedicated license report
- ADDED: Multi-line command scripts for Run Command task
- ADDED: Option to create a Computer user group in the “Add computer user” wizard
- CHANGED: Management Agent - supported operating systems
- CHANGED: Retention policy defaults
- CHANGED: License unit/sub-units visualization changed to "used/total" for online licenses and "X offline" for offline licenses
- CHANGED: Access to behavior reports (when EDTD is purchased and enabled) are available (in the UI) only if an eligible license is present
- IMPROVED: Ability to define a retention policy for certain logs
- IMPROVED: Exclusions mechanism extended to firewall threats
- IMPROVED: Computer details now directly accessible by clicking the computer name
- IMPROVED: One-click Network isolation
- IMPROVED: Columns ordering
- IMPROVED: Pop-up with search option
- IMPROVED: Hierarchical Dynamic groups tree
- IMPROVED: Multi-select in pop-up (modal) windows
- IMPROVED: Ability to create one exclusion from multiple detentions with standard exclusion criteria(s)
- IMPROVED: Breadcrumbs for better navigation in Wizards
- IMPROVED: Various other performance and security improvements
- FIXED: “Delete task action” removes all client tasks, not just selected items in a task list for a specific group

- FIXED: Status filter not visible for server tasks (only in client tasks)
- FIXED: Failed to send a wake-up call from the client task details executions
- FIXED: Incorrect target group type displays when editing a client trigger
- FIXED: “Status update” type notifications fail to save if they contain the “$” character
- FIXED: Import of policies with large file sizes
- FIXED: Infinite units or subunits in tooltips for licenses in the License Management screen display incorrectly
- FIXED: License-related notifications (for example, expiration/overuse) trigger when a license is suspended
- FIXED: Policy does not block the selected Scan profile
- FIXED: Filters previously set are not saved
- FIXED: Various other bug fixes

ESET Cloud Administrator 1.2.118.0

- Added: Support for ESET Dynamic Thread Defense (Sold separately. Available for purchase in upcoming weeks)
- Added: Submitted files screen
- ADDED: Ability to pause ESET Full Disk Encryption available from EFDE client version 1.2 (EFDE - purchased separately)
- ADDED: Automatic resolution of firewall logs and filtered websites
- ADDED: Ukrainian language
- ADDED: New filtering options
- ADDED: Many other performance, usability, and security improvements
- IMPROVED: Discontinued the default limit for the number of displayed static groups
- IMPROVED: Performance improvements in the “groups” tree on the “Computers” and “Detections” screens
- IMPROVED: Selected screens redesign: Users, scheduled reports and edit updates in the navigation bar
- IMPROVED: Unified table design for task selection, computers selection, and other features
- IMPROVED: Second-level menu added under "Change assignments" in the policy screen
- FIXED: Delay of product version status shown in the main web console
- FIXED: System applications are not reported on macOS 10.15
- FIXED: Language detection on macOS Catalina

- FIXED: Table sorting behavior: Clicking column headers adds columns to multi-sorting until it has been clicked 3 times
- FIXED: Last scan time in “computer details” screen won’t impact the computer security status tile
- FIXED: User cannot resolve detections when the “Resolved” column is not shown in the “detections” table
- FIXED: The side panel does not remember the expanded/collapsed state after log-out and log-in
- FIXED: Some threats cannot be marked as resolved
- FIXED: After moving computers from a specific group, the view is changed to the group "ALL."

ESET Cloud Administrator - ESET Management Agent release- June

- ADDED: New version of ESET Management Agent
- ADDED: Updating ESET Management Agent to the latest version can be deployed centrally alongside the cloud service update
- ADDED: Agent compatibility with H1/2021 Windows version 10

ESET Cloud Administrator 1.2.82.0

- IMPROVED: Email domain validation when sending live installer link was discontinued
- IMPROVED: Checkbox "automatically reboot when needed" not checked by default when activating EFDE from encryption tile
- IMPROVED: Dozens of usability, security, performance and stability improvements
- FIXED: Clicking column headers adds columns to multi-sorting until it has been clicked 3 times
- FIXED: Last Scan Time should note trigger red security status
- FIXED: Not possible to resolve detections when "Resolution" column is not shown
- FIXED: The side panel doesn't remember expanded/collapsed state after log-out and log-in
- FIXED: Agents stop connecting to cloud service under some circumstances
- FIXED: Recipients not visible in notifications emails
- FIXED: Computer with outdated OS are not visible in appropriate dynamic group
- FIXED: Ability to create hash exclusion without a hash present
- FIXED: ESET Full Disk Encryption not included within the selective export task configuration

ESET Cloud Administrator 1.2

- NEW: ESET Full Disk Encryption

- NEW: Tagging - mark all relevant objects (e.g., computers) using user-defined tags
- NEW: Support for the newest generation of Linux products, starting with ESET File Security for Linux v7
- NEW: Centralized Exclusions and wizard
- ADDED: Option to automatically delete computers that are not connecting
- ADDED: Option to rename computers based on defined criteria
- ADDED: Computer isolation task
- ADDED: Unified table design with new navigation elements
- ADDED: Ability to export tables across all the main screens to different formats
- ADDED: New "empty screen states" for simpler object creation
- ADDED: Detections view is now aggregated by time and other criteria to simplify operations and to resolve them
- ADDED: Execute one click actions from the "task executions" screen
- ADDED: Create a combined installer including ESET Full Disk Encryption
- ADDED: Option to deactivate individual products
- ADDED: New dynamic groups related to newly introduced products
- ADDED: Search by group name in computer screens and search bar
- ADDED: Option to save dashboard layout as preset for other users
- ADDED: Generate defined reports filtered to a selected group
- ADDED: Indonesian language support
- ADDED: New ESET Management Agent version (Windows) supports the latest security products
- IMPROVED: Many UI Improvements & other usability changes
- IMPROVED: Context menu now applies for all selected rows
- IMPROVED: Filtering panel has many new options such as autocomplete
- IMPROVED: New column selector element for primary tables
- IMPROVED: Layout of detections (previously "threats") screen with new detection details
- IMPROVED: Reports screen layout includes a one click report generation option
- IMPROVED: Task section was updated and triggers are now displayed in a separate view of "task details"
- IMPROVED: Layout of policies screen, with simpler orientation and navigation

- IMPROVED: Layout of notifications screen with notification details
- IMPROVED: Quick links menu
- IMPROVED: AV remover (part of management agent) supports auto update
- IMPROVED: Download speeds from the repositories were significantly improved
- IMPROVED: Management agent file size significantly reduced
- CHANGED: "Threats" section was renamed to "Detections"
- CHANGED: Management agent compatibility update related to macOS 10.7 and 10.8 support (see the documentation for more details)
- CHANGED: ESET Cloud Administrator ends support for Endpoint and Server Security versions 6.4 and earlier
- FIXED: Various other bug fixes and internal performance improvements

ESET Cloud Administrator 1.1.360.0

- Added: Full support for endpoint version 7.1 products
- Fixed: Various bugs

ESET Cloud Administrator 1.1.359.0

- Improved: Internal performance improvements

ESET Cloud Administrator 1.1.358.0

- Improved: Overall performance improvements
- Changed: Updated copyright information
- Fixed: ESET Cloud Administrator (ECA) server does not receive all "Web protection" threats
- Fixed: "Web protection" threat details view in the webconsole displays an unexpected error
- Fixed: An uncaught exception occurs when working with ECA
- Fixed: Indonesian language support is missing in product installation filters
- Fixed: Server Device Status chart is missing

ESET Cloud Administrator 1.1.356.0

- FIXED: Issue with too many notifications send from one incident

ESET Cloud Administrator 1.1.350.0

- New version of ESET Management Agent fixing various installation/upgrade/repair issues
- Internal service performance improvements
- Fixed invalid installer CA certificate encoding in GPO installer script

ESET Cloud Administrator 1.1.349

- Various minor performance improvements

ESET Cloud Administrator 1.1.345

- Various minor bug fixes
- Wrong information is displayed under "Policy Product" column while creating the ECA Live installer

ESET Cloud Administrator 1.1.343.0

- One-click actions
- New one-click action - One click upgrade option – even from aggregated data
- New One-click actions to resolve "resolvable" actions – activate, reboot, update OS, or various protection issues
- Hardware inventory
- Redesigned client details section
- New "incident overview" dashboard, with new types of graphical elements, and one-click navigation to threats
- Improved Automatic resolving of handled threats
- Option to generate live installer without security product selected
- New status overview section
- Live installer now support offline cache to speed up the deployment
- Overall UI improvements (polished UI, new vector icons, updated menus)
- Updated "overview" dashboard with one click navigation & Configurable RSS feed
- Redesigned quick links & help links
- New layout for wizard elements
- Ability to switch ECA do different language in EBA (support for NEW languages)

- Automatic detection of "machine cloning"
- Ability to send e-mail directly from ECA when sending installer
- Automatic log-outs
- New more streamlined way when adding computers or using introductory wizard
- Redesigned "filter bar" with the option to remove / reset / save filter presets + "category filter" moved to "filters"
- New columns for number / highest severity of alerts, cloning questions, and hardware detection reliability status
- Enhanced filtering options by product name, version, number of alerts, policies, threats, & other options
- New "remove computer from management" wizard, showing clear steps how to correctly remove devices from ECA
- Redesigned task wizard
- New task types - Diagnostic (enable diagnostic / Log Collector)
- Section "logs" now includes tabs to display "Log Collector" and new section for "diagnostic logs"
- Alerts - Alert (problem) details are reported from the supported security products
- New dynamic groups for desktops and servers
- Questions to resolve conflicts
- Possible to locate threats detected by the same scan
- Added current detection engine version and a hash value
- Possibility to filter by cause, threat type, scan, scanner and define more granular criteria for the time filter in threats
- Possibility to collapse and expand all reports in one click
- Software installation task executes a "pre-execution check", and reports "task failed" with further details
- New report template categories Hardware Inventory, Cloning Detection
- Restyled report creation wizard
- Extended options for filtering for specific values
- Redesigned installer generation flow
- Ability to configure LiveGrid and PUA settings when creating live installer
- Ability to configure Live Installer proxy settings during the installer creation

- Support for GPO (Group policy)
- New filter to "hide not-assigned policies"
- Policy details showing "assigned to" (combines computers / groups) and "applied on" (actually applied targets)
- New predefined policies for optimal usage of ESET Live Grid, and few tweaks to existing recommended templates for maximum protection
- Possibility to allow "local lists"
- Possible to edit multiple notifications at once
- New announcement channel to inform users about planned outages and other important events
- Improved migration from ERA6 (ESMC) managed environment when executing live installers

Navegadores web, productos de seguridad de ESET e idiomas compatibles

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

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.

Producto	Versión del producto
ESET Endpoint Security para Windows	Superiores a 7.3
ESET Endpoint Antivirus para Windows	Superiores a 7.3
ESET Endpoint Security para macOS	Superiores a 6.10
ESET Endpoint Antivirus para macOS	Superiores a 6.10
ESET File Security para Windows Server	Superiores a 7.3
ESET Server Security para Microsoft Windows Server	Superiores a 7.3

Producto	Versión del producto
ESET Mail Security para Microsoft Exchange Server	Superiores a 7.3
ESET Security para Microsoft SharePoint Server	Superiores a 7.3
ESET Mail Security para IBM Domino Server	Superiores a 7.3
ESET File Security en Linux	Superiores a 7.2
ESET Server 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 Endpoint Security para Android	3.3+
ESET Inspect Connector	1.8+
ESET Full Disk Encryption para Windows	
ESET Full Disk Encryption para macOS	
ESET LiveGuard Advanced	

Idiomas compatibles

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

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

Sistemas operativos compatibles

En las siguientes tablas se muestran los sistemas operativos compatibles con cada componente de ESET PROTECT:

Versiones y soporte de ESET Management Agent

El agente ESET Management sigue el número de versión ESET PROTECT On-Prem y la directiva de fin de ciclo de vida:

- Las versiones compatibles de ESET Management Agent son 9.x–11.x.
- Cada versión de ESET Management Agent recibe seis meses de soporte completo y dos años de soporte limitado. Posteriormente, la versión pasa al fin de la vida útil.

La versión de ESET Management Agent compatible más reciente es 11.x. 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.

Windows

Sistema operativo	Agente	RD Sensor
Windows Server 2012 x64	9.x—10.x, 11.x	✔
Windows Server 2012 CORE x64	9.x—10.x, 11.x	✔
Windows Server 2012 R2 x64	9.x—10.x, 11.x	✔
Windows Server 2012 R2 CORE x64	9.x—10.x, 11.x	✔
Windows Storage Server 2012 R2 x64	9.x—10.x, 11.x	✔
Windows Server 2016 x64	9.x—10.x, 11.x	✔
Windows Storage Server 2016 x64	9.x—10.x, 11.x	✔
Windows Server 2019 x64	9.x—10.x, 11.x	✔
Windows Server 2022 x64	9.x—10.x, 11.x	✔
Windows Server 2022 CORE x64	11.x	

Sistema operativo	Agente	RD Sensor
Windows 10 x86	9.x—10.x, 11.x	✔
Windows 10 x64 (todas las versiones oficiales)	9.x—10.x, 11.x	✔
Windows 10 en ARM	9.x—10.x, 11.x	
Windows 11 x64	9.x (21H2) 10.x, 11.x (21H2,22H2) 10.1, 11.x (23H2)	✔
Windows 11 en ARM	10.x, 11.x	

ESET Management Agent 10.x es la última versión compatible con Windows 7/8.x y Windows Server 2008 R2/Microsoft SBS 2011.

Linux

Sistema operativo	Agente	RD Sensor
Ubuntu 18.04.1 LTS x64 Desktop	9.x—10.x, 11.x	✔
Ubuntu 18.04.1 LTS x64 Server	9.x—10.x, 11.x	✔
Ubuntu 20.04 LTS x64	9.x—10.x, 11.x	✔
Ubuntu 22.04 LTS x64	10.x, 11.x	✔
Linux Mint 20	10.x, 11.x	✔
Linux Mint 21	10.1, 11.x	✔
RHEL Server 7 x64	9.x—10.x, 11.x	✔
RHEL Server 8 x64	9.x—10.x, 11.x	
RHEL Server 9 x64	9.x—10.x, 11.x	✔
CentOS 7 x64	9.x—10.x, 11.x	✔
SLED 15 x64	9.x—10.x, 11.x	✔
SLES 12 x64	9.x—10.x, 11.x	✔
SLES 15 x64	9.x—10.x, 11.x	✔
Debian 9 x64	9.x—10.x, 11.x	✔
Debian 10 x64	9.x—10.x, 11.x	✔
Debian 11 x64	9.x—10.x, 11.x	✔
Debian 12 x64	10.1, 11.x	✔
Oracle Linux 8	9.x—10.x, 11.x	✔
Amazon Linux 2	9.x—10.x, 11.x	✔
Alma Linux 9	10.1, 11.x	✔
Rocky Linux 8	10.1, 11.x	
Rocky Linux 9	10.1, 11.x	

ESET Management Agent se ha probado y se ejecuta en las versiones secundarias más recientes de las distribuciones de Linux indicadas.

Mac

Sistema operativo	Agente
macOS Catalina (10.15)	9.x—10.x, 11.x
macOS Big Sur (11.0)	9.x—10.x, 11.x
macOS Monterey (12.0)	9.x—10.x, 11.x
macOS Ventura (13.0)	9.x—10.x, 11.x
macOS Sonoma (14.0)	10.1, 11.x

Móvil

Sistema operativo	EESA	Inscripción de entrada limitada en EESA	Propietario del dispositivo EESA	MDM iOS	MDM iOS ABM
Android 6.x+	✔	✔			
Android 7.x+	✔	✔	✔		
Android 8.x+	✔	✔	✔		
Android 9.0	✔	✔	✔		
Android 10.0	✔	✔	✔		
Android 11	✔	✔	✔		
Android 12	✔	✔	✔		
Android 13	✔	✔	✔		
Android 14	✔	✔	✔		
iOS 9.x+				✔	*
iOS 10.x+				✔	*
iOS 11.x+				✔	*
iOS 12.0.x				✔	*
iOS 13.x+				✔	✔
iOS 14.x+				✔	✔
iOS 15				✔	✔
iOS 16				✔	✔
iOS 17				✔	✔
iPadOS 13				✔	✔
iPadOS 14				✔	✔
iPadOS 15				✔	✔
iPadOS 16				✔	✔
iPadOS 17				✔	✔

* iOS ABM solo está disponible en algunos países.

Requisitos previos de la red

Permita los siguientes requisitos previos de la red en su cortafuegos para que ESET PROTECT funcione correctamente.

Dominios y puertos

Dominio	Protocolo	Puerto	Servicio/componente	Descripción
eba.eset.com	TCP	443	ESET Business Account	
msp.eset.com	TCP	443	ESET MSP Administrator	
identity.eset.com	TCP	443	Servidor de identidad de ESET	

Dominio	Protocolo	Puerto	Servicio/componente	Descripción
protect.eset.com	TCP	443	ESET PROTECT	
eu02.protect.eset.com	TCP	443	ESET PROTECT Web Console	Ubicación: Europa
us02.protect.eset.com	TCP	443		Ubicación: EE. UU.
jp02.protect.eset.com	TCP	443		Ubicación: Japón
*.a.ecaserver.eset.com	TCP	443	Conexión entre el agente y ESET PROTECT	
edf.eset.com	TCP	443	Live Installer	
redirector.eset.systems	TCP	443		
repository.eset.com	TCP	80		Repositorio necesario para la implementación
epns.eset.com	TCP	8883	Conexión del servicio EPNS (llamadas de activación)	
eu.mdm.eset.com (EUROPA) us.mdm.eset.com (EE. UU.) jp.mdm.eset.com (JAPÓN)	TCP	443	Cloud MDM	Inscripción
checkin.eu.eset.com (EUROPA) checkin.us.eset.com (EE. UU.) checkin.jp.eset.com (JAPÓN)	TCP	443		Registrar
mdmcomm.eu.eset.com (EUROPA) mdmcomm.us.eset.com (EE. UU.) mdmcomm.jp.eset.com (JAPÓN)	TCP	443		Comunicación
mdm.eset.com (GLOBAL)	TCP	443		Inscripción de dispositivo de entrada limitada
	TCP	139	ESET PROTECT Remote Deployment Tool (Puerto de destino desde el punto de vista de Remote Deployment Tool)	Uso de ADMIN$ compartido
	TCP	445		Acceso directo a recursos compartidos utilizando TCP/IP durante la instalación remota (una alternativa a TCP 139)
	UDP	137		Resolución del nombre durante la instalación
	UDP	138		Explorar durante la instalación remota

Direcciones IP

Dirección IP	Servicio	Descripción
20.82.100.209	Conexión entre el agente ESET Management y ESET PROTECT	Ubicación: Europa
20.245.38.118		Ubicación: EE. UU.
20.194.197.189		Ubicación: Japón
13.69.61.76	Conexión con ESET PROTECT Web Console	Ubicación: Europa
23.99.91.144		Ubicación: EE. UU.
20.46.163.70		Ubicación: Japón

Encontrará los requisitos previos de red para **ESET Connect** en la Ayuda en línea de ESET Connect.

Disponibilidad del servicio

Disponibilidad

Nuestro objetivo es ofrecer un 99,5 % de disponibilidad del servicio. Nuestro esfuerzo y nuestros procesos bien definidos nos permiten lograrlo. En caso de interrupción del servicio ESET PROTECT, los equipos siguen siendo seguros y no se ven afectados.

El Portal de estado de ESET muestra el estado actual de los servicios en la nube de ESET, las interrupciones programadas y los incidentes pasados. Si tiene un problema con un servicio ESET compatible y no lo ve listado en el Portal de estado, comuníquese con el soporte técnico de ESET.

Los equipos de supervisión verifican los posibles problemas internamente, y los incidentes confirmados se publican y actualizan manualmente para mantener una alta credibilidad y precisión. Por lo tanto, aparecen en el Portal de estado con un ligero retraso. Es posible que un incidente de corta duración no se publique si se resuelve antes de confirmarse manualmente.

Mantenimiento

El servicio ESET PROTECT está sujeto a procedimientos de mantenimiento rutinario. Todas las ventanas de mantenimiento que superen los 15 minutos se anuncian a los administradores de la consola de antemano. Las interrupciones durante las ventanas de mantenimiento no afectan a nuestro objetivo de disponibilidad. El mantenimiento se realizará durante fines de semana y fuera del horario laboral (centro de datos de EE. UU.: durante las horas de la noche de EE. UU.; centro de datos de la UE: durante las horas de la noche en la UE; centro de datos de Japón: durante las horas de la noche en Japón).

Diferencias entre la consola de administración local y la de la nube

ESET PROTECT incluye todas las funciones y capacidades clave que conoce de ESET PROTECT On-Prem, pero se adaptó a las necesidades de una gestión basada en la nube. Puede migrar de ESET PROTECT on-prem a ESET PROTECT.

La siguiente tabla incluye descripciones de las principales diferencias entre ESET PROTECT y ESET PROTECTOn-Prem.

Diferencia general	ESET PROTECT	ESET PROTECT On-Prem
Alojamiento	Se ejecuta en el entorno en la nube mantenido por ESET.	Se ejecuta en su entorno físico o virtualizado.
Número máximo de dispositivos que se pueden administrar	50.000 dispositivos cliente.	La limitación depende de las limitaciones del hardware del servidor.
Versiones del producto compatibles	• Productos empresariales versión 6 y posteriores.	• Productos empresariales versión 4 y posteriores.
Componentes	• ESET Management Agent • RD Sensor • Herramienta de implementación • CloudMDM	• ESET Management Agent • RD Sensor • Herramienta de implementación • MDM
Active Directory	La sincronización de Active Directory está disponible con el uso de ESET Active Directory Scanner.	La sincronización de Active Directory está disponible.
Administración de dispositivos móviles	• La administración de dispositivos móviles está disponible de forma predeterminada a través de CloudMDM. • La inscripción de entrada limitada para dispositivos Android está disponible como opción de inscripción.	• La administración de dispositivos móviles está disponible mediante ESET PROTECT On-PremMDM. ⚠ 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.
Certificados	ESET gestiona la administración de certificados.	El usuario puede crear, editar o importar/exportar certificados y autoridades certificadoras

Diferencia general	ESET PROTECT	ESET PROTECT On-Prem
Derechos de acceso	La administración de derechos de acceso se ha movido a ESET Business Account, pero puede especificar el acceso a características específicas de ESET PROTECT para un usuario que tenga permisos personalizados.	Modelo avanzado de seguridad de derechos de acceso multiempresa que se administra desde la interfaz ESET PROTECT On-Prem
Administración de licencias	La administración de licencias se ha movido totalmente a ESET Business Account.	La administración de licencias se encuentra de forma parcial tanto en ESET PROTECT On-Prem como en ESET Business Account.
Cómo agregar ordenadores	Los ordenadores se pueden agregar mediante la sincronización de Sincronizar con Active Directory, desde un informe de RD Sensor y con scripts de instalador de SCCM y GPO.	Los ordenadores pueden agregarse a través de la sincronización con Active Directory, desde un informe de RD Sensor, con los scripts de GPO y SCCM Installer, manualmente agregando un nuevo dispositivo con la adición de una tarea de implementación de agente o instalando el agente de forma local.
Capas de protección adicionales	• ESET Administración de revisiones y vulnerabilidades • ESET LiveGuard • ESET Full Disk Encryption • ESET Inspect ESET PROTECT no es compatible con ESET Inspect On-Prem, pero sí con ESET Inspect. Si migra de ESET PROTECT On-Prem a ESET PROTECT, no podrá administrar ESET Inspect On-Prem desde ESET PROTECT, pero podrá administrar ESET Inspect desde ESET PROTECT.	• ESET LiveGuard • ESET Full Disk Encryption • ESET Inspect On-Prem

Introducción a ESET PROTECT

ESET PROTECT es la solución de fábrica que le permite administrar los productos de seguridad de ESET en la red de su pequeña o mediana empresa. Representa un nuevo enfoque que amplía la anterior solución in situ de ESET e introduce un nuevo servicio en la nube más flexible, alojado y mantenido por ESET.

Esta solución puede utilizarse de inmediato y omite los pasos de instalación y configuración requeridos por las soluciones in situ. ESET PROTECT se ha diseñado para que sea fácil de implementar y utilizar. Este nuevo servicio alojado en la nube incluye una consola de administración web actual (ESET PROTECT Web Console), a la que podrá conectarse desde prácticamente cualquier ubicación o dispositivo con una conexión a Internet adecuada.

En las siguientes secciones se explican las funciones de ESET PROTECT Web Console y su uso. Puede crear instaladores e implementar ESET Management Agent y productos de seguridad de ESET en ordenadores cliente. Tras la implementación de ESET Management Agent, podrá administrar grupos, crear y asignar políticas y configurar notificaciones e informes.

Introducción a ESET PROTECT

Utilizo ESET Business Account

1.Cree una nueva instancia de ESET PROTECT.

2.Configure usuarios de ESET PROTECT en ESET Business Account.

3.Abra ESET PROTECT Web Console. Consulte también el ESET PROTECTrecorrido por *** y la descripción general de ESET PROTECT Web Console.

4.Asigne usuarios de ESET Business Account en ESET PROTECT Web Console.

5.Agregue ordenadores cliente de su red a la estructura de ESET PROTECT.

6.Administre productos Endpoint desde ESET PROTECT.

Utilizo ESET MSP Administrator

1.Cree una nueva instancia de ESET PROTECT.

2.Configure usuarios de ESET PROTECT en ESET MSP Administrator.

3.Abra ESET PROTECT Web Console. Consulte también el ESET PROTECTrecorrido por *** y la descripción general de ESET PROTECT Web Console.

4.Agregue usuarios de ESET MSP Administrator a ESET PROTECT Web Console durante la configuración de clientes MSP.

5.Agregue ordenadores cliente de su red a la estructura de ESET PROTECT.

6.Administre productos Endpoint desde ESET PROTECT.

Crear una nueva instancia de ESET PROTECT con ESET Business Account

Requisitos previos

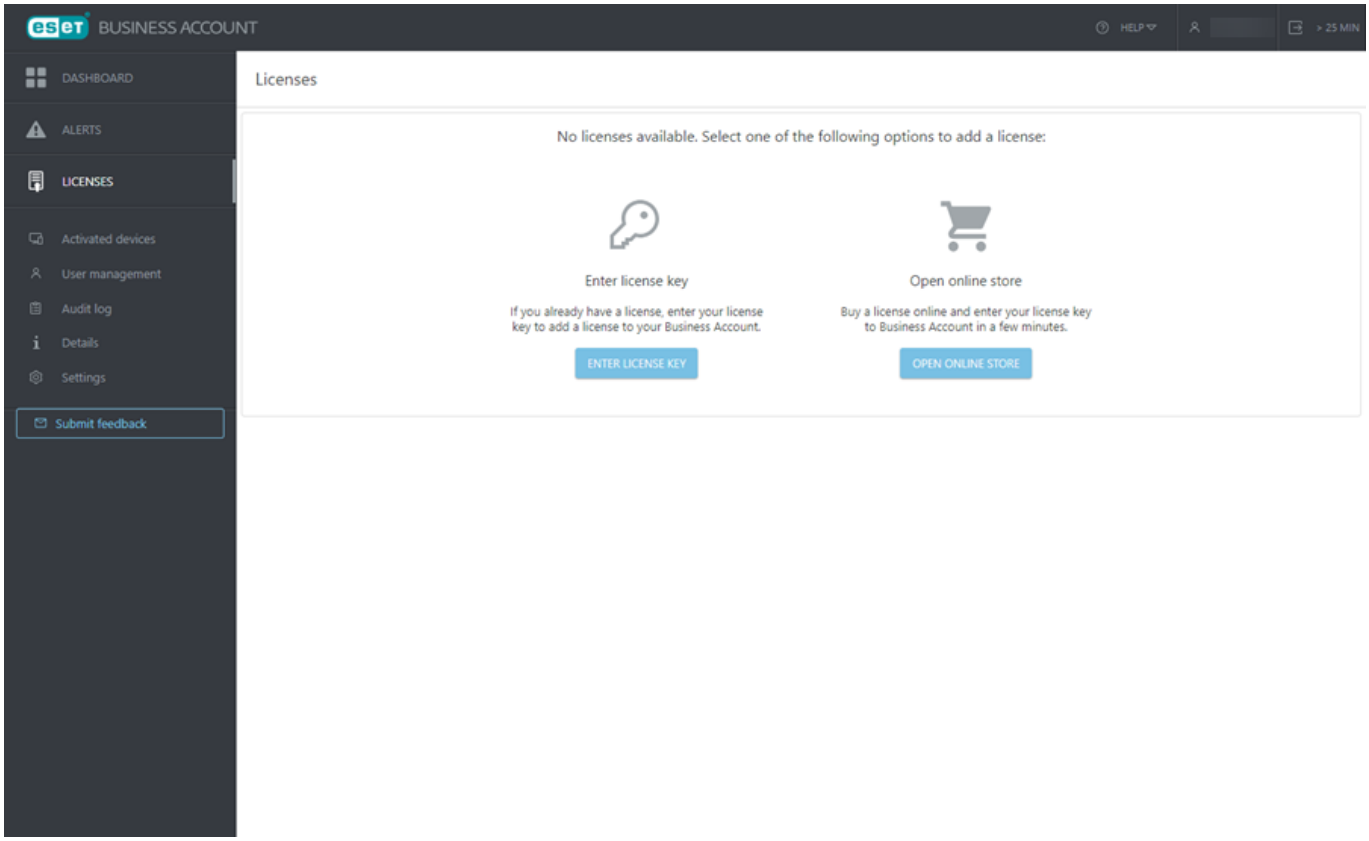
- Una cuenta de superusuario en ESET Business Account.
- Una licencia válida para ESET PROTECT.

Si sus cuentas de EBA y EMA2 se registran con la misma dirección de correo electrónico, ESET PROTECT solo se puede activar desde una cuenta. La cuenta (EBA o EMA2) a partir de la que elige crear la instancia de ESET PROTECT será la única que puede utilizar para activar o eliminar la instancia.

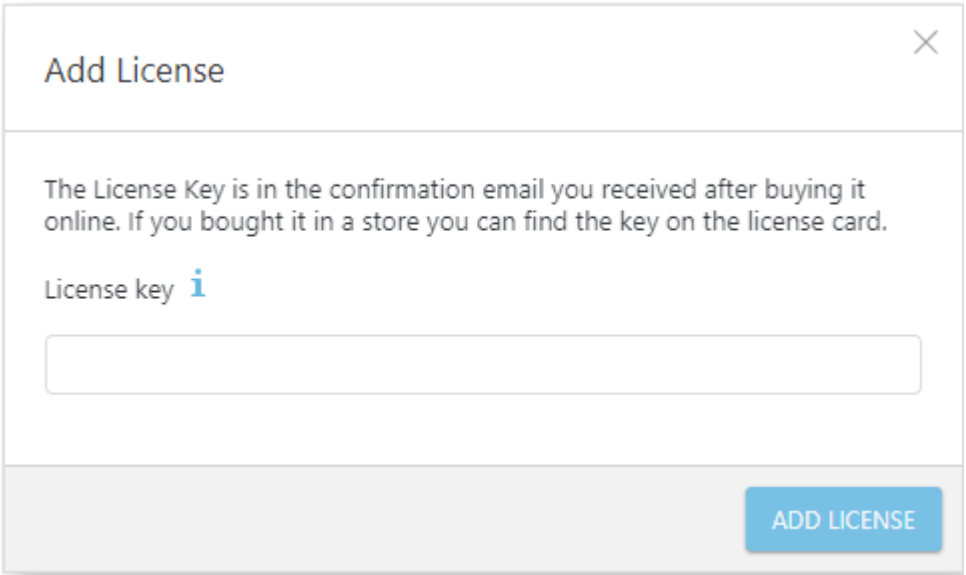
Crear una nueva instancia de ESET PROTECT

1. Abra ESET Business Account e inicie sesión (o cree una nueva cuenta).

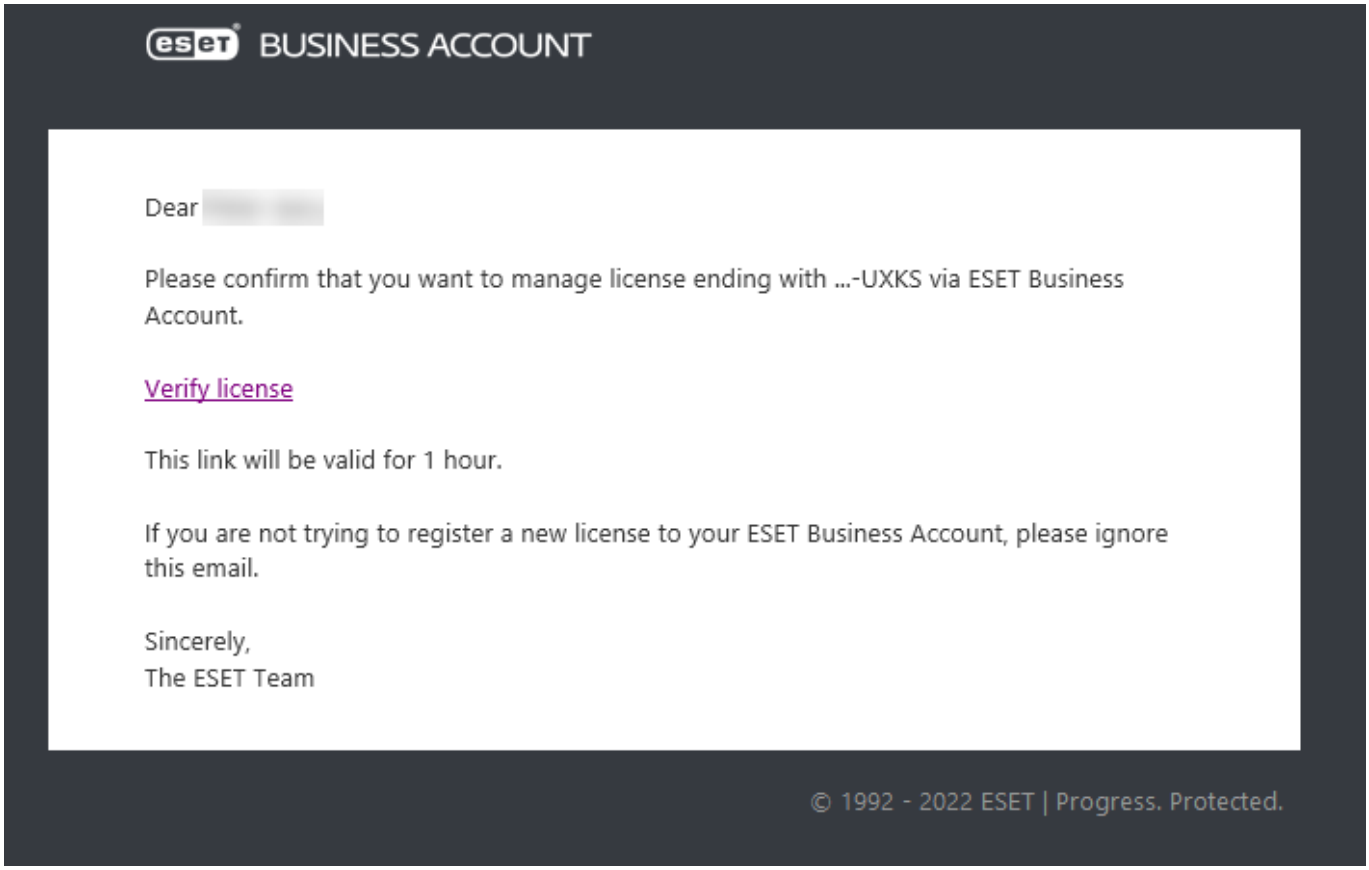
2. Haga clic en **Licencias** > **Introducir clave de licencia**.



3. En la ventana **Agregar licencia**, introduzca su **clave de licencia** de ESET PROTECT y haga clic en **Agregar licencia**.



4. Recibirá un mensaje de correo electrónico de verificación (si no recibe el mensaje de correo electrónico, siga las instrucciones del artículo de la base de conocimiento). Haga clic en **Verificar licencia**.



5. En el **Panel**, haga clic en **Activar** en **ESET PROTECT**.

⚠ Compruebe la configuración de idioma de ESET Business Account. Algunos elementos de las ventanas del programa principal de ESET PROTECT se definen la primera vez que configura el idioma en la configuración de idioma de ESET Business Account y no se pueden cambiar posteriormente.

6. Se abrirá la ventana **Activar ESET PROTECT**. Lea los Términos de uso y marque la casilla de verificación si los acepta.

7. Seleccione la ubicación de centro de datos de su instancia de ESET PROTECT que sea la más cerca a la ubicación de su red administrada y haga clic en **Continuar**.

⚠ Una vez seleccionada, no podrá cambiar la ubicación de centro de datos de su instancia de ESET PROTECT.

8. Se creará su instancia de ESET PROTECT. Puede esperar unos minutos hasta que se cree o puede cerrar sesión y se le notificará por correo electrónico cuando la instancia de ESET PROTECT esté disponible.

9. Haga clic en **Continuar**. También puede hacer clic en **Panel** y en **Abrir** en la ventana dinámica de ESET PROTECT para abrir una nueva pestaña de ESET PROTECT Web Console.

ESET PROTECT sincroniza su estructura de ESET Business Account con el árbol de grupos estáticos de **Ordenadores** en Web Console.

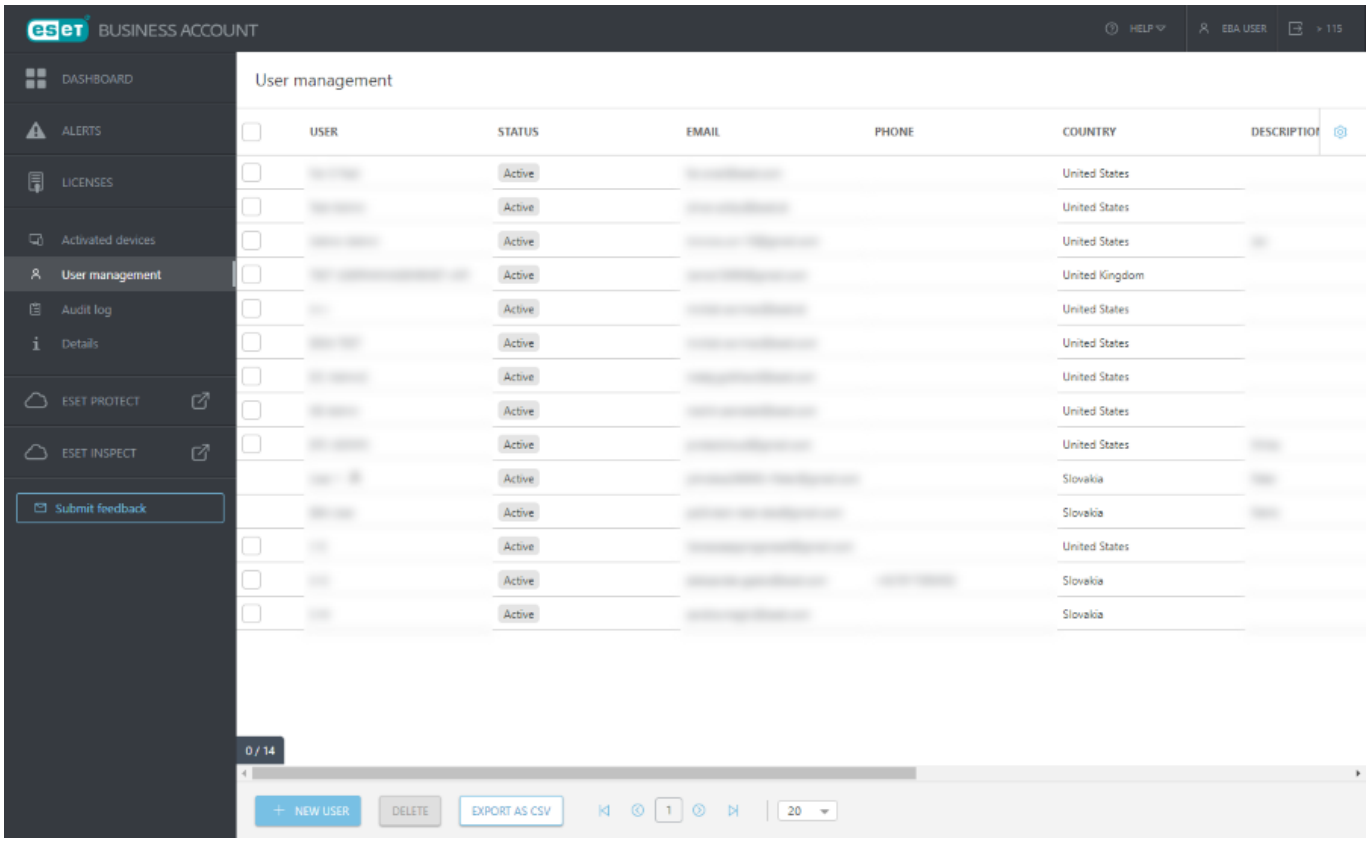
Crear un nuevoESET PROTECT usuario en ESET Business

Account

Siga estos pasos para crear un nuevo usuario de ESET PROTECT en ESET Business Account y asignar la cuenta de usuario en ESET PROTECT:

1. Inicie sesión en su cuenta de ESET Business Account.

2. Seleccione **Administración de usuarios** > **Nuevo usuario**.



3. Rellene los campos obligatorios (encontrará más información en la Ayuda en línea de ESET Business Account):

I.**General**: ofrece información básica sobre el usuario.

II.**Derechos de acceso**:

a)**Acceso a la empresa**: seleccione el nivel de acceso a la empresa del usuario: **Escritura**, **Lectura**, **Acceso solo a sitios seleccionados**.

Un usuario debe tener **Acceso a la empresa de Escritura** para ver a otros usuarios de ESET Business Account en ESET PROTECT.

b)**Acceso a la administración de usuarios**: marque esta casilla de verificación para permitir que el usuario gestione a otros usuarios de ESET Business Account.

c)**Acceso a ESET PROTECT y ESET Inspect**:

- **Escritura**: el usuario dispone de acceso total a ESET PROTECT y ESET Inspect.

- **Lectura**: el usuario solo puede ver los datos de ESET PROTECT y ESET Inspect.
- **Personalizado**: puede definir el acceso del usuario más adelante en ESET PROTECT en Conjuntos de permisos.
- **Sin acceso**: el usuario no tiene acceso a ESET PROTECT y ESET Inspect.

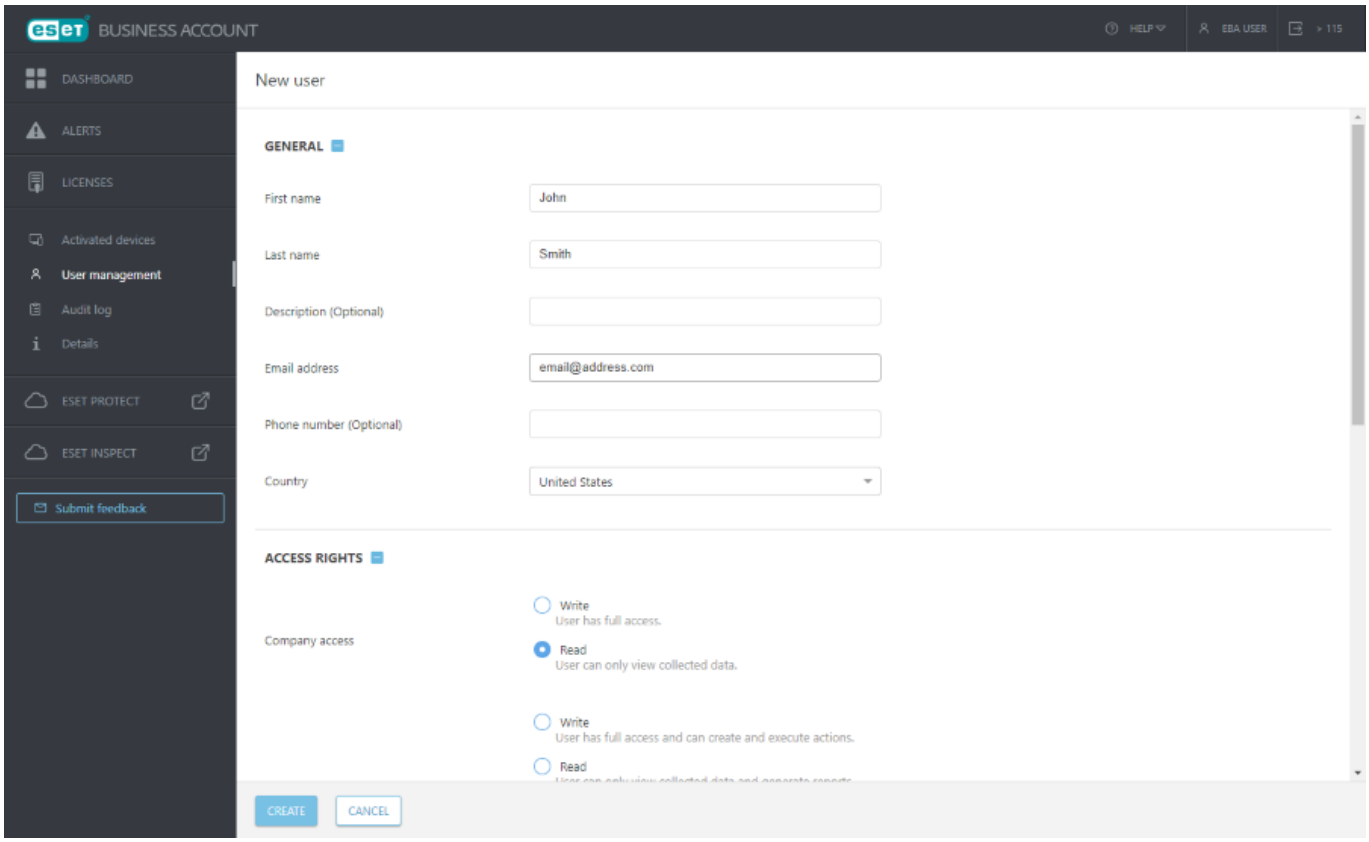
Para acceder a ESET PROTECT, un usuario debe tener derechos de acceso de **Escritura** o **Lectura** en al menos una empresa con una licencia válida (activa) de ESET PROTECT.

- Para un usuario del sitio, seleccione **Personalizado** en **Acceso a ESET PROTECT**.
- Para crear otro usuario con derechos de acceso de administrador, siga los pasos para crear un segundo administrador en ESET PROTECT.

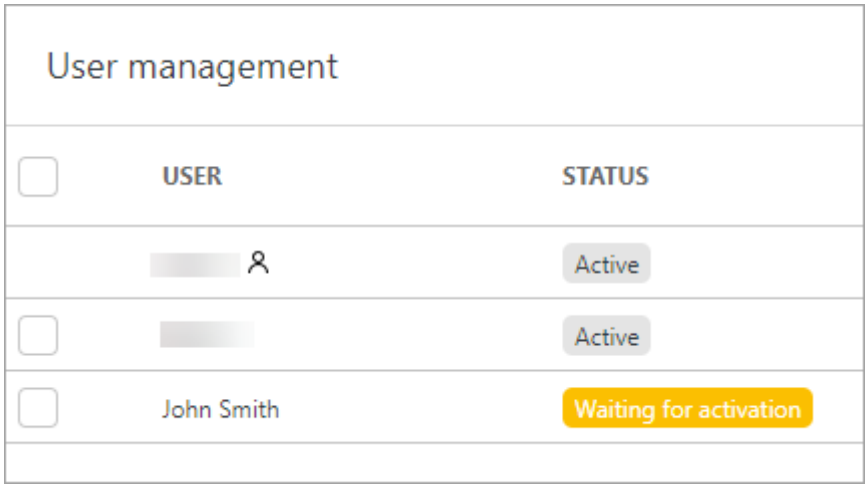
III.**Preferencias**: defina el idioma del usuario de ESET Business Account y ESET PROTECT y establezca la zona horaria.

IV.**Seguridad**: ajuste la configuración de seguridad del usuario (caducidad de la contraseña, tiempo de espera de la sesión agotado, verificación de doble factor).

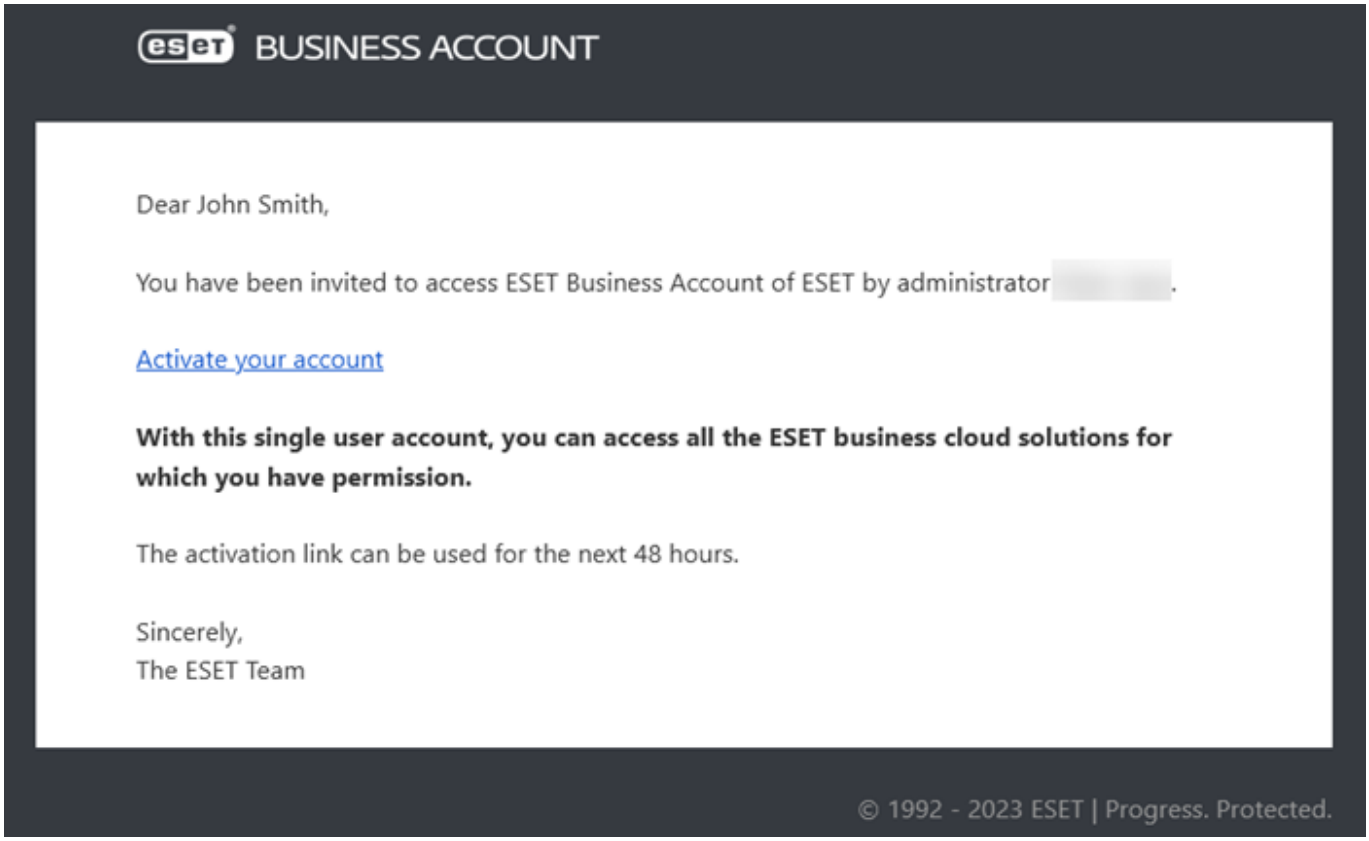
Haga clic en **Crear** para crear el usuario.



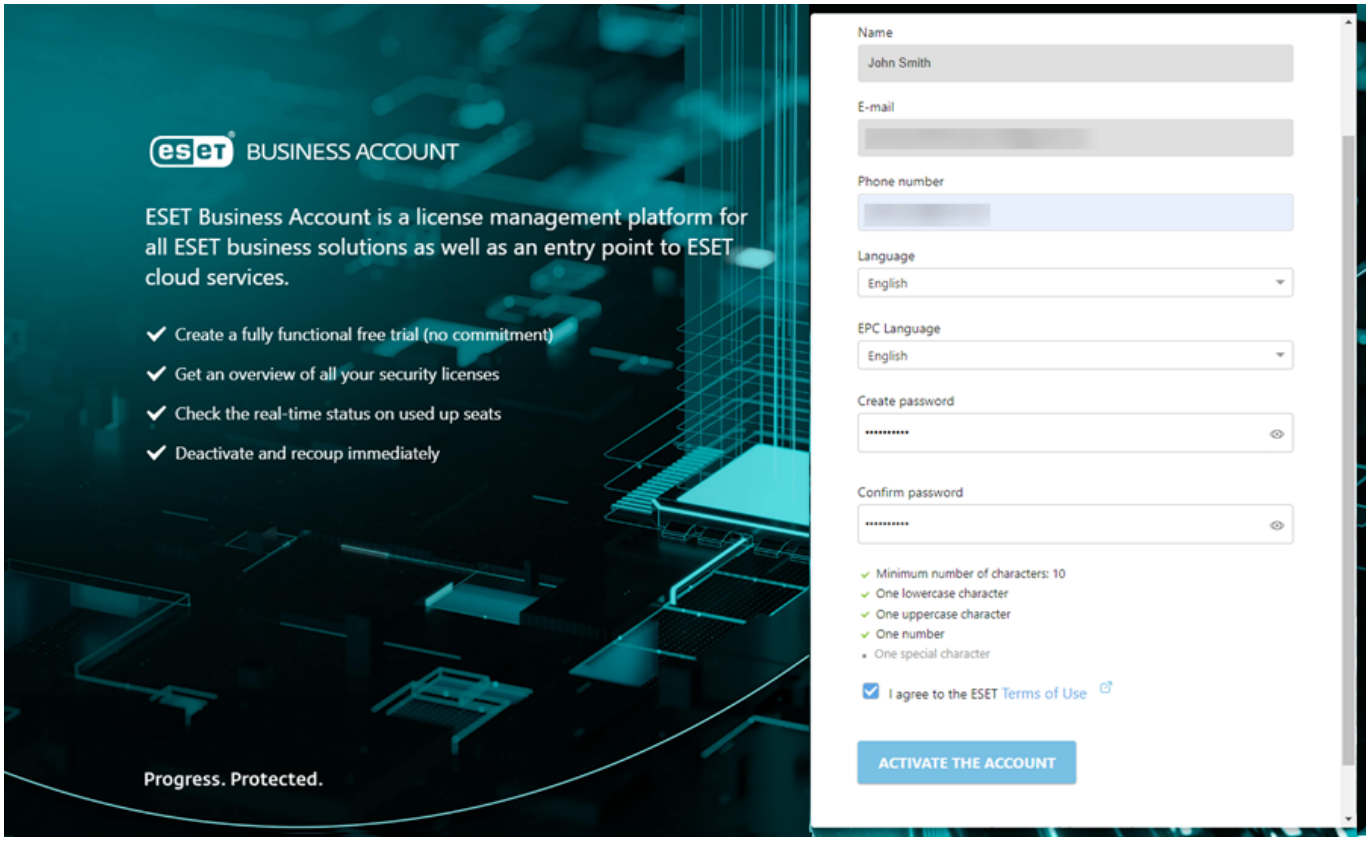
4. El nuevo usuario aparece en la sección Administración de usuarios con la etiqueta **Esperando activación**.



5. El usuario recibirá un mensaje de correo electrónico de activación (en la dirección de correo electrónico que especificó al crear el usuario). El usuario debe hacer clic en **Activar su cuenta**.



6. El usuario debe ajustar la configuración del usuario y escribir la contraseña dos veces (**Crear contraseña** y **Confirmar contraseña**), marcar la casilla de verificación **Acepto los términos de uso de ESET** y hacer clic en **Activar la cuenta**.



7. Asigne el usuario en ESET PROTECT 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 PROTECTRecorrido 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, 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 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** y **Cuentas asignadas**. 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 sus dispositivos
• Dispositivos Windows
• Dispositivos macOS
• Dispositivos Linux
• Dispositivos móviles
Administrar dispositivos
• Crear tarea del cliente
• Crear nueva directiva
• Asignar directiva
• Descargar política de migración
• Configurar protección
Administrar cuenta
• Abrir ESET Business Account
• Administrar derechos de acceso
• Administrar licencias
Otros
• Funciones de vista previa

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

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

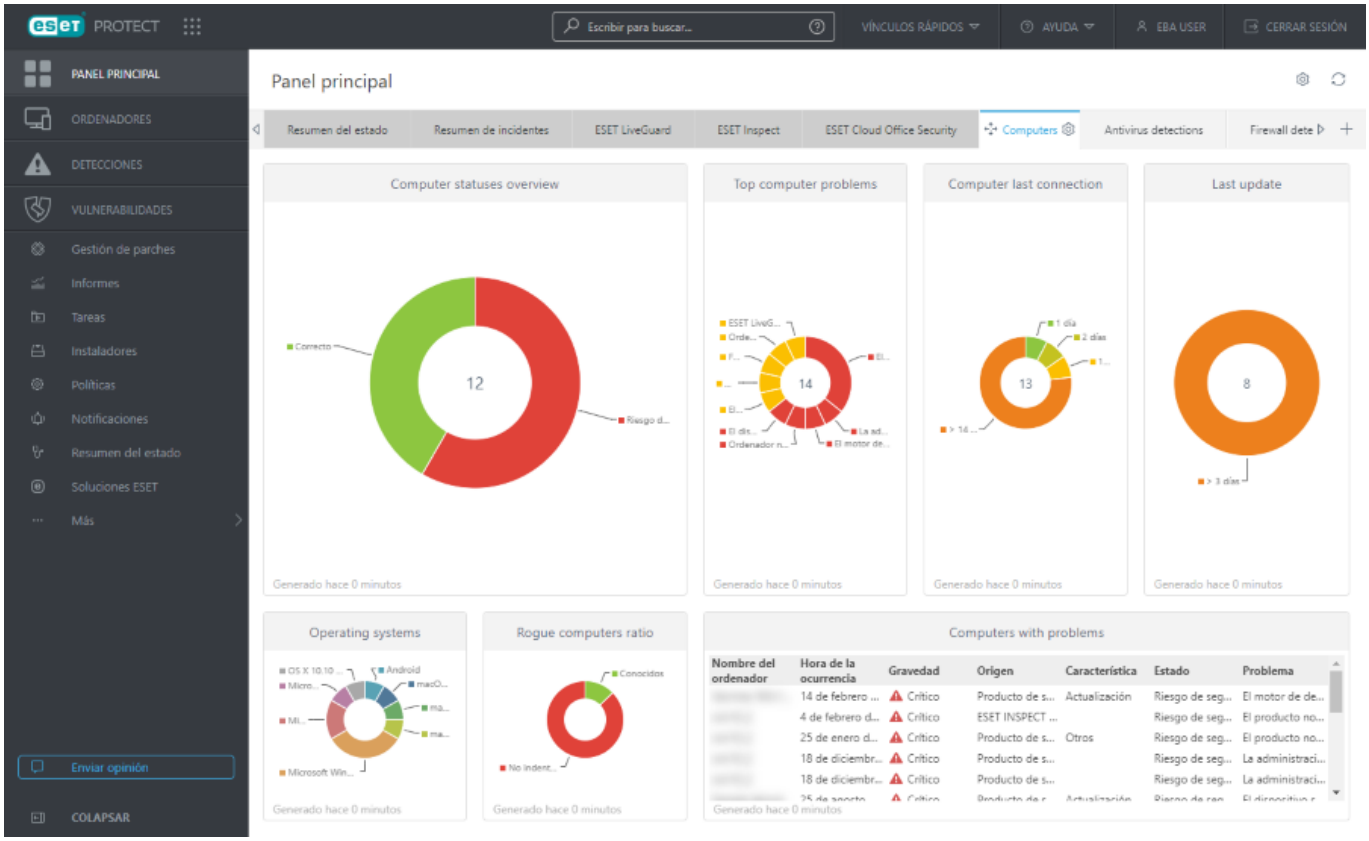
- Haga clic en **Actualizar** para actualizar la información que se muestra.

- 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.

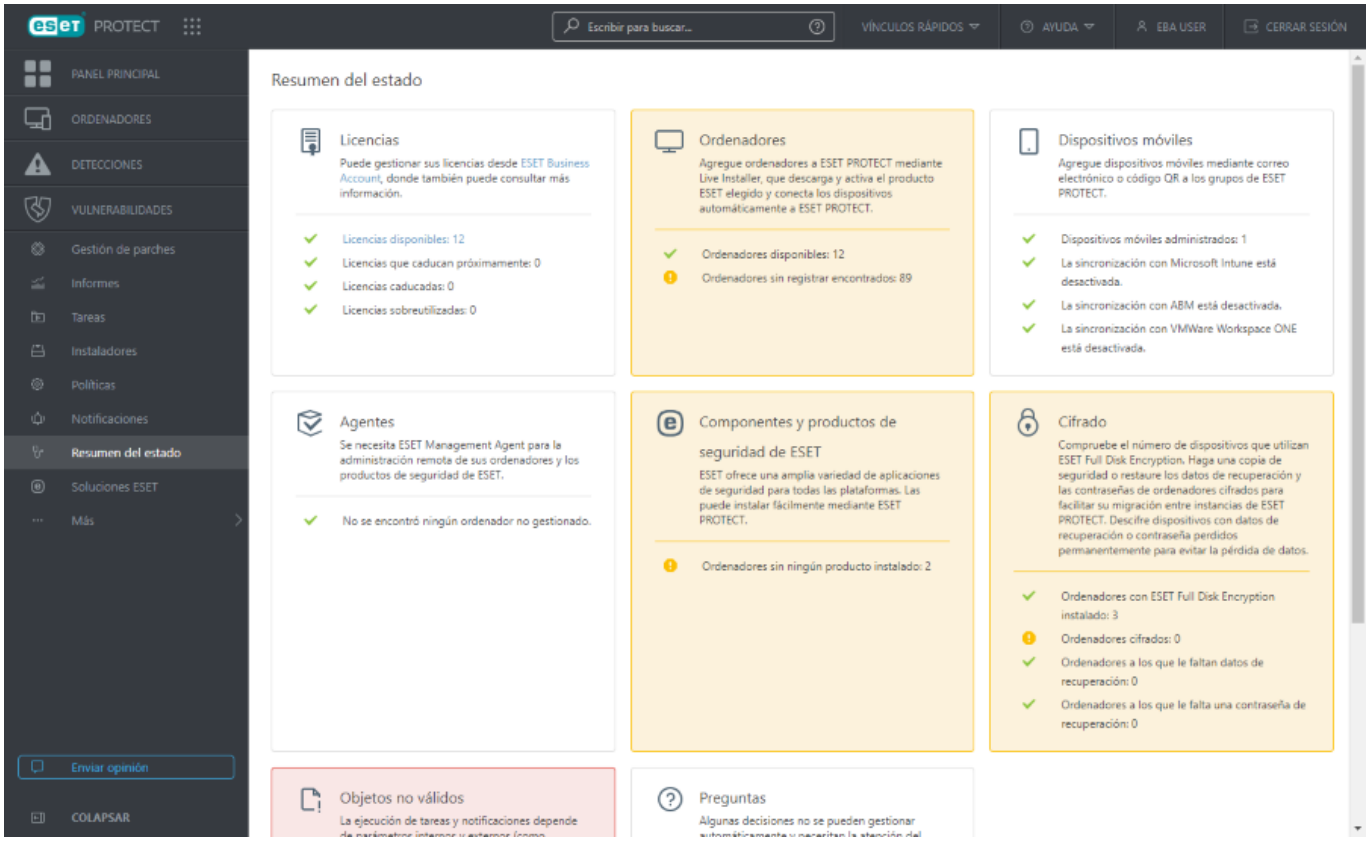
- ESET PROTECT Web Console informa al administrador sobre los Acuerdos de licencia de usuario final actualizados de los productos de seguridad ESET administrados o el tráfico inusualmente elevado de los

ordenadores administrados.

- Haga clic en el logotipo de ESET PROTECT para abrir la pantalla Panel.

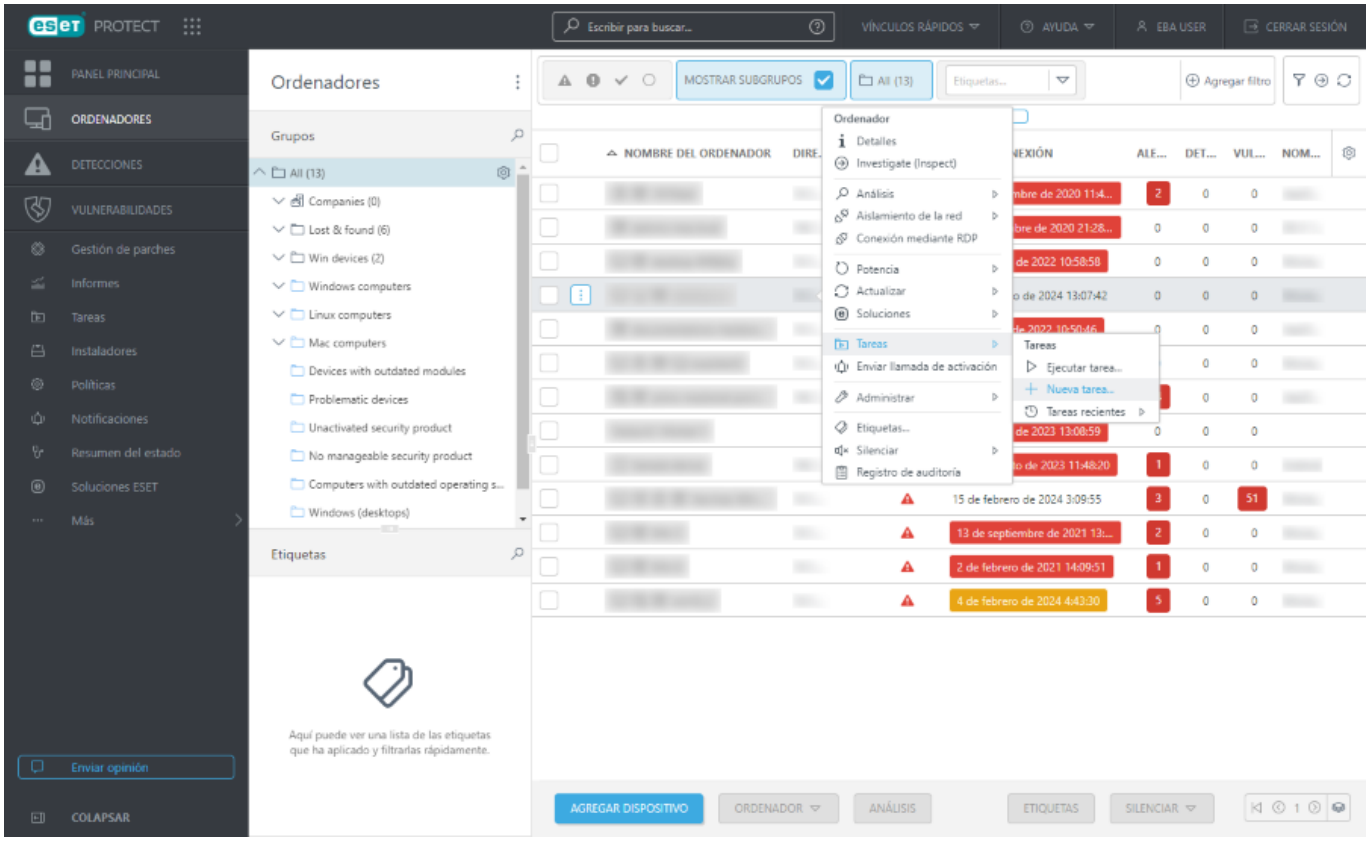


Resumen del estado le enseña cómo sacar el máximo partido de ESET PROTECT. Le guiará a lo largo de los pasos recomendados.



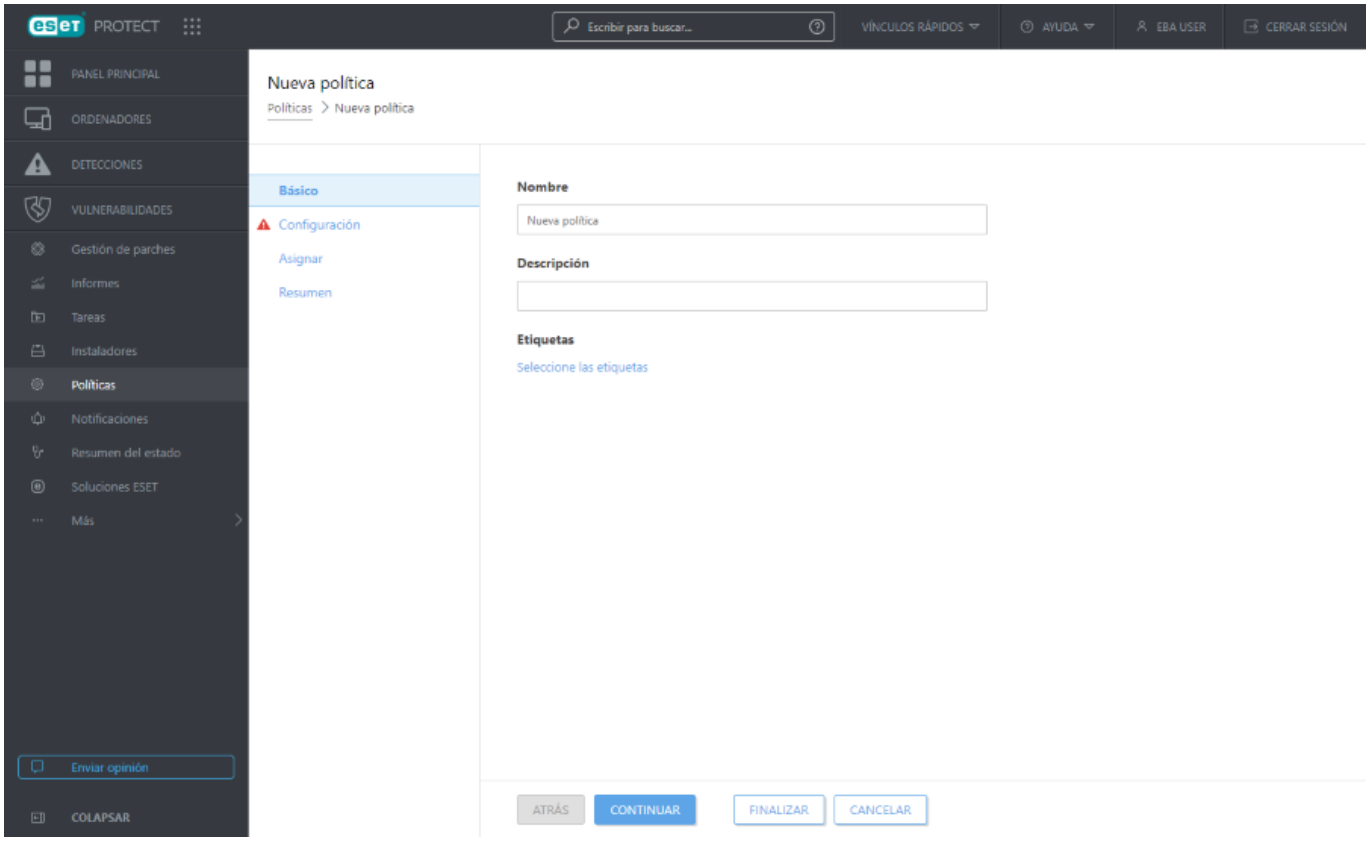
Las pantallas con árboles tienen controles específicos. El árbol en sí se encuentra a la izquierda con las acciones debajo. Haga clic en un elemento del árbol para ver las opciones.

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 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

Le recomendamos que inicie sesión en ESET PROTECT a través de ESET Business Account. Desde ESET Business Account puede abrir ESET PROTECT directamente. Este es el método de inicio de sesión recomendado porque, de esta forma, iniciará sesión en ESET Business Account y ESET PROTECT de forma simultánea. Aunque también puede iniciar sesión en ESET PROTECT directamente desde el inicio de sesión de ESET PROTECT, puede experimentar problemas con determinadas funciones que requieren que inicie sesión en ESET Business Account.

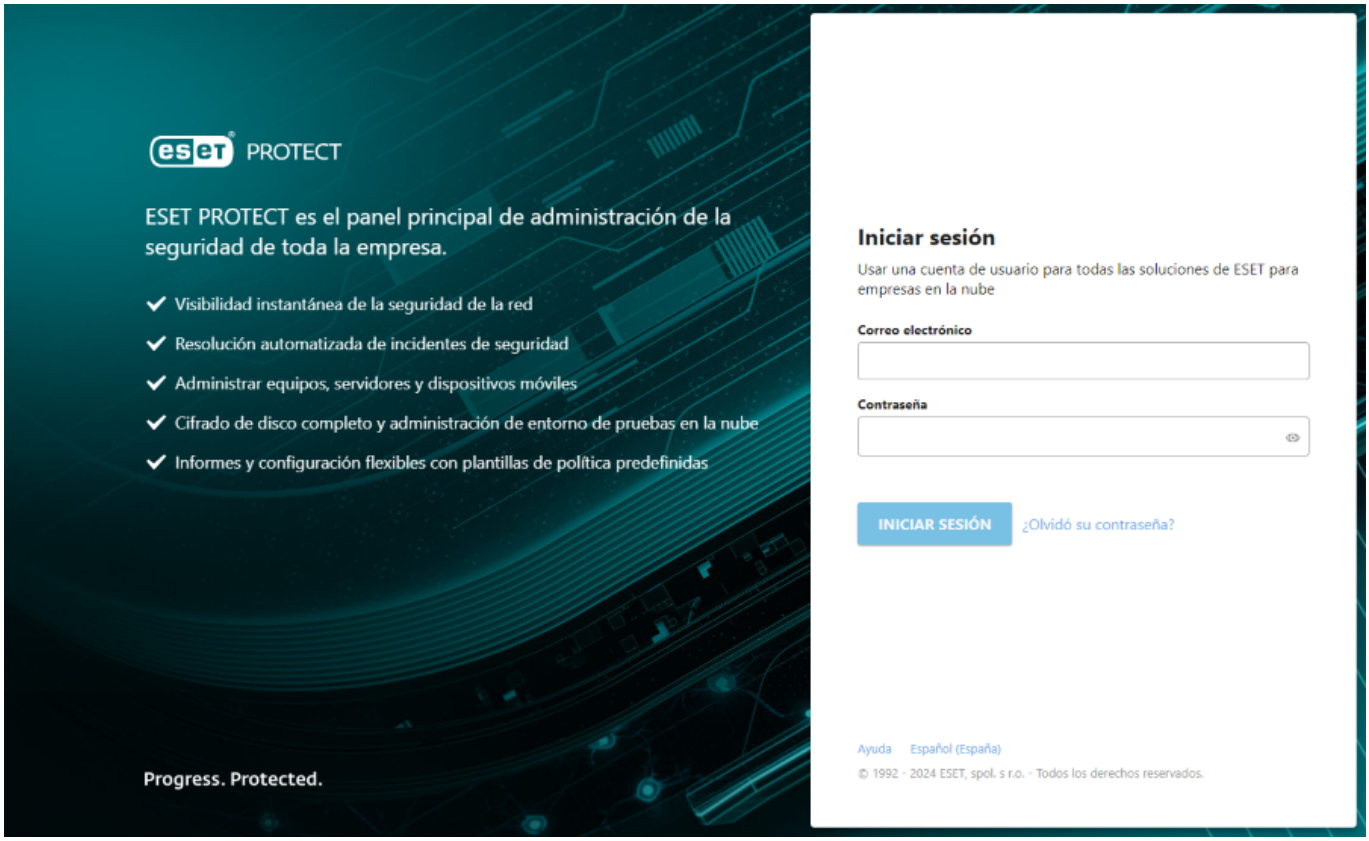
Las credenciales de inicio de sesión de ESET Business Account (nombre de usuario y contraseña) se utilizan para los dos métodos descritos anteriormente.

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.

El idioma de la pantalla de inicio de sesión y de ESET PROTECT Web Console se puede cambiar en **Configuración del usuario** > **Idioma** en ESET Business Account.

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 configuración inicial de su instancia de ESET PROTECT y su idioma no puede cambiarse.

Contraseña olvidada le permite recuperar la contraseña olvidada de su cuenta.



Administración de la sesión y medidas de seguridad:

Bloqueo de la dirección IP de inicio de sesión

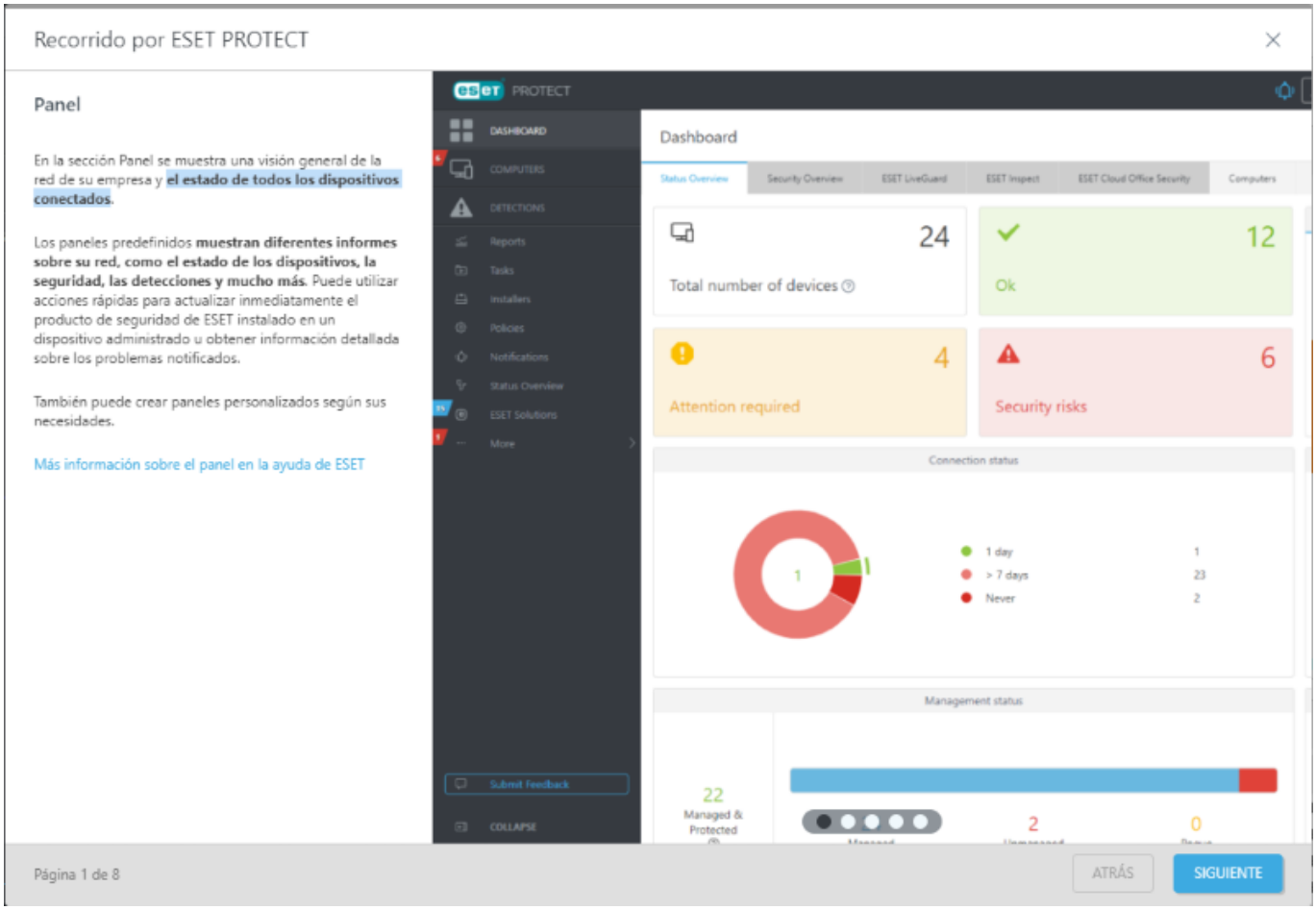
Después de 10 intentos de inicio de sesión sin éxito desde la misma dirección IP (por ejemplo, si se utilizan credenciales de inicio de sesión incorrectas), se bloquearán temporalmente los intentos adicionales de inicio de sesión desde esta dirección IP. Transcurridos 15 minutos, inicie sesión con las credenciales correctas. La prohibición de intentos de inicio de sesión de la dirección IP no afecta a las sesiones existentes.

Recorrido por ESET PROTECT

Cuando inicie sesión en Web Console por primera vez, aparecerá un ESET PROTECTRecorrido 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** 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**, haga clic en **X**. Se abrirá ESET PROTECT Web Console. El **Recorrido por ESET PROTECT** no aparecerá la próxima vez que inicie sesión en ESET PROTECT Web Console.

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

Configurar protección

La siguiente configuración solo es válida para usuarios de ESET Business Account con ESET PROTECT.

Cuando inicia sesión en Web Console, aparece el asistente **Configurar su protección**. Puede configurar fácilmente ajustes de seguridad específicos de forma global en toda la red sin utilizar políticas ni grupos dinámicos.

También puede abrir el asistente desde:

- **Vínculos rápidos** > haga clic en **Configurar protección**.
- **Ordenadores** > haga clic en el icono del engranaje situado junto a **Todo** en Grupos, > haga clic en **Configurar protección**.
- **Políticas** > haga clic en la política **Configuración de la protección: mediante la configuración de la protección** > haga clic en **Configurar protección**.
- **Resumen del estado** > haga clic en la ventana **Componentes y productos de seguridad de ESET** > haga clic en el botón **Configurar protección**.

Para ver el asistente **Configurar su protección**, necesita los siguientes derechos de acceso:
- Acceso de lectura: grupo estático Todo
- Acceso de lectura: políticas

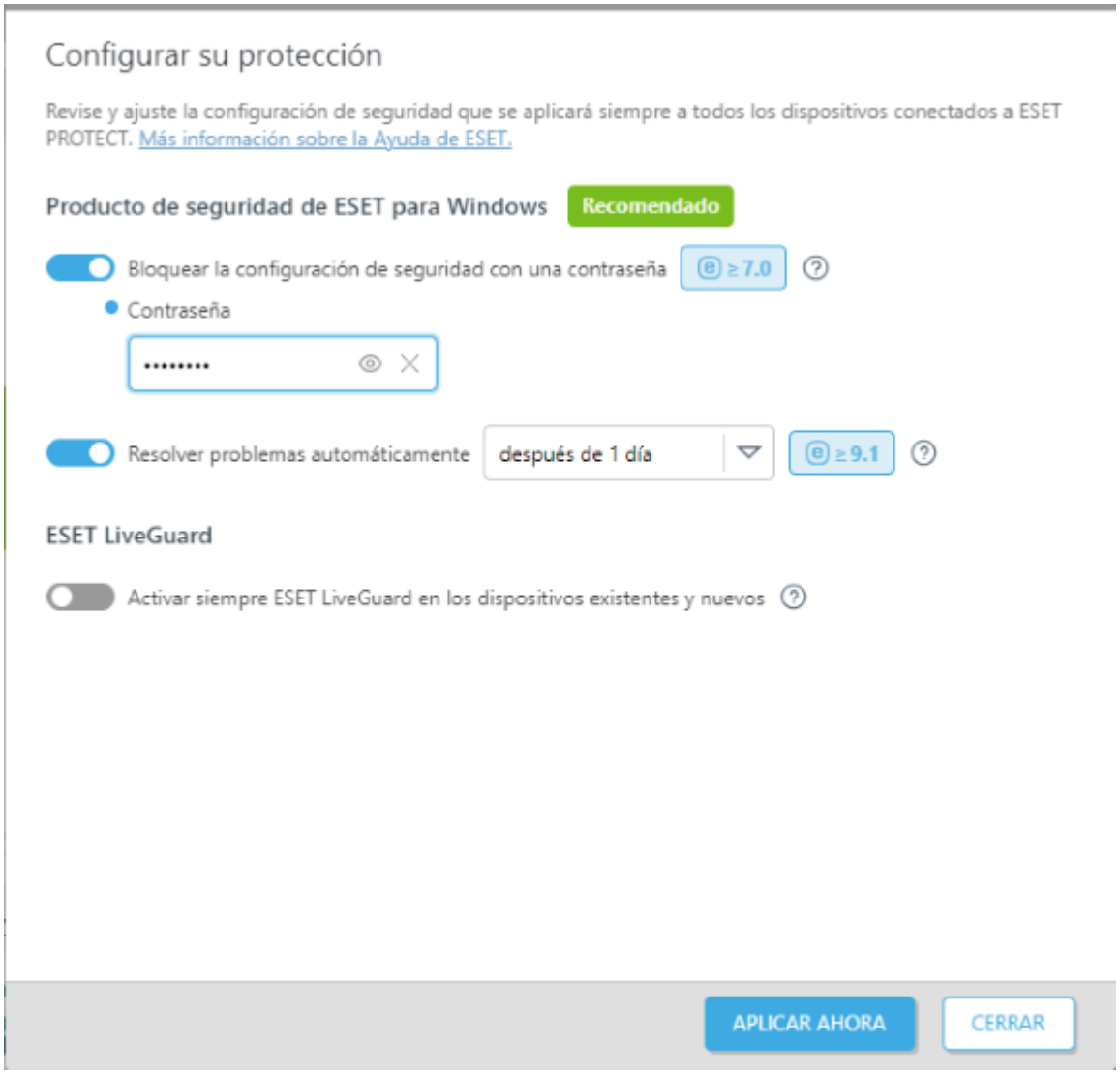
Para editar el asistente **Configurar su protección**, necesita los siguientes derechos de acceso:
Producto de seguridad de ESET para Windows parte:
- Acceso de uso: grupo estático Todo
- Acceso de escritura: políticas

Si no tiene los derechos de acceso necesarios, la parte **Producto de seguridad de ESET para Windows** se desactiva.
ESET LiveGuard parte:
- Acceso de uso: grupo estático Todo
- Acceso de uso: licencias
- Acceso de escritura: tarea del cliente de activación del producto

Si no tiene los derechos de acceso necesarios, la parte **ESET LiveGuard** se desactiva.
Si no tiene licencia de ESET LiveGuard Advanced, la parte **ESET LiveGuard** no está disponible.

Cuando caduque la licencia de ESET LiveGuard Advanced, la configuración de implementación automática se almacenará, pero no se mostrará. Al renovar la licencia, la configuración se habilita y se vuelve a mostrar.

El asistente le pide que aumente el nivel de seguridad de los dispositivos conectados a ESET PROTECT.



Producto de seguridad de ESET para Windows

1. Active **Bloquear la configuración de seguridad con una contraseña** para crear una contraseña que impida a los usuarios finales cambiar las políticas en los dispositivos conectados sin saber la contraseña.

El ajuste es compatible con:
- ESET Endpoint Security para Windows 7.0 y versiones posteriores:
- ESET Server Security for Microsoft Windows Server, ESET File Security for Microsoft Windows Server
- ESET Mail Security for Microsoft Exchange Server
- ESET Mail Security for IBM Domino
- ESET Security for Microsoft SharePoint Server

2. Escriba una contraseña con un mínimo de 8 caracteres en **Contraseña**.

La contraseña que cree se aplicará siempre automáticamente a todos los dispositivos conectados. Recuerde la contraseña. Si olvida la contraseña, puede sobrescribirla con una nueva en ESET PROTECT, pero no podrá recuperar la contraseña anterior.

3. Active **Resolver problemas automáticamente** para activar el reinicio automático de los dispositivos conectados necesario después de actualizar un producto de seguridad de ESET.

Si un usuario final o el administrador no resuelven este reinicio manualmente en un intervalo de tiempo establecido, el dispositivo se reinicia automáticamente.

El ajuste es compatible con ESET Endpoint Security para Windows 9.1 y versiones posteriores. No está disponible para productos de servidor.

4. Seleccione un intervalo de tiempo para el reinicio automático en el menú desplegable:
   - No se puede posponer
   - Después de 1-5 horas
   - Después de 1-30 días

ESET LiveGuard

5. Active **Activar siempre ESET LiveGuard en nuevos dispositivos** para activar la implementación automática de ESET LiveGuard Advanced en dispositivos recién conectados con un producto de seguridad de ESET compatible instalado.

Recomendamos seleccionar **Protección óptima** para asignar nuevas políticas con protección óptima. Puede cambiar su selección también en la sección **ESET LiveGuard Advanced** de Soluciones de ESET.

6. Haga clic en **Aplicar ahora** para aplicar la configuración de seguridad.

Puede ver la configuración en **Políticas** > **Configuración de la protección: mediante la configuración de la protección**. No puede editar ni eliminar estas políticas, pero puede cambiar su asignación (de forma predeterminada, están asignadas al grupo estático **Todo**).

Desactivar configuración

Puede desactivar la configuración con el conmutador de alternancia .

Si desactiva **Bloquear la configuración de seguridad con una contraseña**, se sobrescribirán las políticas de contraseña actuales en los dispositivos conectados. Si una contraseña protegía la configuración de seguridad en esos dispositivos, la contraseña ya no será necesaria.

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.

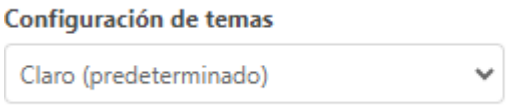
i La configuración del usuario solo se aplica al usuario que ha iniciado sesión.

Configuración de temas

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

- **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:



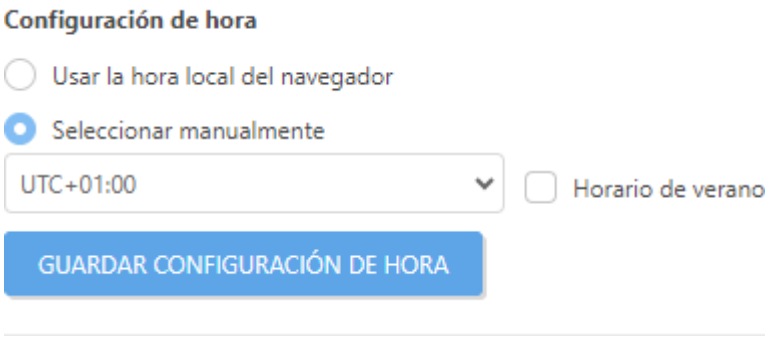
La pantalla permanece en el tema seleccionado tras cerrar sesión en Web Console e iniciar sesión de nuevo.

Configuración de hora

i 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 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.

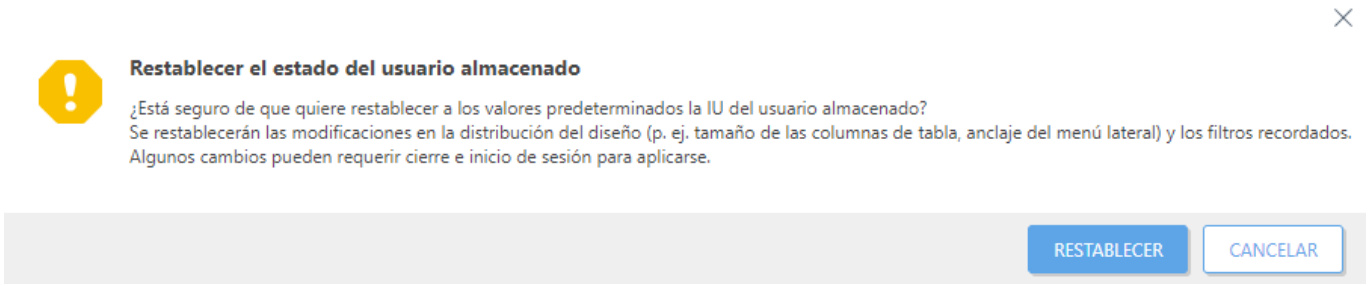


En algunos casos, la opción de utilizar una zona horaria distinta estará disponible. Cuando se configura un desencadenador, se utiliza la zona horaria de ESET PROTECT Web Console de forma predeterminada. También puede marcar la casilla de verificación **Usar la hora local del destino** para usar la zona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

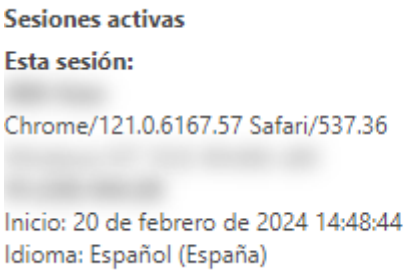
Puede restablecer los valores predeterminados de un estado almacenado de la IU del usuario haciendo clic en **Restablecer estado almacenado del usuario**. Esto incluye el ESET PROTECTRecorrido por***, los tamaños de columna de las tablas, los filtros recordados, el menú lateral anclado, etc.



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.
- Fecha y hora de inicio de sesión del usuario.
- Idioma seleccionado para ESET PROTECT Web Console.



La sesión actual lleva la etiqueta **Esta sesión**.

Filtros y personalización del diseño

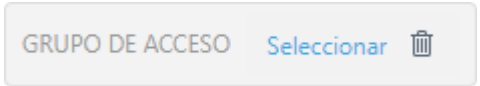
ESET PROTECT Web Console le permite personalizar el diseño de los elementos que aparecen en las secciones principales (por ejemplo, **Ordenadores**, **Tareas**, etc.) de varias maneras:

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.

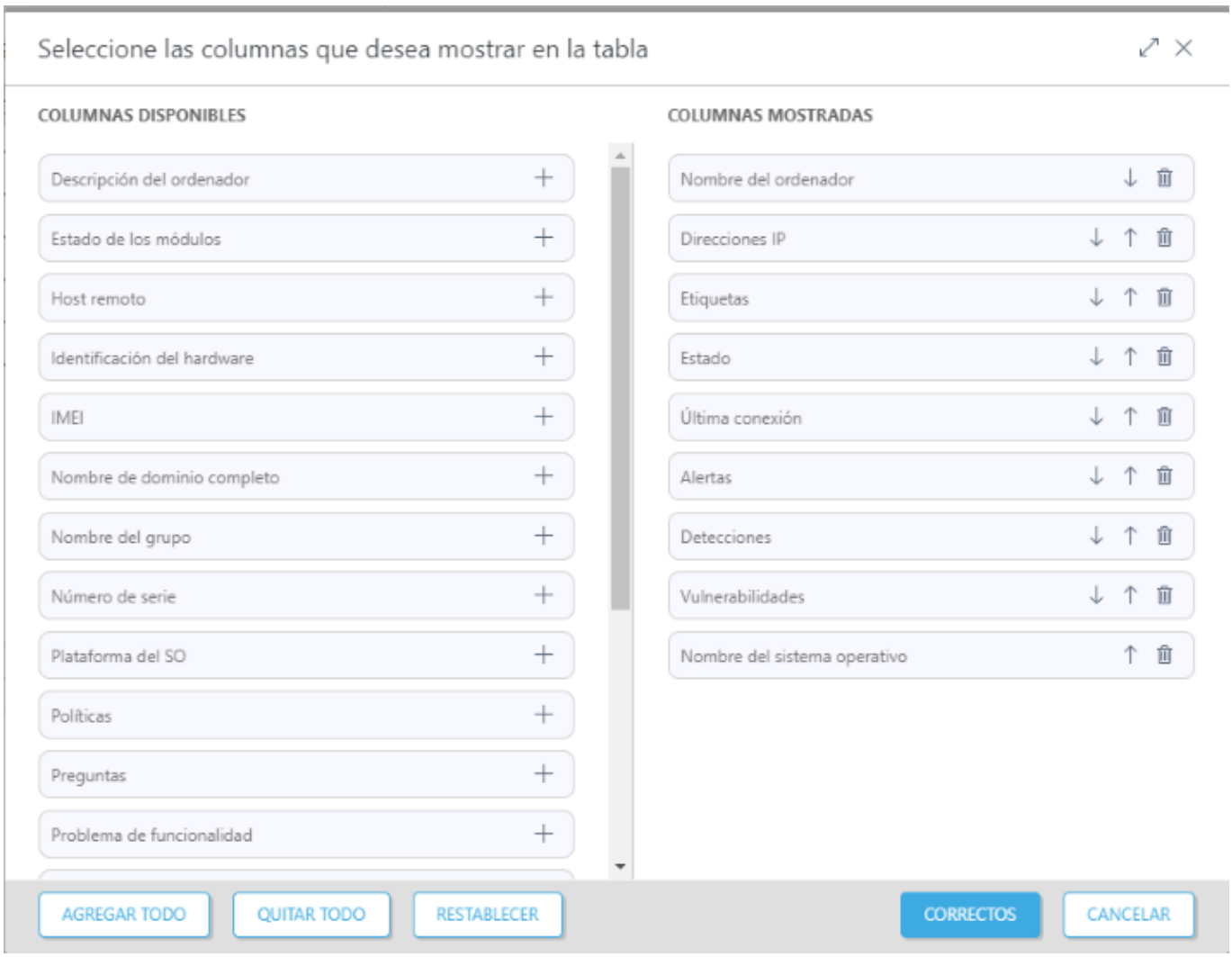
Para clasificar por una sola columna, haga clic en el encabezado de la columna para clasificar las filas de la tabla en función de los datos de la columna seleccionada.

- 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.

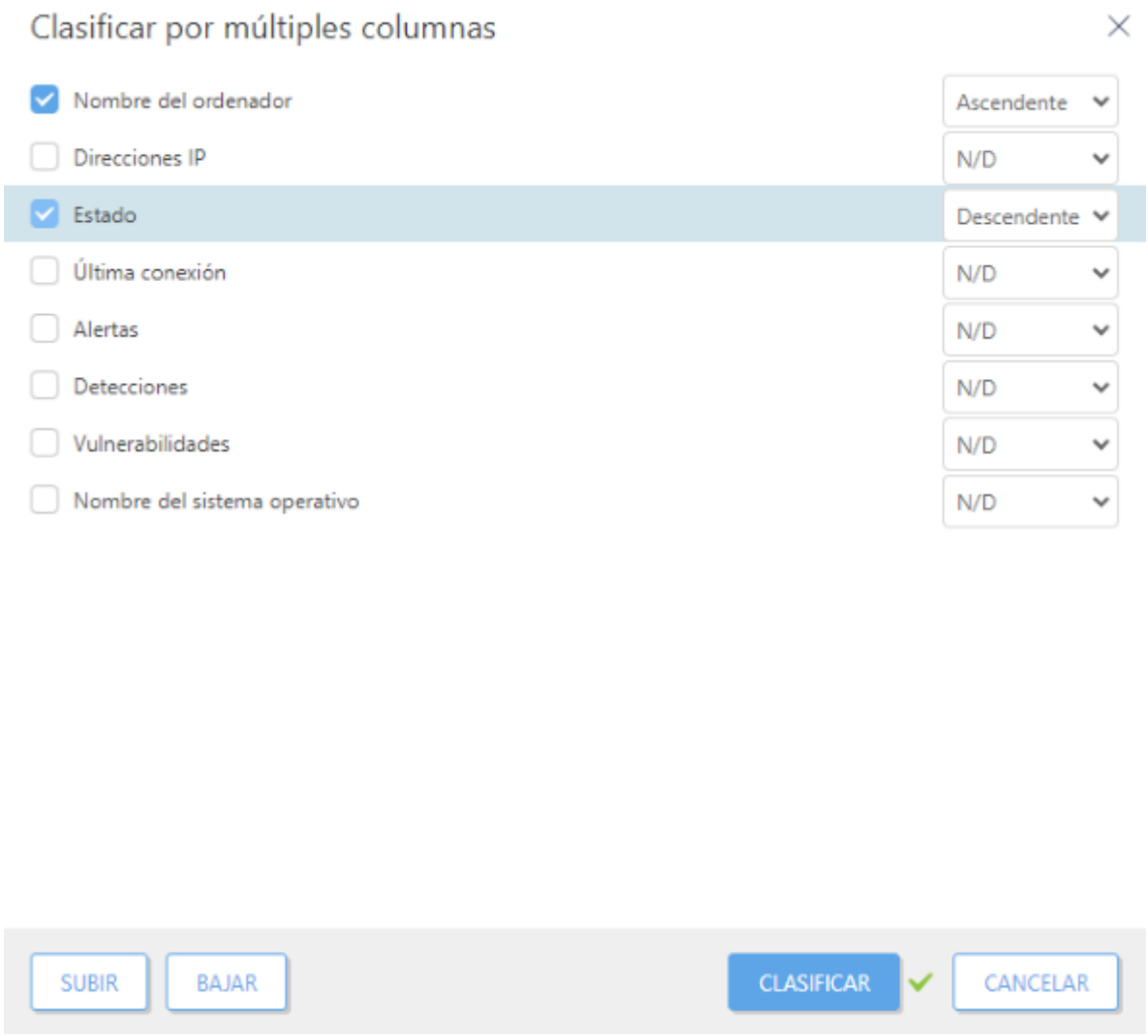
Clasificación de tablas

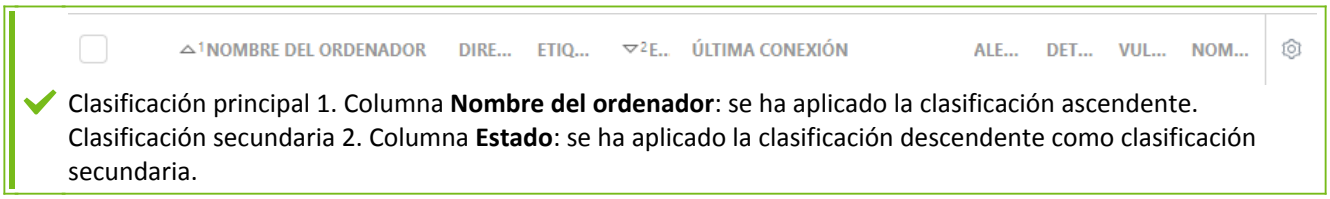
- **Restablecer clasificación**: restablece la clasificación de las columnas.

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

  - Prioridad 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.

  - Comportamiento 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 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

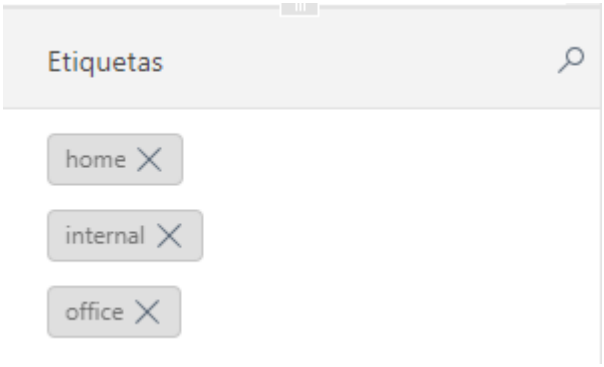
principales de ESET PROTECT Web Console.

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:



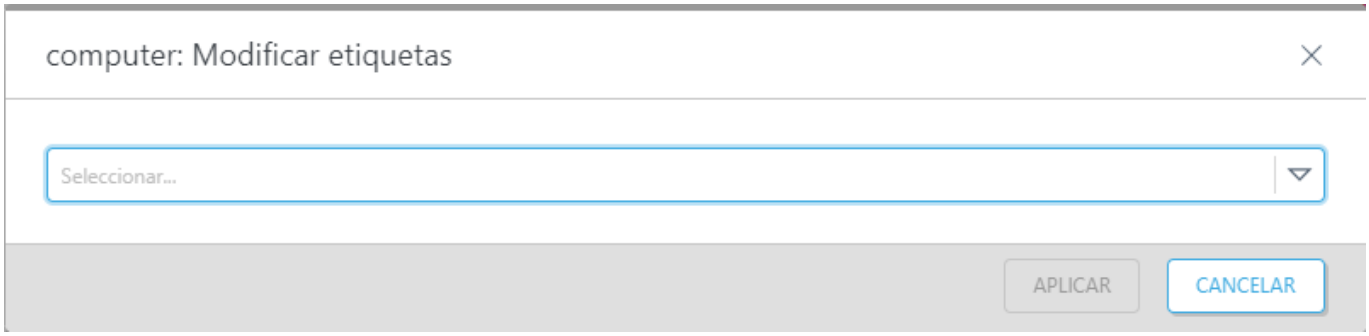
Permisos de administración de etiquetas

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.

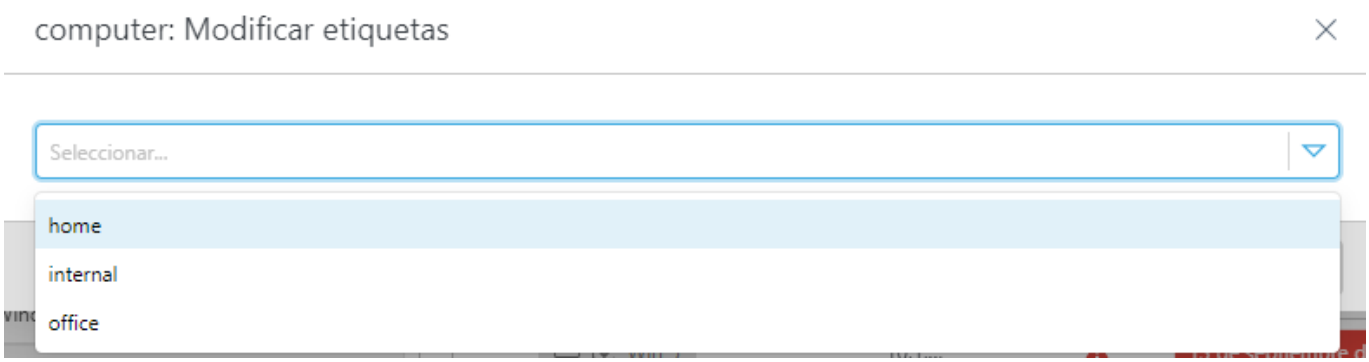
Asignar etiquetas

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**:

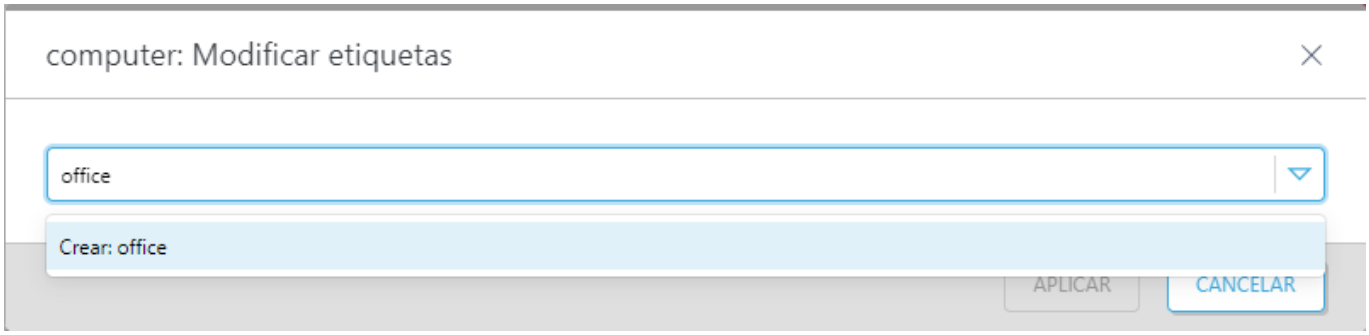


Para asignar etiquetas existentes, haga clic en el campo para escribir de una etiqueta de la lista y haga clic en **Aplicar**.



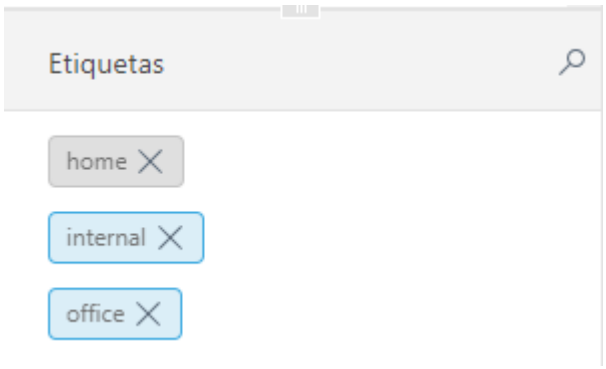
Crear una etiqueta nueva

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.



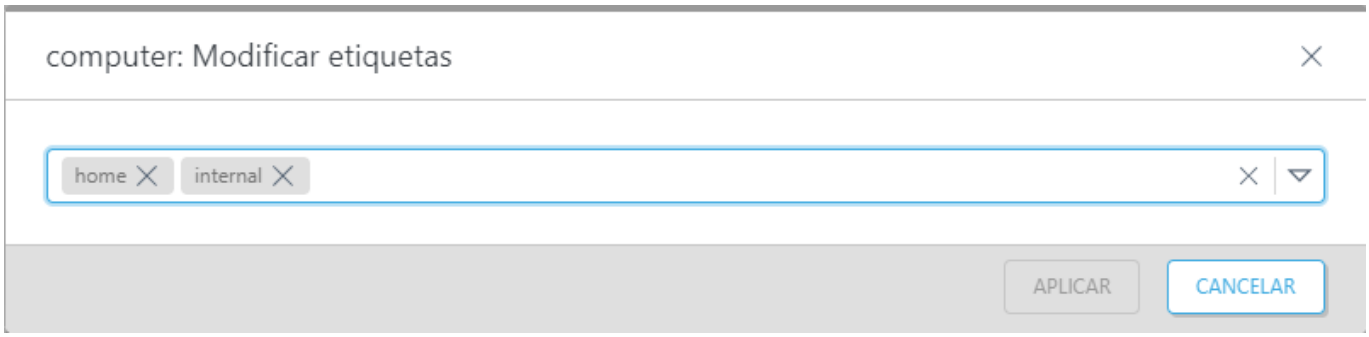
Filtrar objetos con las etiquetas

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



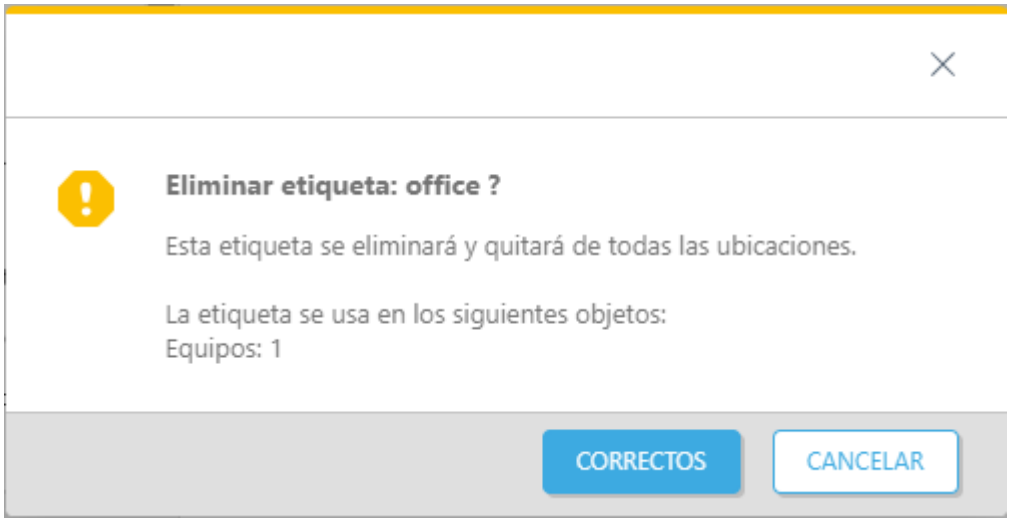
Cancelar asignación de etiquetas

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. 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**.

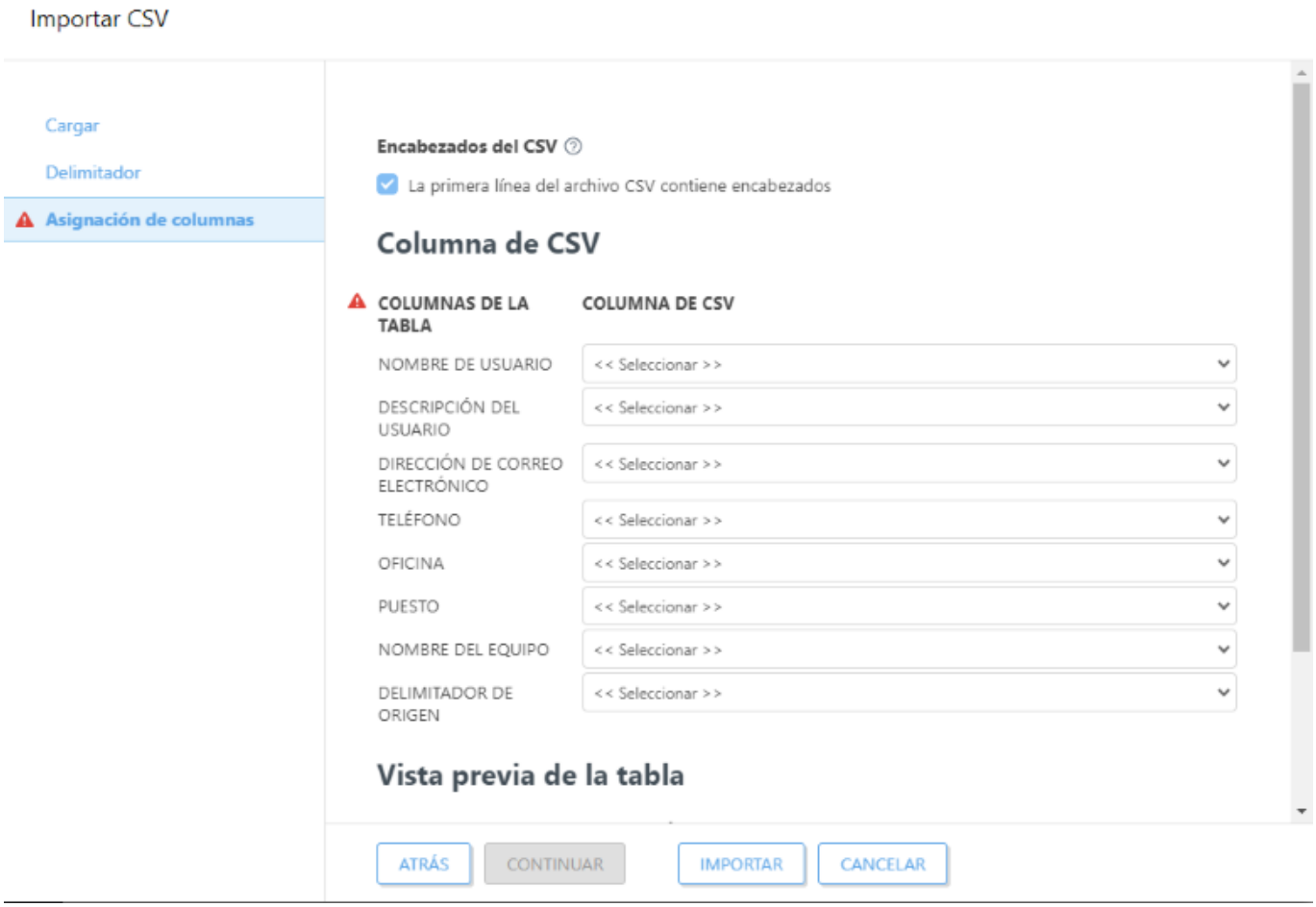
3.**Delimitador**: un delimitador es un carácter utilizado para separar cadenas de texto. Seleccione un delimitador adecuado (**Punto y coma**, **Coma**, **Espacio**, **Tabulador**, **Punto**, **Barra vertical**) en función de la opción que se utilice en el archivo *.csv*. Si en su archivo *.csv* se 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 mostrada en la tabla. Utilice las listas desplegables para seleccionar qué columna de CSV se debe asociar con una columna de ESET PROTECT 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

Como ESET PROTECT se aloja en la nube, la mayoría de los errores que pueden producirse durante el inicio de sesión pueden resolverse siguiendo estos pasos generales de solución de problemas:

- Elimine la memoria caché del navegador y actualice la página de inicio de sesión.

- Si el problema persiste, espere unos minutos y vuelva a intentar iniciar sesión o pruebe con otro navegador (navegadores compatibles).

- Si el problema no se resuelve, póngase en contacto con el servicio de asistencia técnica de ESET.

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:

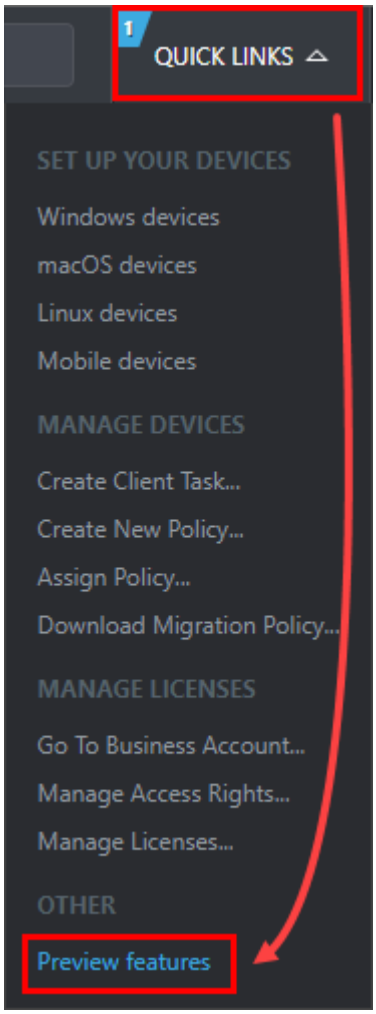
Mensaje de error	Posible causa
⚠ No se pudo iniciar sesión: Se ha bloqueado temporalmente la comunicación desde su dirección	Después de 10 intentos de inicio de sesión sin éxito desde la misma dirección IP (por ejemplo, si se utilizan credenciales de inicio de sesión incorrectas), se bloquearán temporalmente los intentos adicionales de inicio de sesión desde esta dirección IP. Una vez transcurridos 15 minutos, inicie sesión con las credenciales correctas.
⚠ No se pudo iniciar sesión: Error de autenticación ⚠ No se pudo iniciar sesión: la autenticación falló en el servidor	El servidor ha recibido un token de autenticación dañado o incompleto. Asegúrese de utilizar las credenciales de inicio de sesión correctas y de que su conexión a la página de inicio de sesión sea segura. Si el problema persiste, pruebe a borrar las cookies.
⚠ No se pudo iniciar sesión: La conexión ha fallado con el estado de "No conectado" ⚠ No se pudo iniciar sesión: Error de comunicación ⚠ No se pudo iniciar sesión: Tiempo de espera de la conexión agotado	Compruebe la conexión de red y la configuración de firewall para asegurarse de que se pueda acceder a la Consola web ESET PROTECT desde su dispositivo.
⚠ No se pudo iniciar sesión: El usuario no tiene ningún derecho de acceso asignado	La cuenta de usuario con la que intenta iniciar sesión no tiene derechos de acceso asignados. Inicie sesión como administrador y modifique la cuenta del usuario para asignar a este usuario los permisos correspondientes. Si no tiene acceso a la cuenta de administrador, póngase en contacto con su administrador y trasládele esta solicitud.
JavaScript está desactivado. Active JavaScript en su navegador.	JavaScript es necesario para que la página de inicio de sesión funcione correctamente. Active JavaScript o actualice su navegador web.
No ve la pantalla de inicio de sesión o parece estar cargándose continuamente.	Compruebe la conexión de red y la configuración de firewall para asegurarse de que se pueda acceder a la Consola web ESET PROTECT desde su dispositivo. El Portal de estado de ESET muestra el estado actual de los servicios en la nube de ESET, las interrupciones programadas y los incidentes pasados. Si tiene un problema con un servicio ESET compatible y no lo ve listado en el Portal de estado, comuníquese con el soporte técnico de ESET. Los equipos de supervisión verifican los posibles problemas internamente, y los incidentes confirmados se publican y actualizan manualmente para mantener una alta credibilidad y precisión. Por lo tanto, aparecen en el Portal de estado con un ligero retraso. Es posible que un incidente de corta duración no se publique si se resuelve antes de confirmarse manualmente.
"Se ha producido un error inesperado" o "Se ha producido una excepción no detectada"	Este error puede producirse si accede a ESET PROTECT Web Console desde un navegador que no sea compatible con ESET PROTECT Web Console. Consulte navegadores web compatibles.

Mensaje de error	Posible causa
SEC_ERROR_INADEQUATE_KEY_USAGE (solo Mozilla Firefox).	Mozilla Firefox tiene un almacén de certificados dañado.

Funciones de vista previa

Las funciones de vista previa permiten al usuario probar nuevas funciones individuales en ESET PROTECT.

Puede acceder al menú **Funciones de vista previa** desde el menú desplegable **Vínculos rápidos**.



En el menú de funciones de vista previa, el administrador puede encontrar todas las funciones de vista previa disponibles con una breve descripción de la funcionalidad de cada función de vista previa. A continuación, el administrador puede **Activar** o **Desactivar** cada una de las funciones de vista previa y también **Enviar opinión** para cada una de las funciones de vista previa disponibles.

Tras la activación, la función de vista previa está disponible al instante en la consola de administración.

Las funciones de vista previa más recientes disponibles en su consola de administración son:

> En la versión actual no hay disponibles funciones de vista previa.

Sincronizar ESET PROTECT con Active Directory

Utilice el **ESET Active Directory Scanner** para sincronizar los ordenadores y usuarios de Active Directory con ESET PROTECT Web Console.

ESET actualiza Active Directory Scanner de forma periódica para mejorar su funcionalidad. Puede ver más detalles en el registro de cambios.

Requisitos previos

- Ejecute Active Directory Scanner como usuario de Active Directory en un ordenador conectado a Active Directory.
- Sistemas operativos compatibles (compatibilidad con HTTP/2): Windows 10, Windows Server 2016 y versiones posteriores.
- Descargue e instale .NET Core Runtime.
- Prepare el archivo de configuración de usuarios (*config.json*) para la sincronización de usuarios de Active Directory. *config.json* está incluido en el archivo .zip **Active Directory Scanner**.
- Permiso de derechos de acceso del usuario para el **token de acceso del análisis de AD**: **Escritura**

Uso de Active Directory Scanner

1. En ESET PROTECT Web Console, cree el script de implementación de GPO del agente.
2. Inicie sesión en un ordenador en su Active Directory con una cuenta de usuario de Active Directory. Asegúrese de que se ajusta a los requisitos previos mencionados.
3. Descargue el Active Directory Scanner más reciente en el ordenador.
4. Descomprima el archivo descargado.
5. Descargue el script de implementación de GPO del agente (creado en el paso 1) y cópielo en la carpeta *ActiveDirectoryScanner* (una carpeta que contiene todos los archivos de Active Directory Scanner).

Sincronización de ordenadores de Active Directory

1. En ESET PROTECT Web Console, vaya a **Ordenadores** y seleccione el grupo estático en el que desea sincronizar la estructura de Active Directory.
2. Haga clic en el icono del **engranaje** situado junto al grupo estático seleccionado y seleccione **Active Directory Scanner**.
3. Haga clic en **Generar** para obtener el token de acceso.

Cada grupo estático tiene un token. El token identifica el grupo estático en el que se sincronizará Active Directory.
Para invalidar el token actual por motivos de seguridad, haga clic en **Volver a generar** para crear un nuevo token. Si la sincronización de Active Directory con ESET PROTECT ya se está ejecutando, la sincronización se detendrá tras el cambio de token de seguridad. Debe ejecutar Active Directory Scanner con el nuevo token para volver a activar la sincronización de Active Directory.
Para eliminar el token por motivos de seguridad, haga clic en **Desactivar token**. Para confirmar la desactivación del token, haga clic en **Desactivar**.

4. Ejecute Active Directory Scanner (sustituya `token_string` por el token que ha copiado en el paso anterior).

```
ActiveDirectoryScanner.exe --token token_string
```

De forma predeterminada, el Active Directory Scanner más reciente no sincroniza los ordenadores Active Directory desactivados. Para sincronizar ordenadores Active Directory desactivados, utilice el parámetro `--disabled-computers`:

```
ActiveDirectoryScanner.exe --token token_string --disabled-computers
```

5. Cuando se le solicite, escriba la contraseña de usuario de Active Directory.
6. Cuando Active Directory Scanner finalice la sincronización, la estructura de Active Directory (unidades organizativas con ordenadores) aparecerá en **Ordenadores** en ESET PROTECT Web Console como grupos estáticos con los ordenadores.

Incluir o excluir la estructura de la unidad organizativa

Para incluir o excluir la estructura de la unidad organizativa, determine la ruta (por ejemplo: `"Users/Bratislava/TechDepartment"`). `"ExcludeByID"` funciona con `sid` de forma predeterminada.
Un ejemplo de la sintaxis:

```
"Include": [
    "path"
            ],
            "Exclude": [
    "path"
            ],
            "ExcludeByID": [
    "sid1", "sid2"...
            ],
```

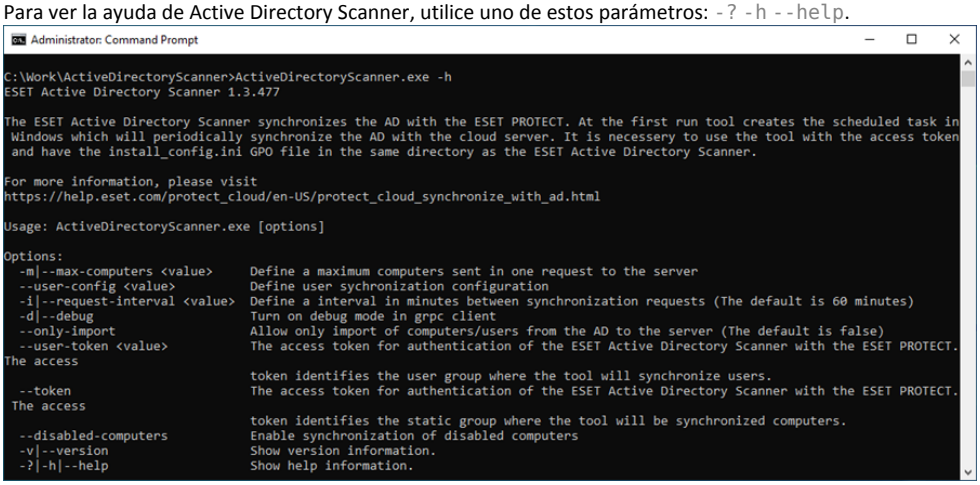
Ejemplo: `"Include" "path" "Users/Bratislava/TechDepartment"` tiene más subunidades, puede excluir cualquier subunidad con `"exclude" "path" "Users/Bratislava/TechDepartment/Test"`

Active Directory Scanner crea una tarea de **Sincronización** de **Active Directory** en el Programador de tareas de Windows con un intervalo de repetición del desencadenador de 1 hora. Puede ajustar el intervalo de sincronización de Active Directory en el Programador de tareas en función de sus preferencias. Los futuros cambios realizados en la estructura de Active Directory se reflejarán en ESET PROTECT Web Console tras la siguiente sincronización.

Limitaciones de sincronización con Active Directory:

- Active Directory Scanner solo sincroniza unidades organizativas de Active Directory que contengan ordenadores con nombres DNS. Las unidades organizativas que no contengan ordenadores no se sincronizarán.
- Si el nombre de la unidad organizativa cambia en Active Directory, se creará un nuevo grupo estático con el nuevo nombre en ESET PROTECT Web Console tras la siguiente sincronización. El grupo estático correspondiente al nombre de la unidad organizativa anterior continuará siendo ESET PROTECT Web Console y estará en blanco. los ordenadores incluidos se moverán al grupo estático con el nuevo nombre.
- Si elimina una unidad organizativa en Active Directory, todos los ordenadores de la unidad se quitarán del grupo estático correspondiente en ESET PROTECT Web Console.
- Si elimina un ordenador de Active Directory sincronizado de ESET PROTECT Web Console, este no volverá a aparecer tras la próxima sincronización, aunque permanezca en Active Directory.

Para ver la ayuda de Active Directory Scanner, utilice uno de estos parámetros: `-? -h --help`.



Para resolver problemas, consulte los registros que se encuentran en *C:\ProgramData\ESET\ActiveDirectoryScanner\Logs*.

Si elimina un ordenador de Active Directory, el ordenador también se eliminará de ESET PROTECT Web Console.

Sincronizar con Usuario de Active Directory

1. En ESET PROTECT Web Console, vaya a **Más** > **Usuarios del ordenador** y seleccione el grupo de usuarios en el que desea sincronizar la estructura de Active Directory.
2. Haga clic en el icono del **engranaje** situado junto al grupo estático seleccionado, seleccione **Active Directory Scanner** y copie el token de acceso generado.
3. Haga clic en **Generar** para obtener el token de acceso.

Cada grupo estático tiene su token. El token identifica el grupo estático en el que se sincronizará Active Directory.
Para invalidar el token actual por motivos de seguridad, haga clic en **Volver a generar** para crear un nuevo token. Si la sincronización de Active Directory con ESET PROTECT ya se está ejecutando, la sincronización se detendrá tras el cambio de token de seguridad. Debe ejecutar Active Directory Scanner con el nuevo token para volver a activar la sincronización de Active Directory.
Para eliminar el token por motivos de seguridad, haga clic en **Desactivar token**. Para confirmar la desactivación del token, haga clic en **Desactivar**.

3. Ejecute Active Directory Scanner (sustituya `token_string` por el token que ha copiado en el paso anterior).

```
ActiveDirectoryScanner.exe --user-token token_string --user-config config.json
```

`--user-token` y `--token` se pueden usar al mismo tiempo. A continuación, la herramienta sincronizará tanto los ordenadores como los usuarios.

Las recomendaciones del archivo de configuración de usuarios (config.json)

Siga las recomendaciones de formato para configurar el archivo *config.json* (ubicado en la misma carpeta que *ActiveDirectoryScanner.exe*). Haga una copia de seguridad del archivo antes de editarlo (puede volver a descargar una copia nueva si es necesario).

- Elimine los comentarios; solo son instrucciones.
- Utilice los campos `"Include"` y `"Exclude"` para especificar los grupos incluidos en la sincronización o excluidos de ella.
- De acuerdo con las instrucciones del archivo *config.json*, recomendamos identificar los grupos utilizando `objectGUID`, no `Distinguished Name`.
- Escriba los valores de `objectGUID` en el siguiente formato:

```
"Include": [ "{objectGUID1}", "{objectGUID2}", ... ],
"Exclude": [ "{objectGUID3}", "{objectGUID4}", ... ],
```

- Sustituya `{objectGUID}` por los valores de `objectGUID` reales de los grupos que desea incluir o excluir. Cada `objectGUID` debe tener el formato de una cadena hexadecimal entre llaves. Por ejemplo, si tiene dos grupos con valores de `objectGUID` de `"12345678-1234-5678-1234-1234567890AB"` y `"98765432-4321-8765-4321-0987654321AB"`, la sección `Include` sería como se indica a continuación:

```
"Include": [ "{12345678-1234-5678-1234-1234567890AB}", "{98765432-4321-8765-4321-0987654321AB}" ],
```

- Para excluir un grupo con `objectGUID` `"55555555-5555-5555-5555-555555555555"`, la sección `Exclude` sería como se indica a continuación:

```
"Exclude": [ "{55555555-5555-5555-5555-555555555555}" ],
```

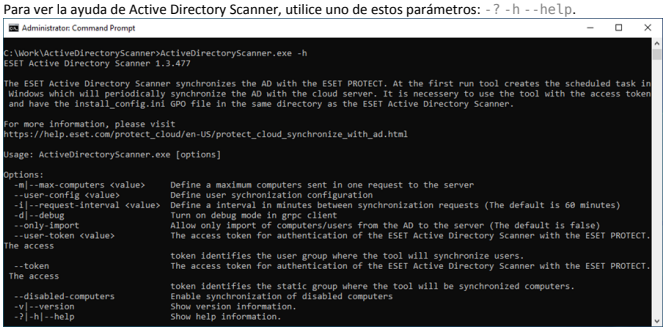
4. Cuando se le solicite, escriba la contraseña de usuario de Active Directory.
5. Cuando Active Directory Scanner finalice la sincronización, la estructura de Active Directory (unidades organizativas con ordenadores/usuarios) aparecerá en **Ordenadores/Usuarios del ordenador** en ESET PROTECT Web Console como grupos estáticos con los ordenadores o **Grupos de usuarios** con los usuarios de **Usuarios del ordenador**.

Active Directory Scanner crea una tarea de **Sincronización** de **Active Directory** en el Programador de tareas de Windows con un intervalo de repetición del desencadenador de 1 hora. Puede ajustar el intervalo de sincronización de Active Directory en el Programador de tareas en función de sus preferencias. Los futuros cambios realizados en la estructura de Active Directory se reflejarán en ESET PROTECT Web Console tras la siguiente sincronización.

Limitaciones de sincronización con Active Directory:

- Active Directory Scanner solo sincroniza las unidades organizativas de Active Directory que contienen usuarios. Las unidades organizativas que no contengan usuarios no se sincronizarán.
- Si elimina una unidad organizativa en Active Directory, todos los usuarios de la unidad se quitarán del grupo de usuarios correspondiente en ESET PROTECT Web Console. Los grupos sincronizados vacíos también se quitan.
- Si elimina un usuario de Active Directory sincronizado desde ESET PROTECT Web Console, este no volverá a aparecer tras la siguiente sincronización, aunque permanezca en Active Directory hasta que alguna de las propiedades sincronizadas se cambie en el origen Active Directory.

Para ver la ayuda de Active Directory Scanner, utilice uno de estos parámetros: `-? -h --help`.



Para resolver problemas, consulte los registros que están en *C:\ProgramData\ESET\ActiveDirectoryScanner\Logs*.

Métodos alternativos

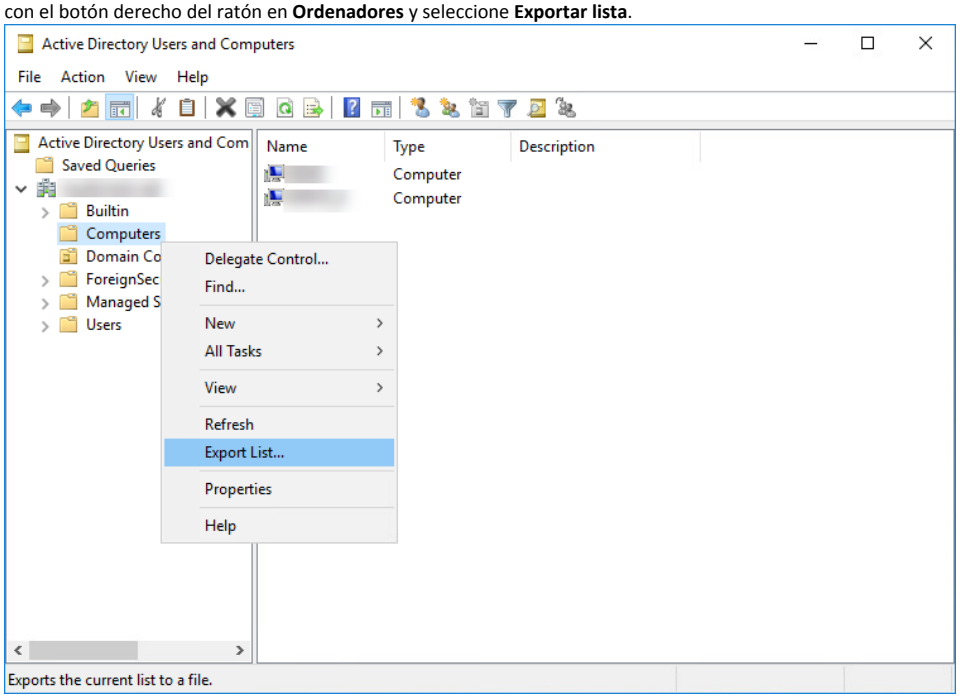
También puede utilizar una de las soluciones alternativas que se indican a continuación:

- Exportar la lista de ordenadores de Active Directory e importarla en ESET PROTECT
- Implementar ESET Management Agent en los ordenadores de Active Directory mediante un objeto de política de grupo

Exportar la lista de ordenadores de Active Directory e importarla en ESET PROTECT

Esta solución solo proporciona una sincronización de Active Directory, y no sincroniza cambios futuros de Active Directory.

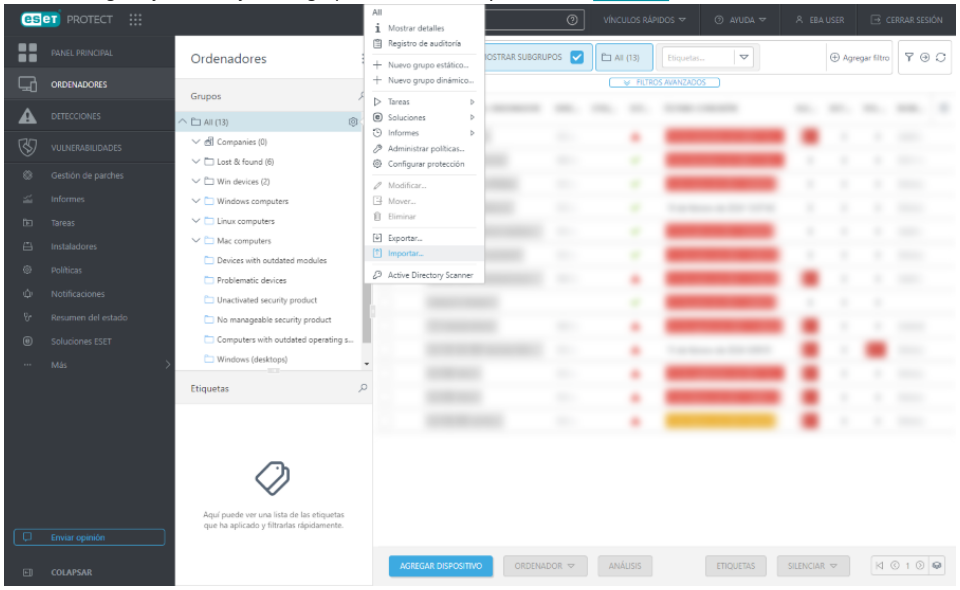
1. Exporte la lista de ordenadores desde Active Directory. Puede utilizar varias herramientas, en función del modo de administración de Active Directory. Por ejemplo, abra **Usuarios y ordenadores** de **Active Directory** y, en su dominio, haga clic con el botón derecho del ratón en **Ordenadores** y seleccione **Exportar lista**.



2. Guarde la lista de ordenadores de Active Directory exportados como archivo *.txt*.
3. Modifique la lista de ordenadores para que su formato sea aceptable para la importación en ESET PROTECT. Asegúrese de que cada línea contenga un equipo y que posea el siguiente formato:

```
\GROUP\SUBGROUP\Computer name
```

4. Guarde el archivo *.txt* actualizado con la lista de ordenadores.
5. Importe la lista de ordenadores de Active Directory en ESET PROTECT Web Console. Haga clic en **Ordenadores** > haga clic en el icono del engranaje situado junto al grupo estático **Todos** y seleccione **Importar**.



Implementar ESET Management Agent en los ordenadores de Active Directory mediante un objeto de política de grupo

1. Cree el script de implementación GPO del agente.
2. Implemente ESET Management Agente mediante un objeto de política de grupo (GPO): comience por el paso 3 del artículo de la base de conocimiento. .
3. Una vez implementado ESET Management Agent correctamente mediante GPO, ESET Management Agent se instalará en los ordenadores de Active Directory y los ordenadores aparecerán en la pantalla **Ordenadores** de ESET PROTECT Web Console. Cuando agregue un nuevo ordenador a Active Directory en el futuro, aparecerá en la pantalla **Ordenadores** de ESET PROTECT Web Console.

Cómo administrar productos Endpoint desde ESET PROTECT

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 PROTECTAsistente 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 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 Business Account 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** > **Activar producto de seguridad** para activar 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

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. 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

Todos los ordenadores cliente se conectan a ESET PROTECT a través de ESET Management Agent. El agente comunica toda la información solicitada sobre el ordenador cliente y su software a ESET PROTECT Server. 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, 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 si ESET PROTECT tiene una notificación para el cliente. La conexión está establecida de modo que ESET PROTECT 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.

Detalles de conexión

Para configurar su red local de modo que permita la comunicación con EPNS, las instancias de ESET Management Agent 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).

VDI, clonación y detección de hardware

ESET PROTECT 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, 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 Cloud 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; esto sucede cuando ESET PROTECT 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 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, 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).

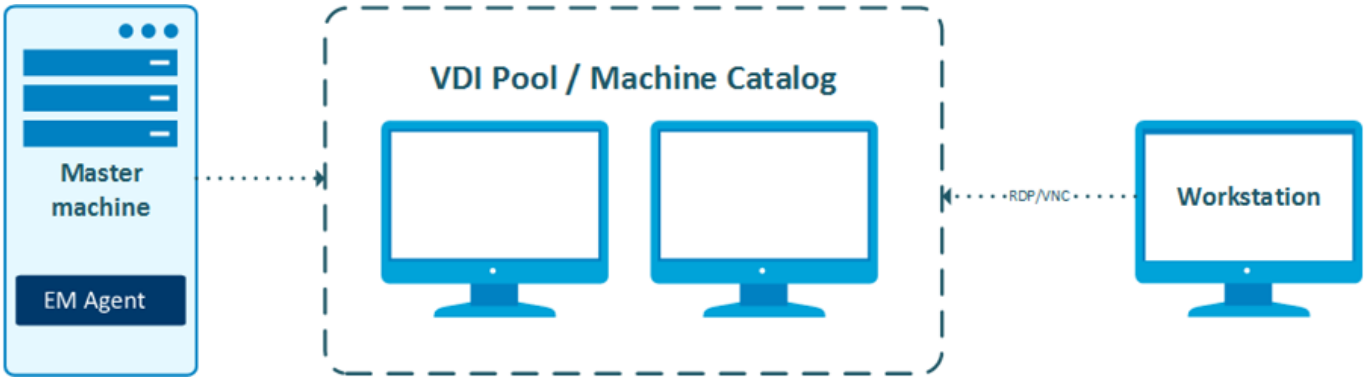
- Cuando un equipo del grupo VDI se conecta por primera vez, tiene un intervalo de conexión obligatorio de 1 minuto. Tras las primeras replicaciones, el intervalo de conexión se hereda del equipo principal.

- 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.

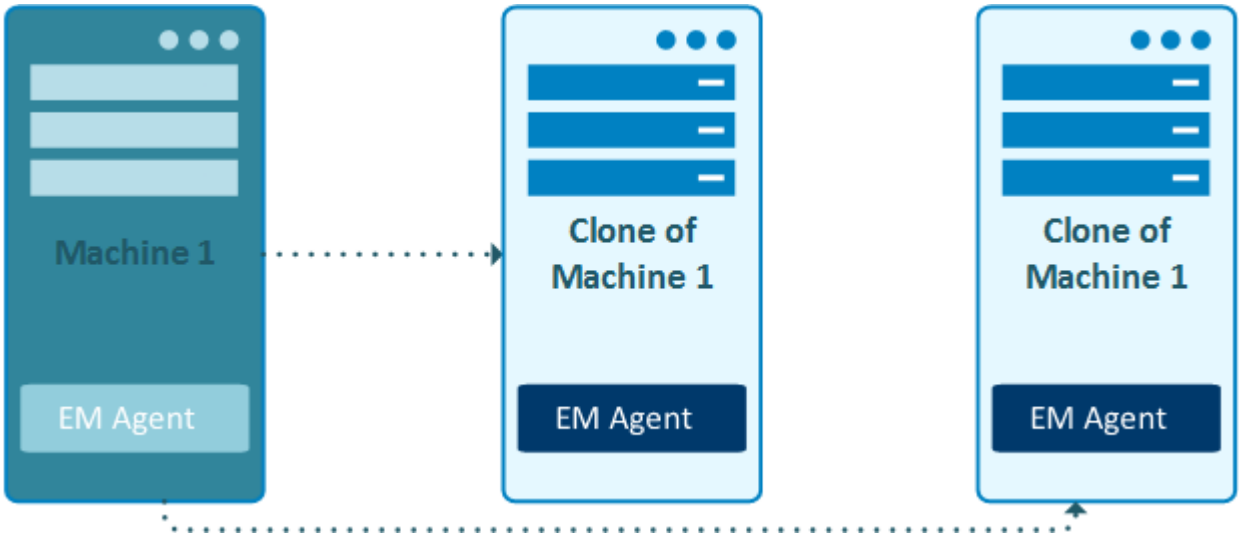
Grupo predeterminado para máquinas de infraestructura de escritorios virtuales

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 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**.

oAutomáticamente: marque el equipo maestro antes de la clonación y seleccione **Marcar como maestro para clonación** > **Crear nuevos ordenadores**.

Relacionar con ordenador existente

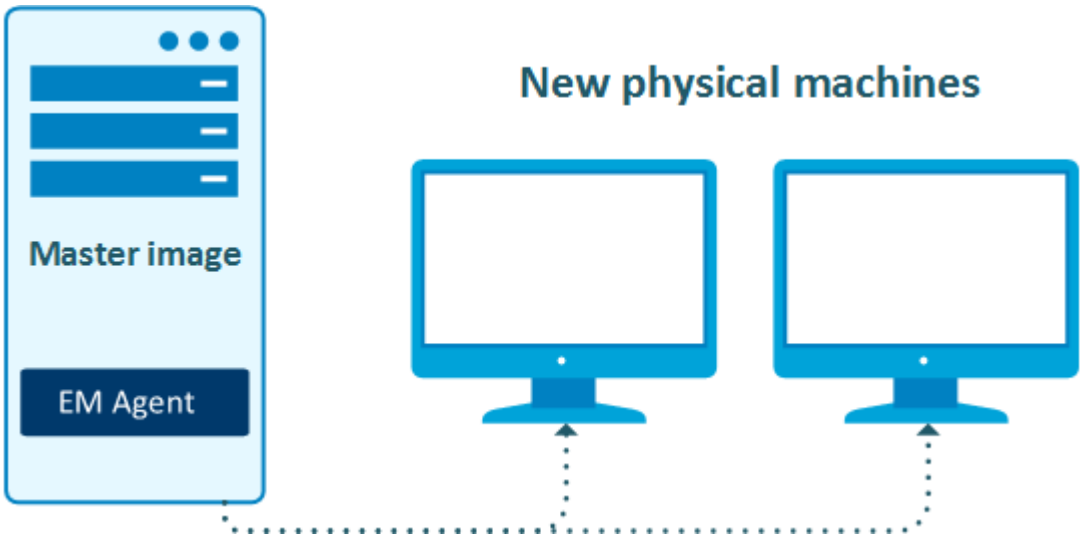
Si la imagen vuelve a implementarse en un equipo con historial previo en ESET PROTECT (que ya tenía ESET Management Agent implementado), este equipo se conecta con su identidad anterior en ESET PROTECT. Si no hay ninguna identidad anterior relacionada, el sistema crea un nuevo equipo en ESET PROTECT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

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

oManualmente: resuelva cada nuevo ordenador manualmente en Preguntas y seleccione **Relacionar con un ordenador existente cada vez**.

oAutomáticamente: 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. 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 preguntas de clonación

Cada vez que un equipo se conecta con ESET PROTECT, 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

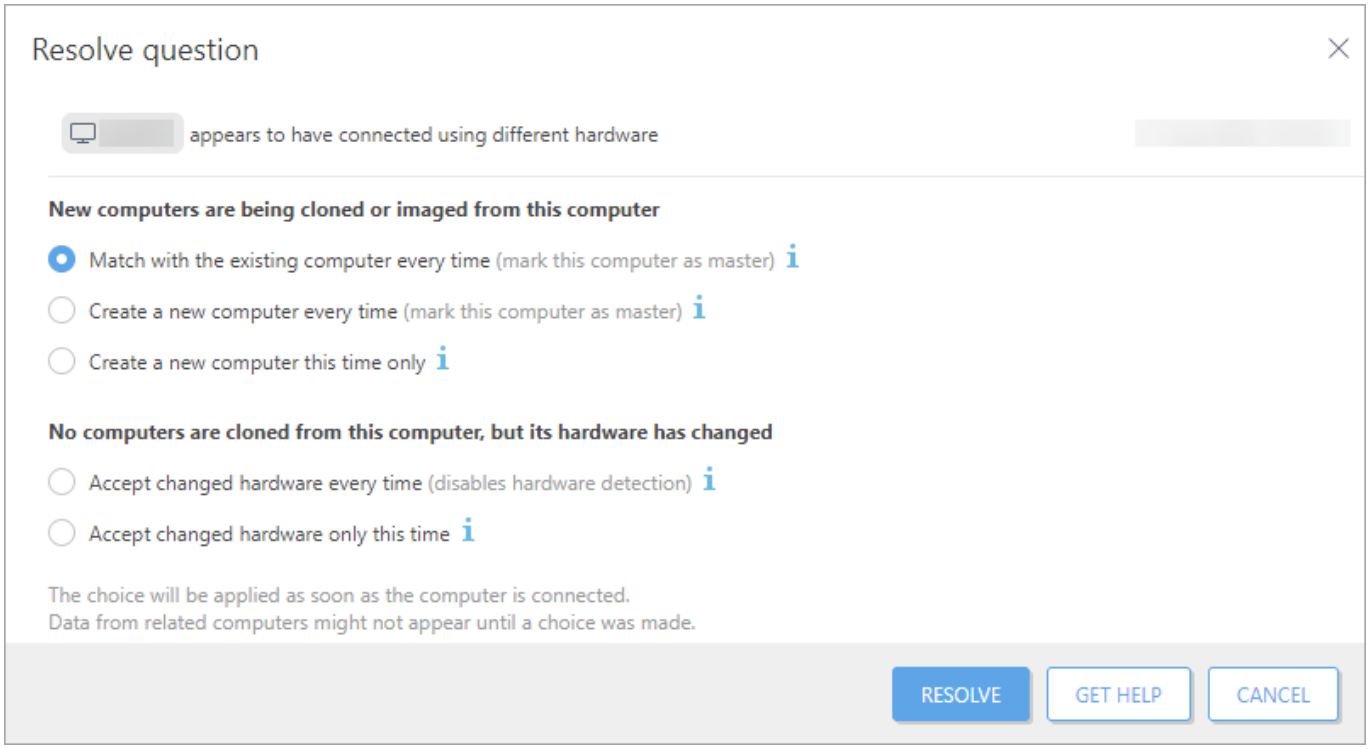
La detección de huella digital de hardware no es compatible con:
- Linux, macOS, Android, iOS
- equipos sin ESET Management Agent

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. • 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 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.
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.



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 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.

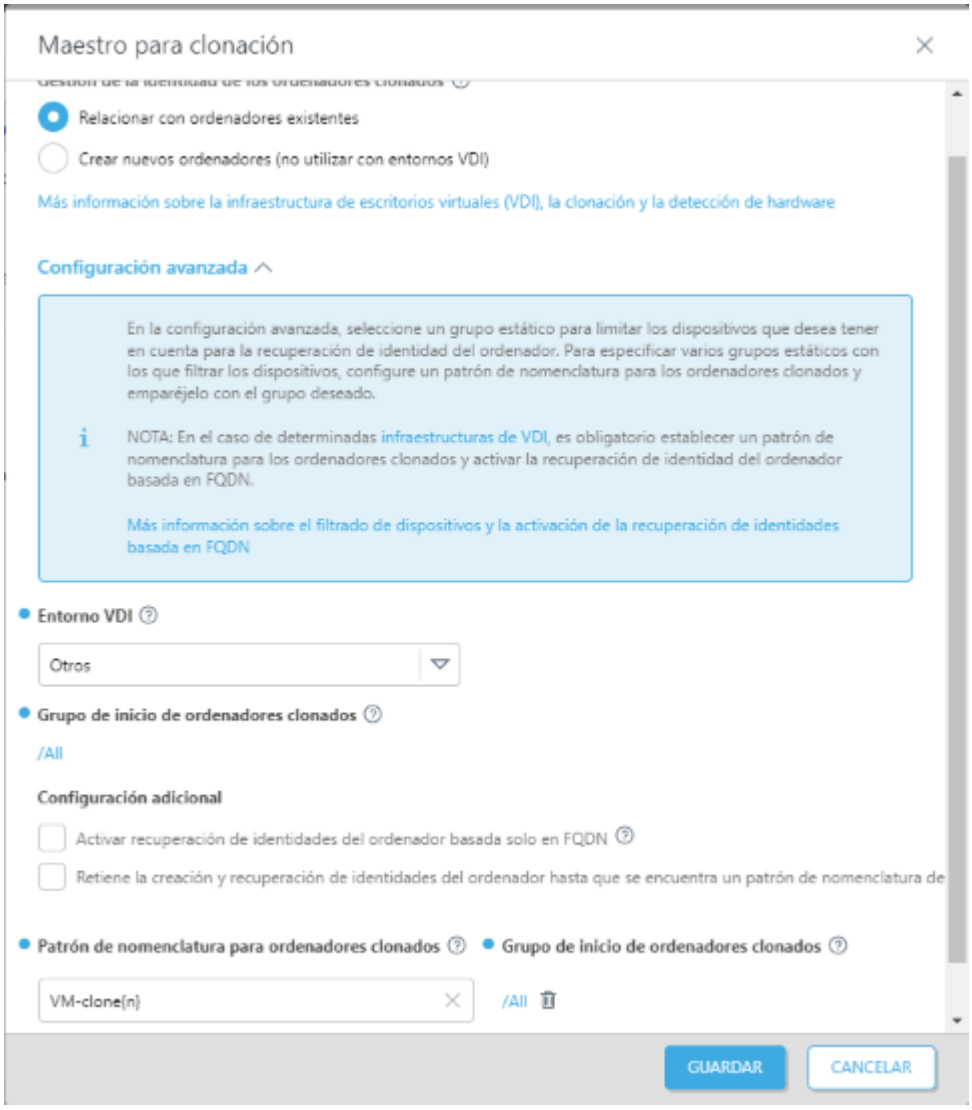
Identificación de hardware

ESET PROTECT recopila detalles sobre el hardware de cada dispositivo administrado e intenta identificarlo. Cada dispositivo conectado a ESET PROTECT 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 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 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**.

ESET BridgeProxy HTTP -

Puede utilizar ESET Bridge con ESET PROTECT como servicio proxy para:

- Descarga y almacena en caché: actualizaciones de los módulos de ESET, paquetes de instalación y actualización enviados por ESET PROTECT (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.

Lea la ayuda en línea de ESET Bridge para obtener más información sobre la instalación y la configuración de ESET Bridge.

Apache HTTP Proxy usuarios
A partir de ESET PROTECT 4.0 (publicado en noviembre de 2022), ESET Bridge reemplaza Apache HTTP Proxy. Apache HTTP Proxy ha alcanzado el soporte limitado. Si utiliza Apache HTTP Proxy, le recomendamos migrar a ESET Bridge.

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.

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.

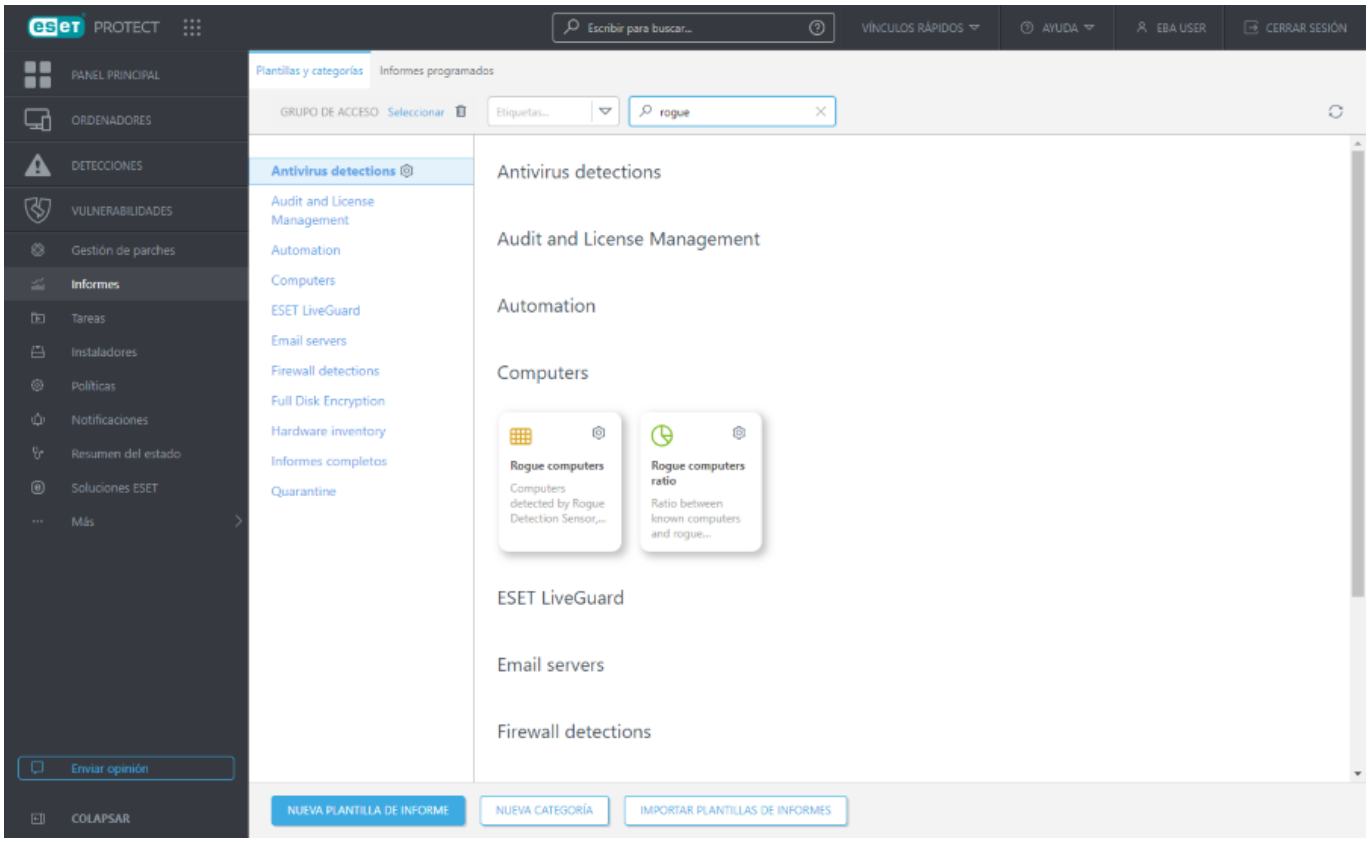
Le recomendamos que utilice la implementación local solo si tiene una red pequeña (hasta 50 ordenadores). Si la red es mayor, puede implementar ESET Management Agent mediante el uso de GPO o SCCM.

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

Agregar ordenadores con RD Sensor

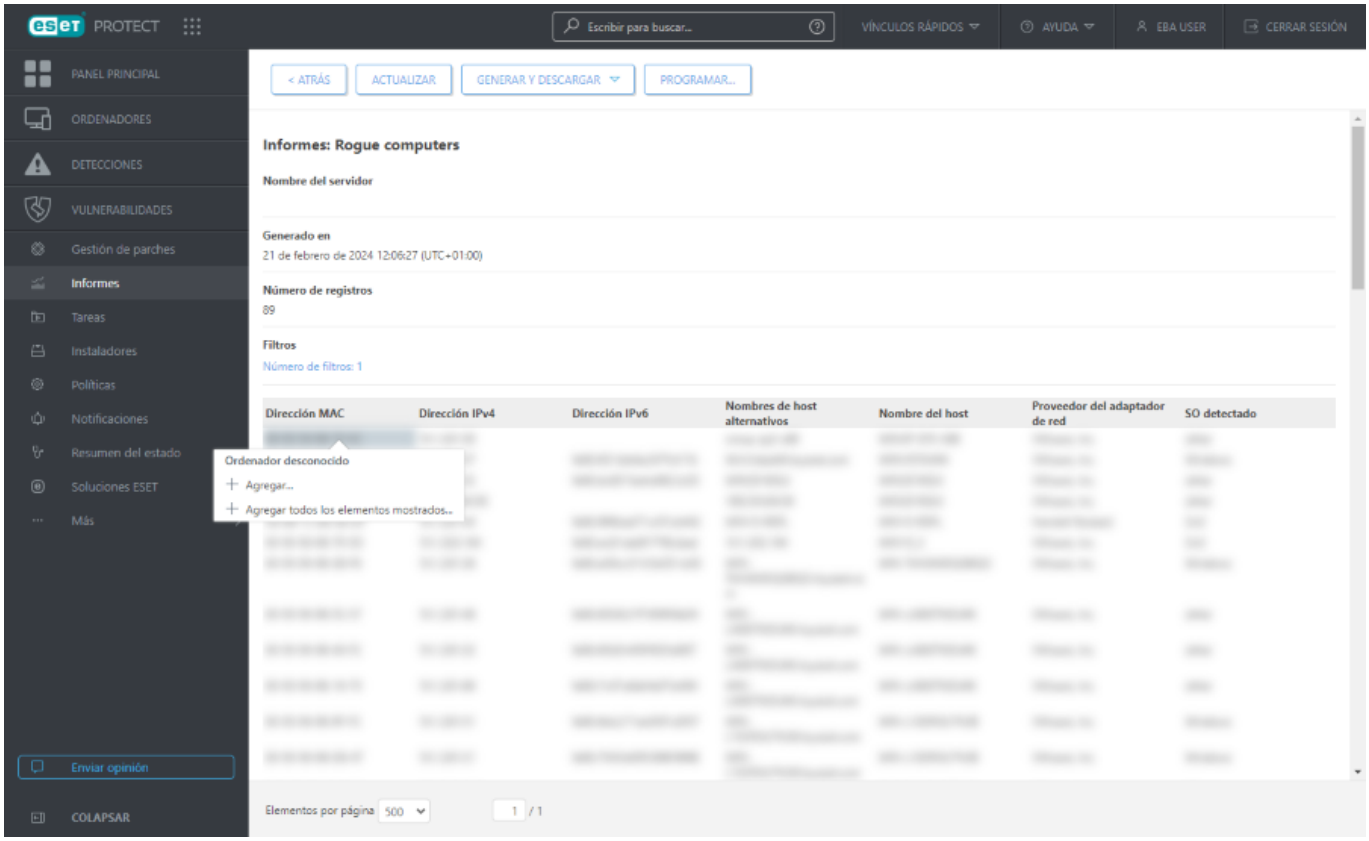
La forma más fácil de encontrar un ordenador no administrado en la estructura de su red es utilizar RD Sensor. RD Sensor supervisa la red en la que se implementa y, cuando se conecta a la red un nuevo dispositivo sin agente, envía esta información a ESET PROTECT. El componente RD Sensor no se puede implementar con Live Installer. Para implementar RD Sensor en su red, siga los pasos de instalación de RD Sensor.

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 detectados por RD Sensor a ESET PROTECT, descargue el informe en formato *.csv* y utilice esta lista en la Herramienta de implementación en la opción Importar lista de ordenadores.



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

Instalación de RD Sensor

Puede instalar ESET Rogue Detection Sensor en Windows o Linux.

Requisitos previos

- Solo Windows: WinPcap: utilice la versión más reciente de WinPcap (4.1.0 y posteriores).

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

- La instancia de ESET PROTECT es accesible

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

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

Instalación en Windows

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

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

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

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

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

4. 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).

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

6. ESET Rogue Detection Sensor se iniciará una vez finalizado el proceso de instalación.

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

Instalación en Linux

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

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

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (*rdsensor-linux-i386.sh* o *rdsensor-linux-x86_64.sh*).

2. Configure el archivo de instalación de RD Sensor como un ejecutable: `chmod +x rdsensor-linux-x86_64.sh`

3. Utilice el siguiente comando para ejecutar el archivo de instalación como sudo:

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

4. Lea el Acuerdo de licencia para el usuario final. Use la **barra espaciadora** para ir a la siguiente página del Acuerdo de licencia para el usuario final.
El instalador le preguntará si acepta el acuerdo. Pulse **Y** en el teclado si la acepta. De lo contrario, pulse **N**.

5. Pulse **Y** si desea participar en el programa de mejora del producto. De lo contrario, pulse **N**.

6. ESET Rogue Detection Sensor se iniciará una vez finalizado el proceso de instalación.

7. Para ver si la instalación se ha realizado correctamente, compruebe que el servicio está en funcionamiento ejecutando el siguiente comando:

```
sudo systemctl status rdsensor
```

Puede encontrar el archivo de registro de Rogue Detection Sensor aquí:
/var/log/eset/RogueDetectionSensor/trace.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.

Vaya a la sección Instaladores y seleccione el paquete del instalador que desee.

La implementación local se puede realizar de las siguientes formas:

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

ESET Management Agent está preconfigurado para conectarse correctamente con ESET PROTECT, por lo que solo se puede realizar un número limitado de modificaciones en la configuración de ESET Management Agent a través de la política de ESET Management Agent.

Crear Live Installer - Agent y productos de seguridad de ESET (Windows/macOS).

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

- **Vínculos rápidos** > **Dispositivos Windows** o **dispositivos macOS**
- **Instaladores** > **Crear instalador** > **Windows** o **macOS**
- Recorrido por ESET PROTECT

1. **Configuración de protección e instalación** – Marque la casilla de verificación situada junto al ajuste para

activarlo para el instalador:

- Windows solo:

  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.

- 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. 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.

3. Haga clic en **Descargar** para descargar el paquete del instalador o seleccione otras opciones de distribución del paquete del instalador.

Haga clic en **Personalizar instalador** para personalizar el paquete del instalador:

4. **Distribución**: seleccione **Descargar o enviar el instalador, o utilizar ESET Remote Deployment Tool** (Windows) o **Descargar o enviar instalador** (macOS).

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

5. **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. No puede cancelar la selección del producto de seguridad de ESET en un instalador de macOS.

- Windows solo: **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.

- Windows solo: **ESET Inspect Connector**: incluya ESET Inspect Connector en el instalador. Esta opción solo se muestra si la licencia de ESET Inspect 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.

6. 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).

7. **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.

8. 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.

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

10. 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.
b. Windows solo: 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**).
o**Configuración** También puede seleccionar una **política** para que se aplique al producto de seguridad de ESET durante la instalación.
o Windows solo: **Ejecutar ESET AV Remover**: marque la casilla de verificación para desinstalar o quitar por completo otros programas antivirus del dispositivo de destino.

Windows solo: 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**).

ESET Inspect Connector

Requisitos de ESET Inspect Connector:
- Debe tener una licencia de ESET Inspect 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**).

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.

11. Haga clic en **Finalizar**.

12. Puede distribuir el paquete de Live Installer de varias formas:

- Haga clic en para copiar el vínculo de descarga del paquete de Live Installer, distribuir el vínculo entre los usuarios y permitir que descarguen e instalen el paquete de Live Installer.

- También puede **Descargar** el paquete Live Installer y distribuirlo personalmente o cargarlo en una ubicación compartida para que accedan los usuarios.

- Solo Windows: Utilice la Remote Deployment Tool para implementar el paquete de Live Installer de forma remota.

- Haga clic en para usar el servidor SMTP de ESET PROTECT y enviar un mensaje de correo electrónico con el vínculo de descarga del paquete de Live Installer a los usuarios especificados.

  oPara agregar un usuario, haga clic en **Agregar** > rellene el campo **Dirección de correo electrónico** > pulse **Entrar** o haga clic en . Si lo desea, haga clic en **Crear usuario,** > escriba el **nombre** del usuario > haga clic en **Guardar**. Puede editar los detalles del usuario en Usuarios del ordenador. Haga clic en **Ver vista previa de mensaje de correo electrónico**, seleccione el **idioma del correo electrónico** en el menú desplegable y haga clic en **Guardar**.

  oPara 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).

Tras la creación, Live Installer se comportará como se muestra en esta tabla.
Live Installer requiere una conexión a Internet, y no funciona en un ordenador sin conexión.
Live Installer en macOS requiere una conexión a Internet directa (para conectarse a los servidores de ESET), y no funciona en un ordenador macOS conectado a Internet mediante proxy sin conexión a Internet directa.

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

13. Ejecute el archivo del paquete de instalación en un ordenador cliente. El paquete de Live Installer descargará ESET Management Agent y el producto de seguridad de ESET compatible con la plataforma del sistema operativo del ordenador (x86, x64, ARM64). Instalará ESET Management Agent y el producto de seguridad de ESET en el dispositivo y conectará a ESET PROTECT. El instalador de ESET Endpoint Antivirus/Security creado en ESET PROTECT es compatible con Windows 10 Enterprise para escritorios virtuales y el modo multisesión de Windows 10. Para obtener instrucciones detalladas, consulte la sección Asistente de instalación para Windows o macOS.

comportamiento Live Installer

Una vez creado Live Installer, se almacena en ESET PROTECT y se comportará como se describe en la tabla incluida a continuación.

Acción	Comportamiento del vínculo de descarga de Live Installer	Comportamiento de Live Installer descargado
Live Installer se elimina de ESET PROTECT.	El vínculo de descarga se desactiva.	Las copias de Live Installer descargadas antes de la eliminación dejan de funcionar.
Live Installer ya no está en el repositorio.	El vínculo de descarga se desactiva. Junto al instalador aparece el mensaje **El paquete seleccionado no está en el repositorio**.	Las copias de Live Installer descargadas antes de las ediciones dejan de funcionar.
Se editan políticas que forman parte de Live Installer.	El cambio de las políticas no se reflejará en las copias existentes de Live Installer y el vínculo de descarga ofrecerá el instalador con políticas definidas cuando se creó. Si quiere que los cambios se reflejen en el instalador, tendrá que crear un nuevo instalador con esta política actualizada.	El instalador funcionará, pero instalará su producto de ESET con políticas definidas cuando se creó.
Se eliminan políticas que forman parte de Live Installer.	Se mostrará la advertencia **No se puede acceder a la política indicada** junto al instalador y el vínculo de descarga se desactivará. Duplicar el instalador y asignarle una nueva política.	Las copias de Live Installer descargadas antes de la eliminación dejan de funcionar.
Se editan grupos que forman parte de Live Installer.		Este cambio no afectará a los instaladores existentes y el ordenador se asignará al grupo actualizado/movido cuando se conecte a ESET PROTECT.
Se eliminan grupos que forman parte de Live Installer.		El instalador se comportará como si no tuviera ningún grupo asignado. Se asignará al grupo **Perdidos y encontrados** predeterminado.

Acción	Comportamiento del vínculo de descarga de Live Installer	Comportamiento de Live Installer descargado
Live InstallerVida útil de	Los instaladores de Live Installer son válidos durante seis meses desde su creación. Para actualizar el vínculo de descarga de un instalador existente, vaya a **Instaladores**, seleccione el instalador existente y seleccione **Mostrar vínculo de descarga**. Descargue un instalador válido desde el nuevo vínculo de descarga.	

Crear instalador de script de agente: 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).

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

- **Vínculos rápidos** > **Dispositivos macOS** o **dispositivos Linux**
- **Instaladores** > **Crear instalador** > **macOS** o **Linux**
- Recorrido por ESET PROTECT

Haga clic en **Personalizar instalador** > **Implementar primero el agente (instalador de scripts del agente)**.

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. 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.

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

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

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

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

ESET PROTECT 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:
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 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`
- 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.

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

ESET PROTECT 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.

Se instalará una instancia de ESET Management Agent nativa de ARM64 (versión 9.1 y versiones posteriores) en los sistemas macOS ARM64.
ESET PROTECT 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.

Implementación remota

En implementaciones remotas, compruebe que todos los ordenadores cliente disponen de conexión a Internet.

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.

Si tiene problemas al implementar ESET Management Agent de forma remota, consulte Resolución de problemas - Conexión con el agente.

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.

> En implementaciones remotas, compruebe que todos los ordenadores cliente disponen de conexión a Internet.

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

1. Haga clic en **Windows** > **Personalizar instalador** > **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. 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.

5. Haga clic en **Finalizar**.

6. 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:

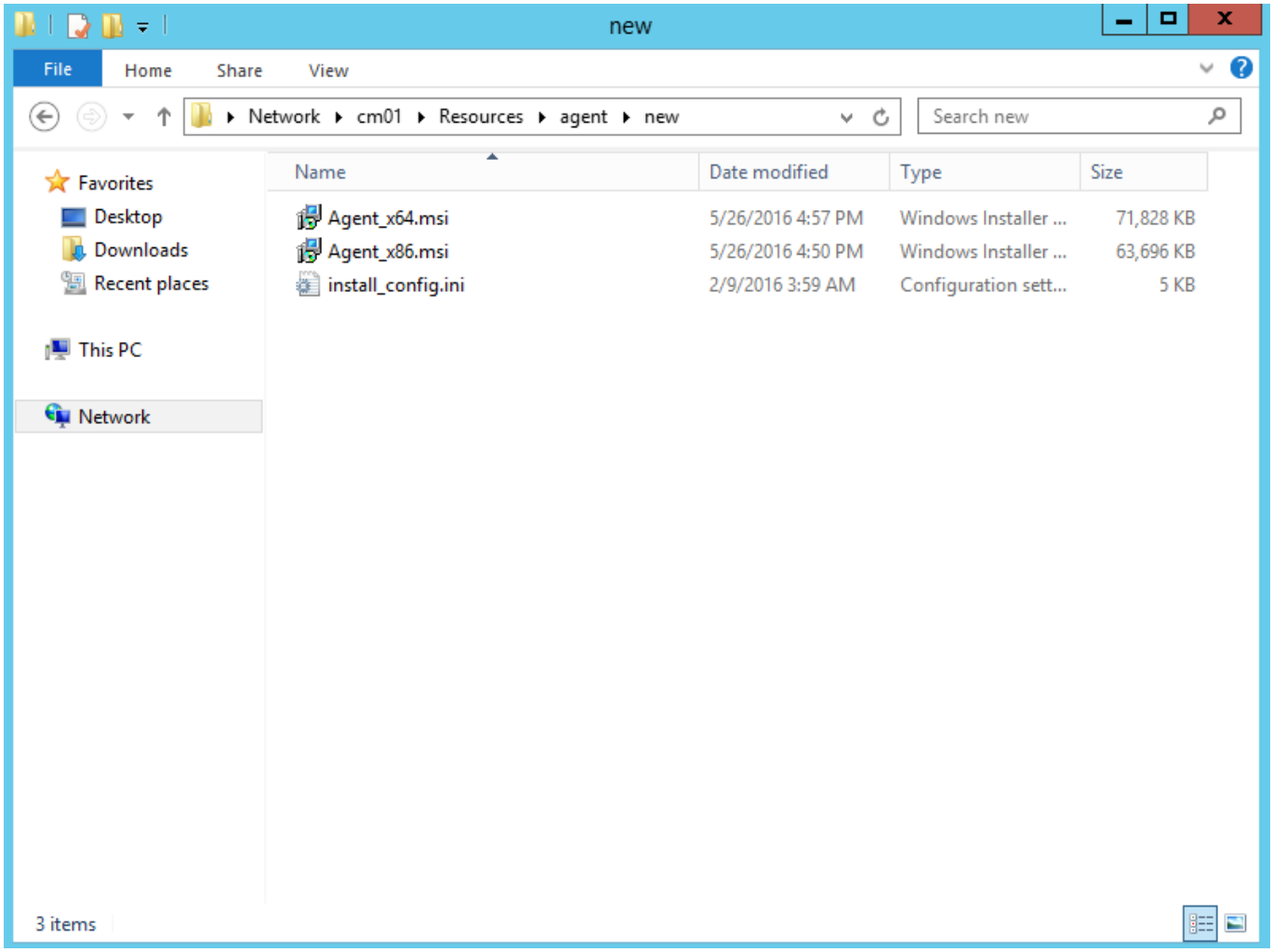
- Implementación de ESET Management Agent utilizando Objeto de política de grupo (GPO): este artículo de la Base de conocimiento puede no estar disponible en su idioma.

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

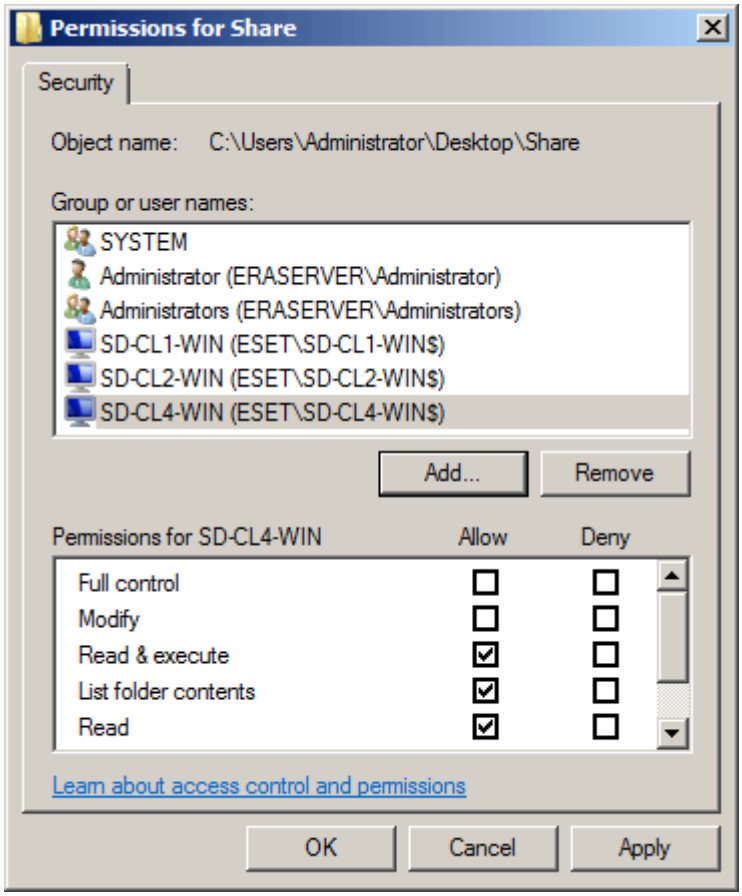
Pasos de implementación - SCCM

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

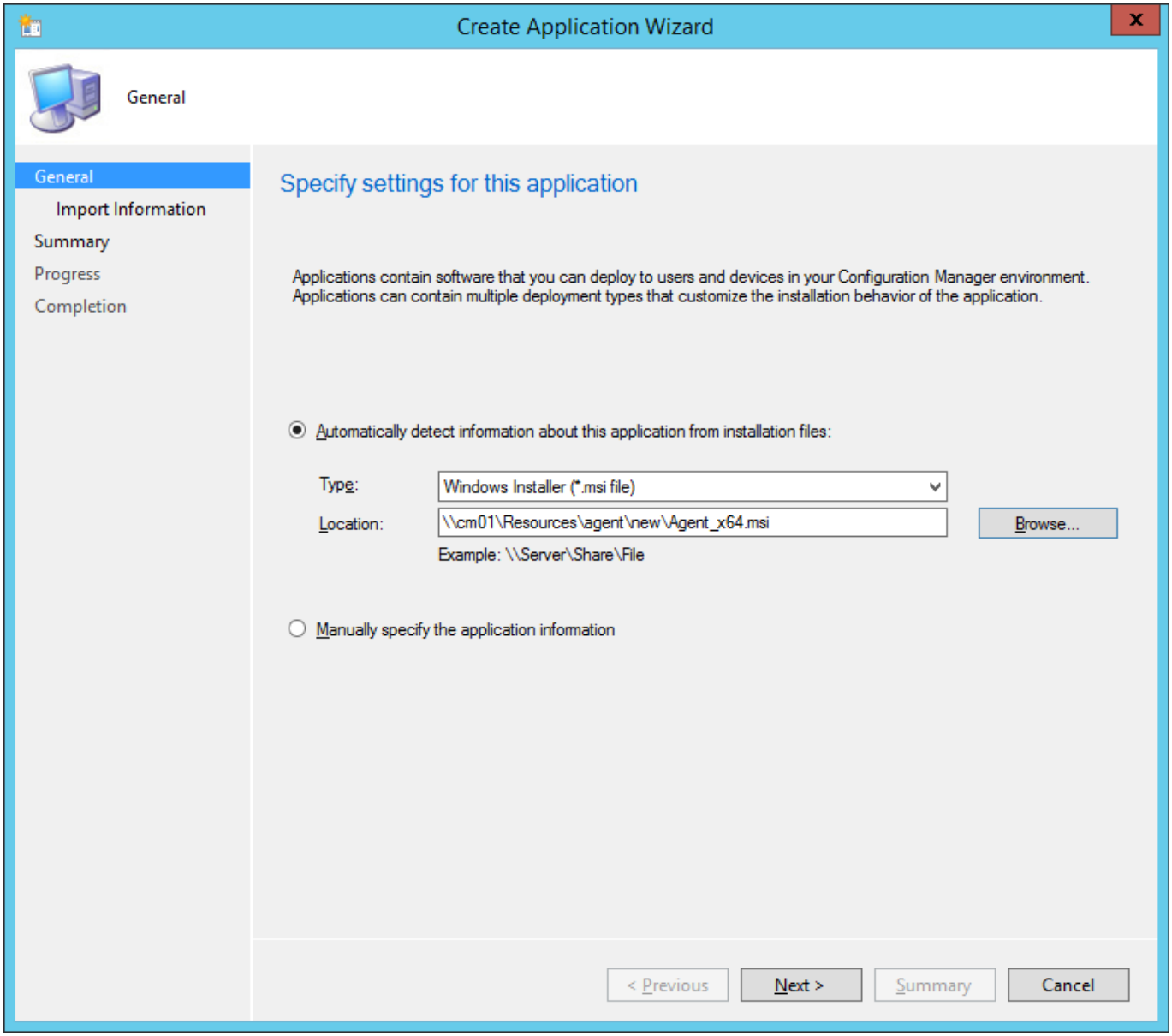
1. Coloque los archivos *.msi* del instalador de ESET Management Agent y el archivo *install_config.ini* en una carpeta compartida.



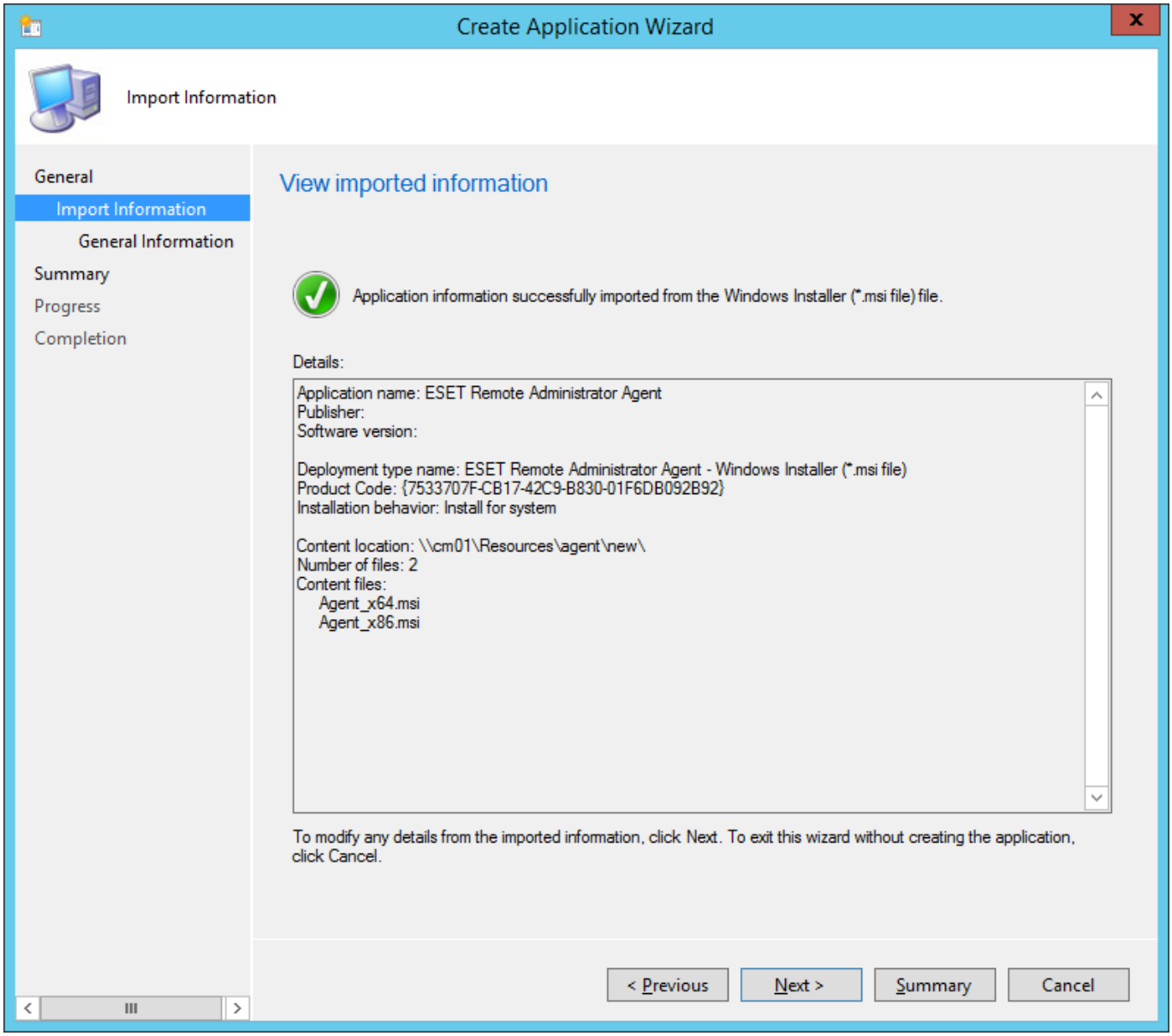
los ordenadores cliente necesitarán acceso de lectura o ejecución en esta carpeta compartida.



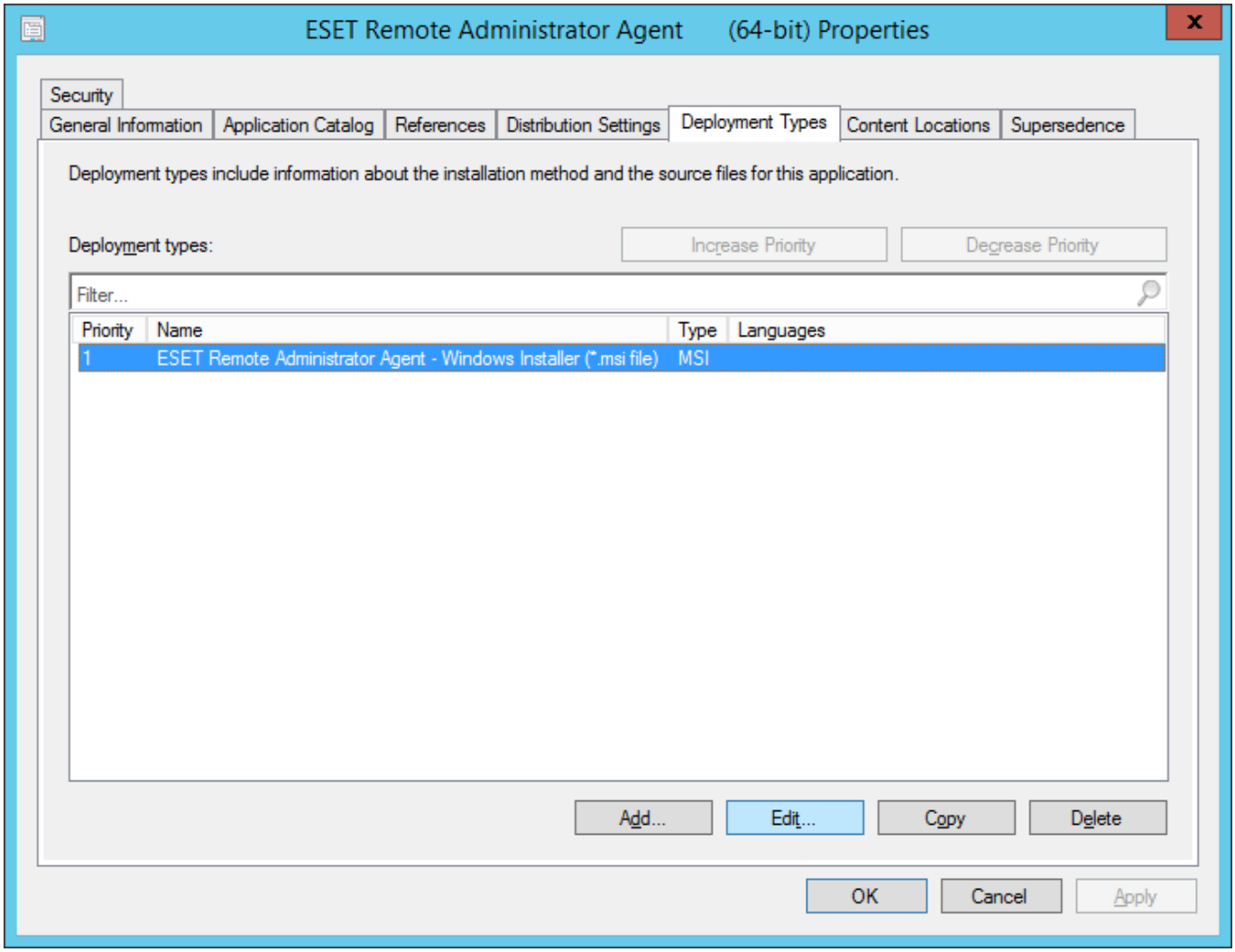
2. Abra la consola de SCCM y haga clic en **Biblioteca de software**. En **Gestión de aplicaciones** haga clic con el botón derecho en **Aplicaciones** y elija **Crear aplicación**. Elija **Instalador de Windows (archivo *.msi)**.



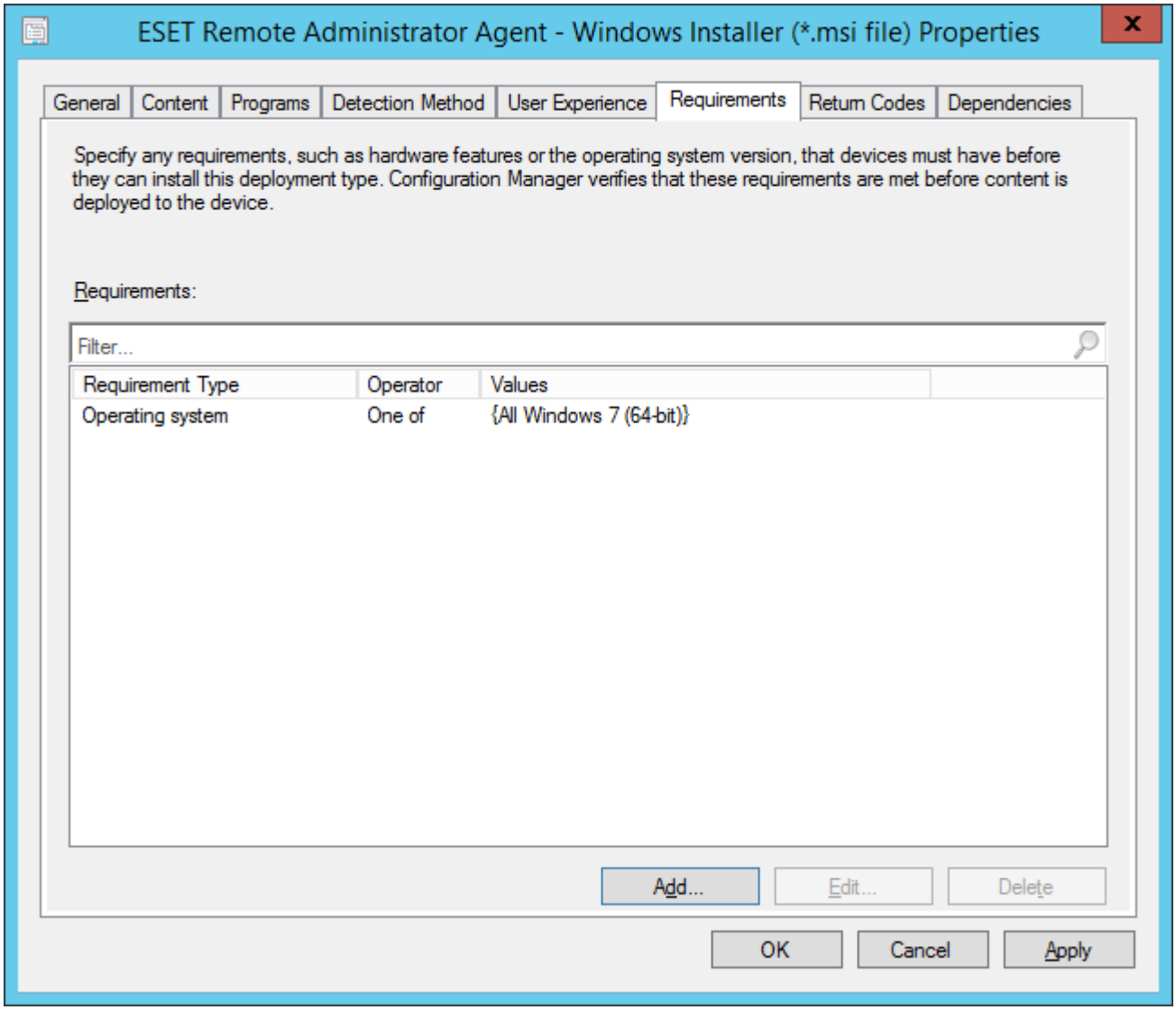
3. Especifique toda la información necesaria sobre la aplicación y haga clic en **Siguiente**.

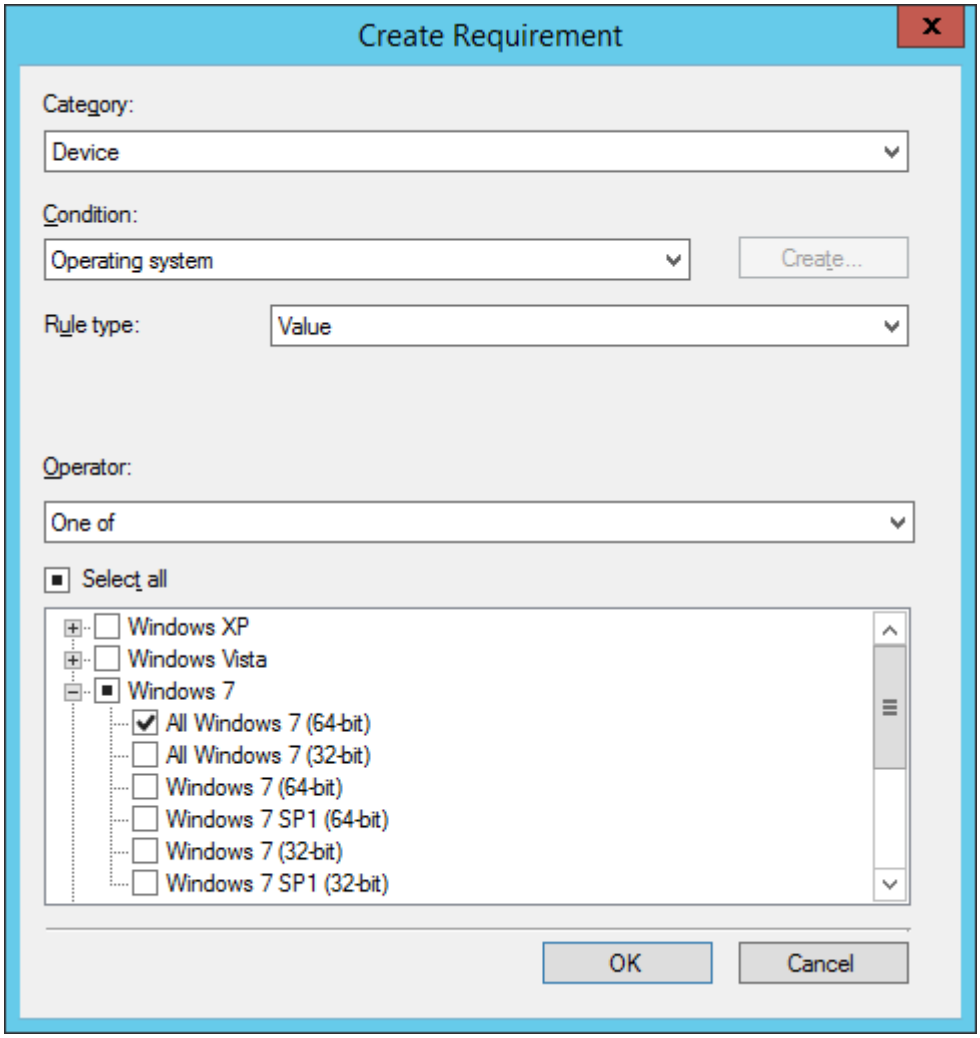


4. Haga clic con el botón derecho en la aplicación ESET Management Agent, haga clic en la ficha **Tipos de implementación**, seleccione la única implementación disponible y, a continuación, haga clic en **Edición**.

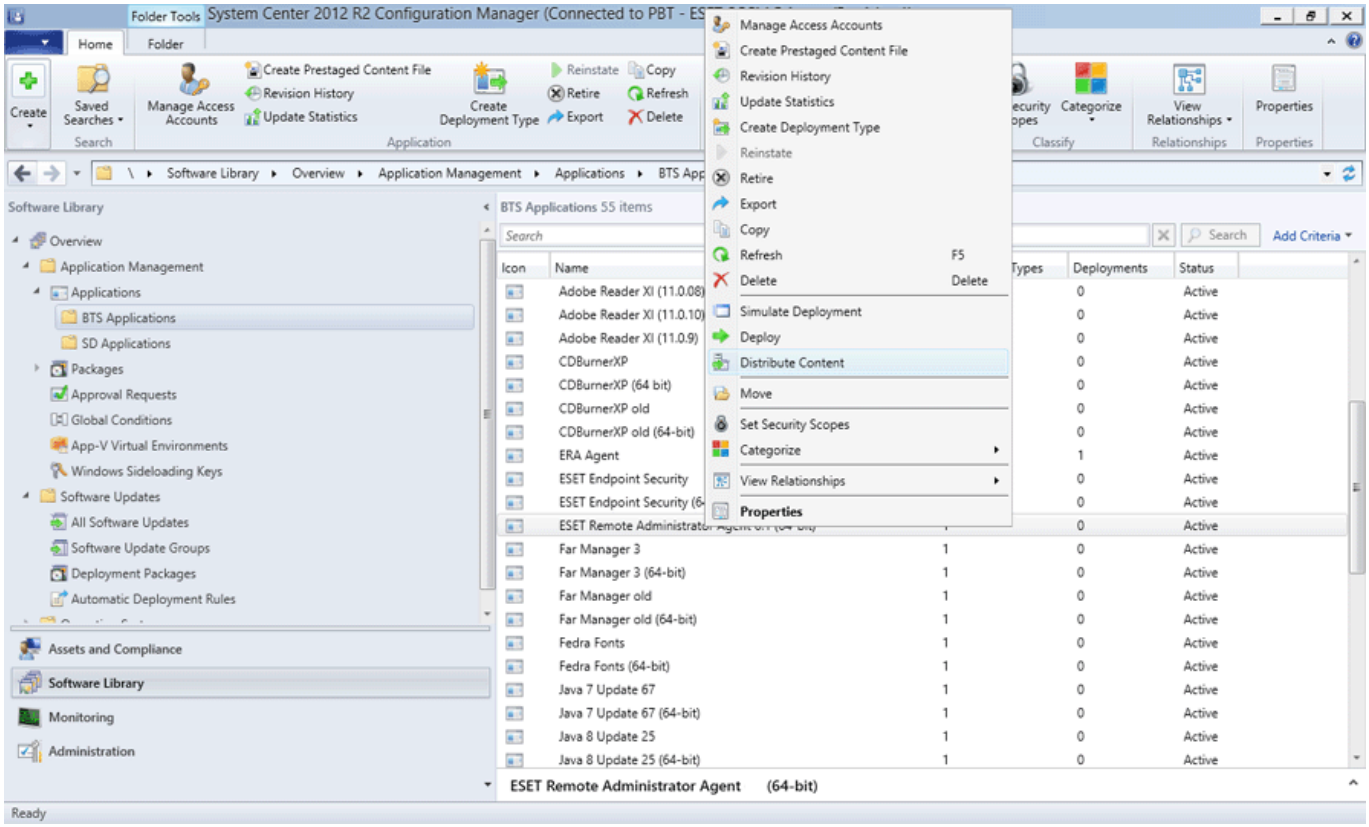


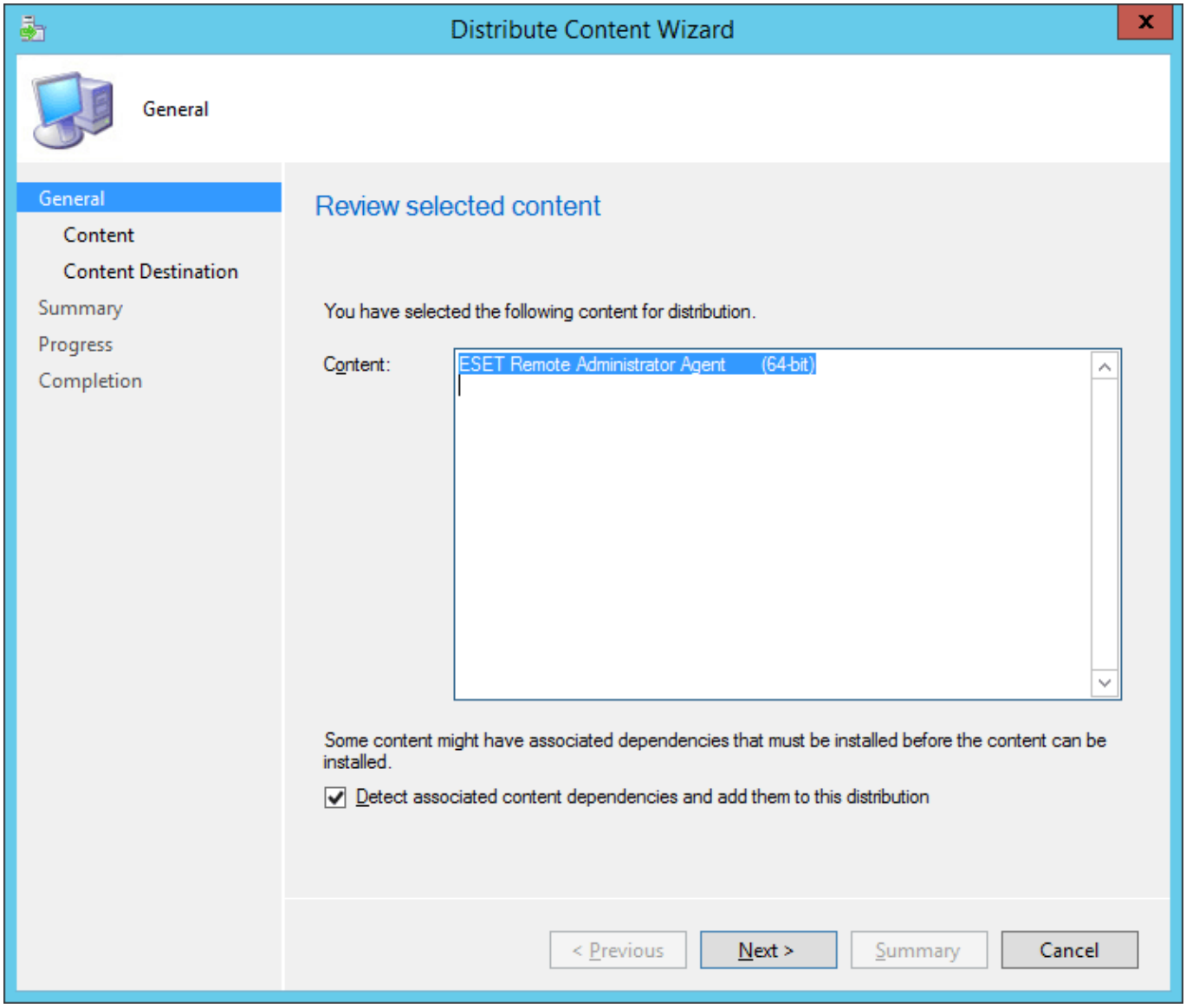
5. Haga clic en la ficha **Requisitos** y, a continuación, haga clic en **Agregar**. Seleccione **Sistema operativo** en el menú desplegable **Condición**, seleccione **Uno de** en el menú desplegable **Operador** y, a continuación, especifique los sistemas operativos en los que realizará la instalación 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.

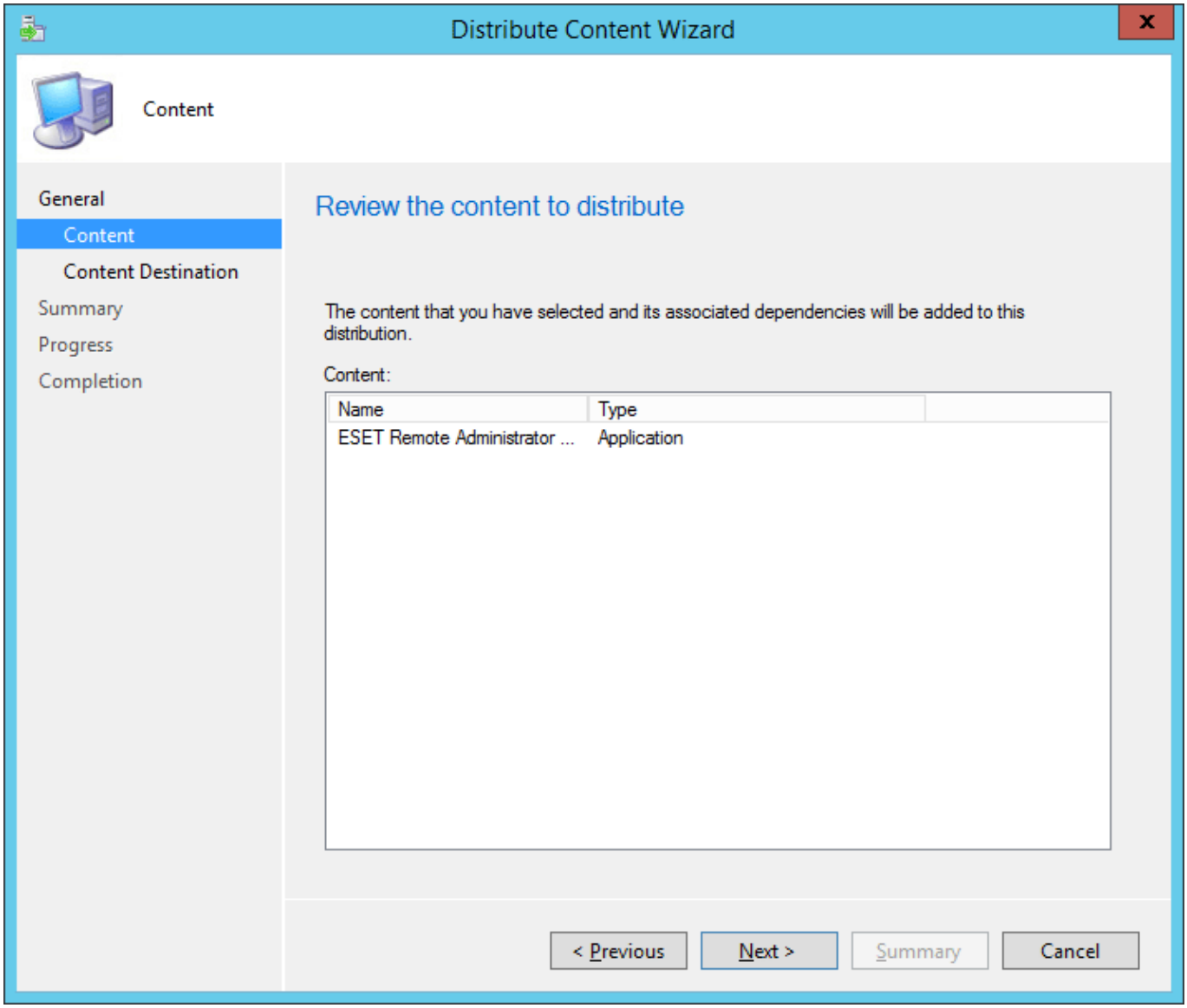

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install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



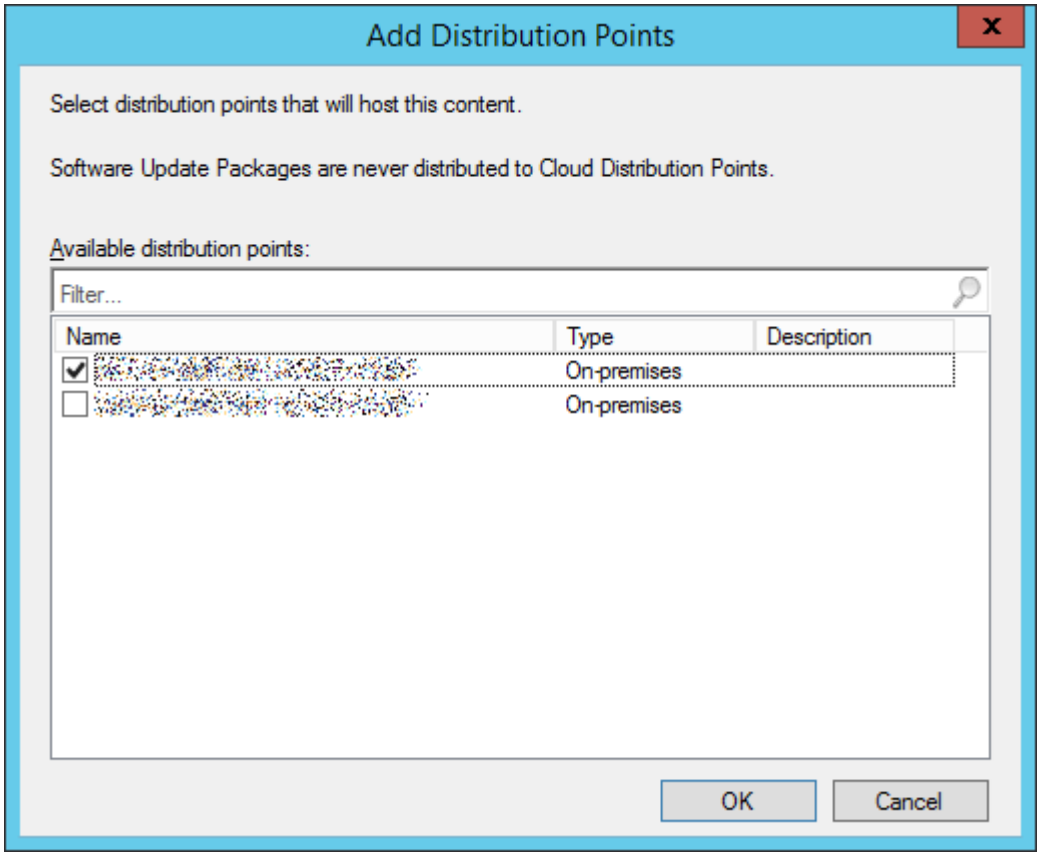
6. En la Biblioteca de software del centro del sistema, haga clic con el botón derecho en su nueva aplicación y seleccione **Distribuir contenido** en el menú contextual. Siga los mensajes del Asistente para la implementación de software para completar la implementación de la aplicación.

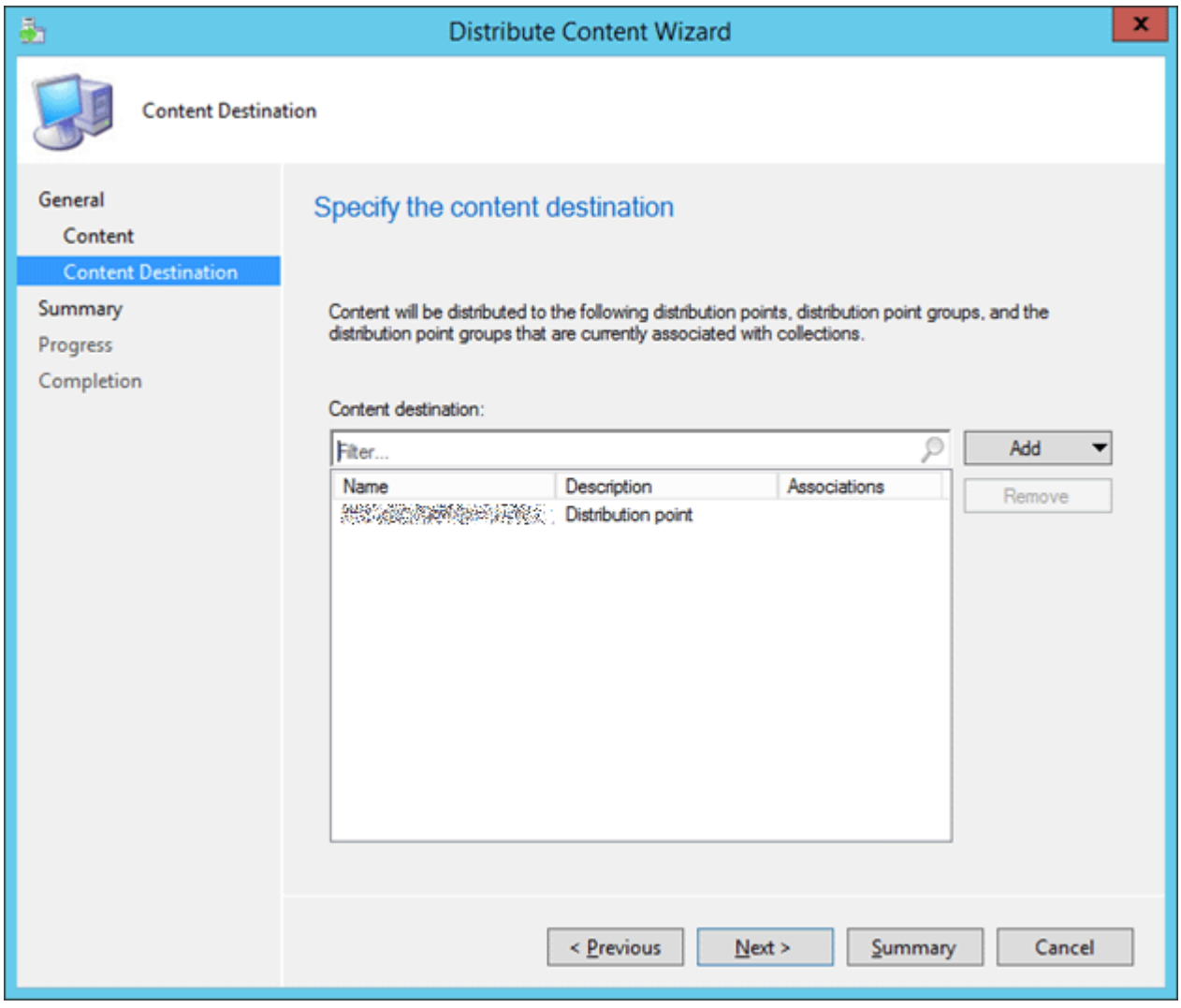

Folder Tools
System Center 2012 R2 Configuration Manager (Connected to PBT - ES
Home
Folder
Create
Saved Searches
Search
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Application
Categorize
Classify
View Relationships
Relationships
Properties
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)
Adobe Reader XI (11.0.10)
Adobe Reader XI (11.0.9)
CDBurnerXP
CDBurnerXP (64 bit)
CDBurnerXP old
CDBurnerXP old (64-bit)
ERA Agent
ESET Endpoint Security
ESET Endpoint Security (6
ESET Remote Administrator
Far Manager 3
Far Manager 3 (64-bit)
Far Manager old
Far Manager old (64-bit)
Fedra Fonts
Fedra Fonts (64-bit)
Java 7 Update 67
Java 7 Update 67 (64-bit)
Java 8 Update 25
Java 8 Update 25 (64-bit)
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

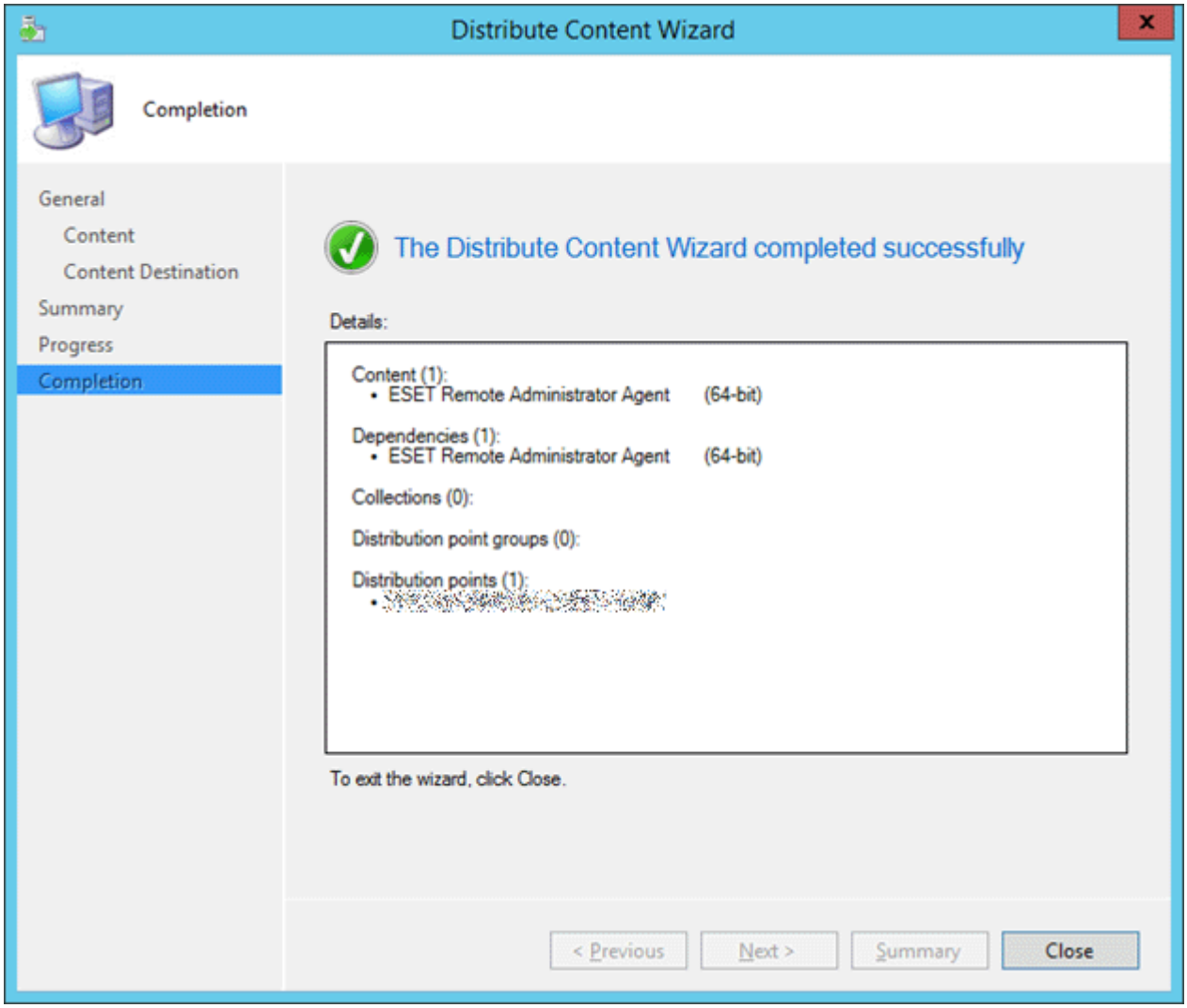

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed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

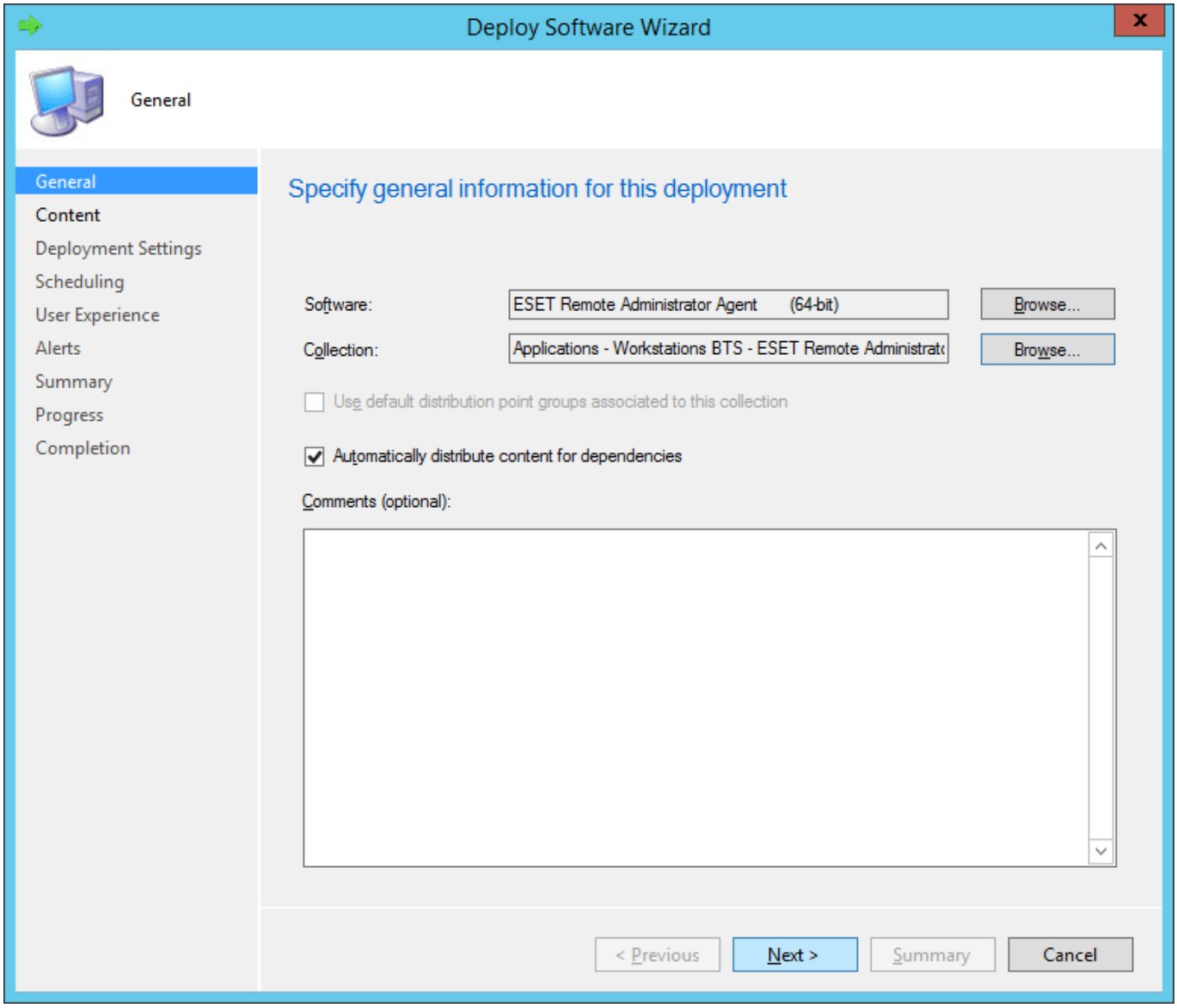


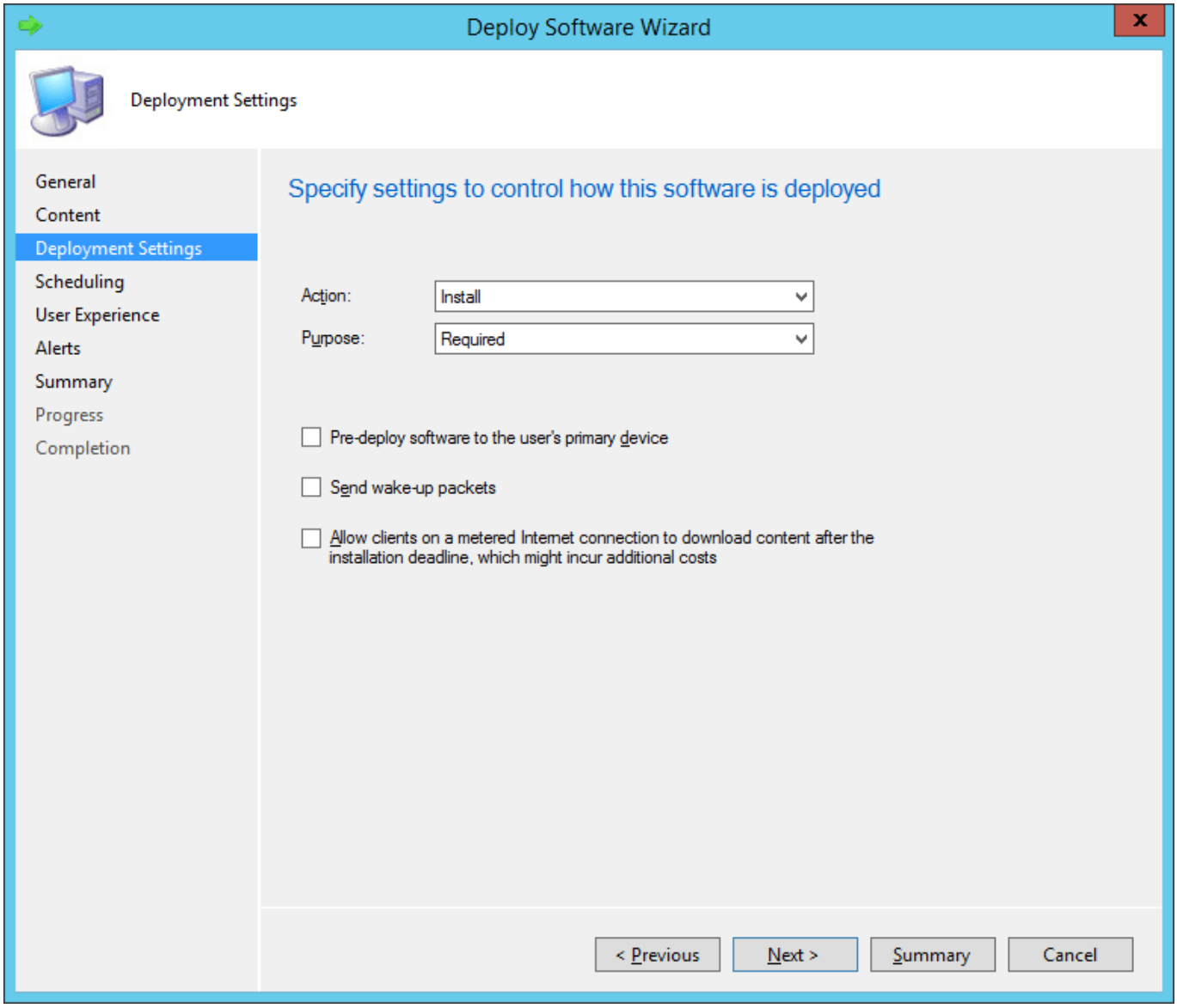
7. Haga clic con el botón derecho del ratón en la aplicación y elija **Implementar**. Siga el asistente y elija la colección y el destino en los que desea implementar el agente.

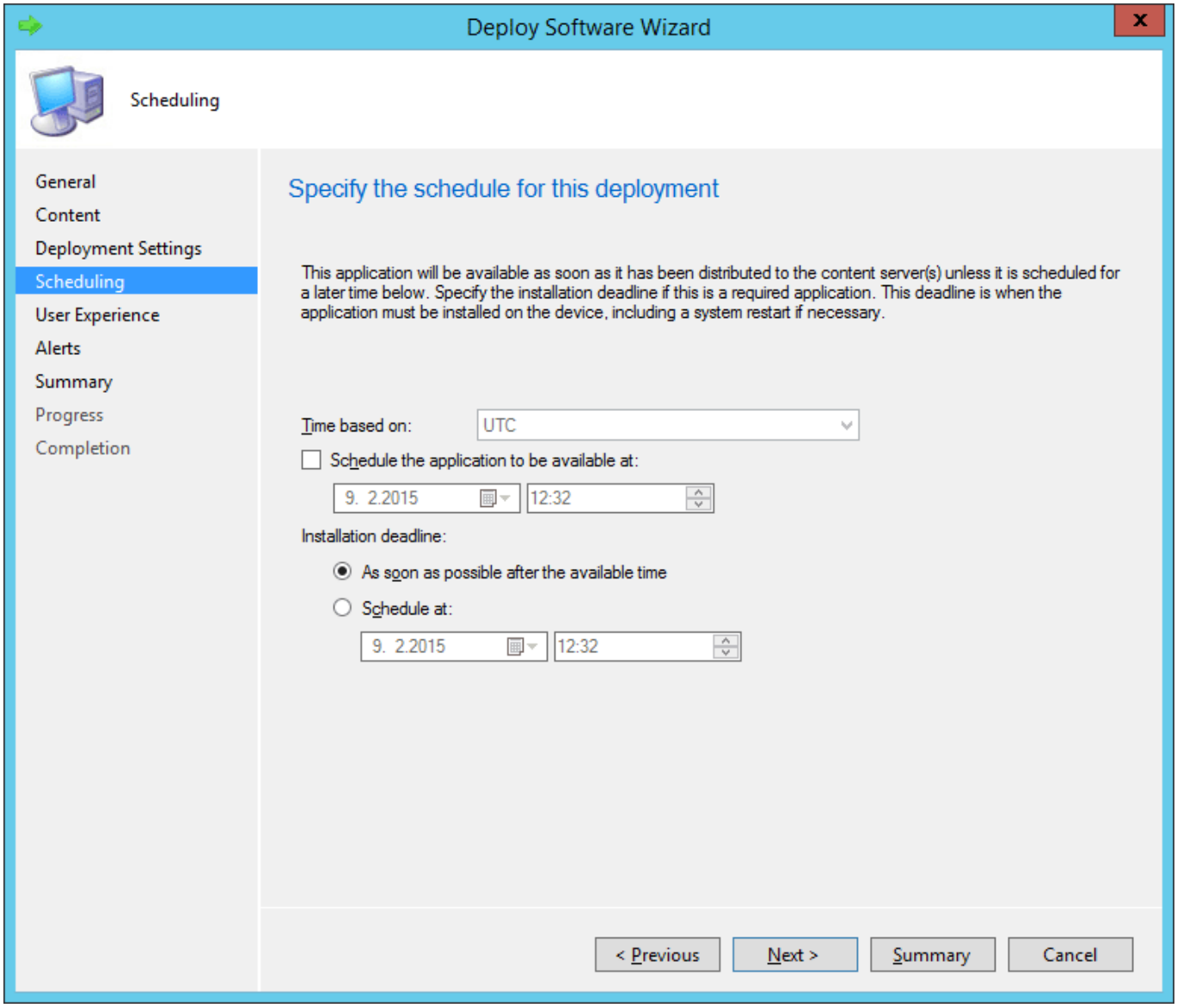

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

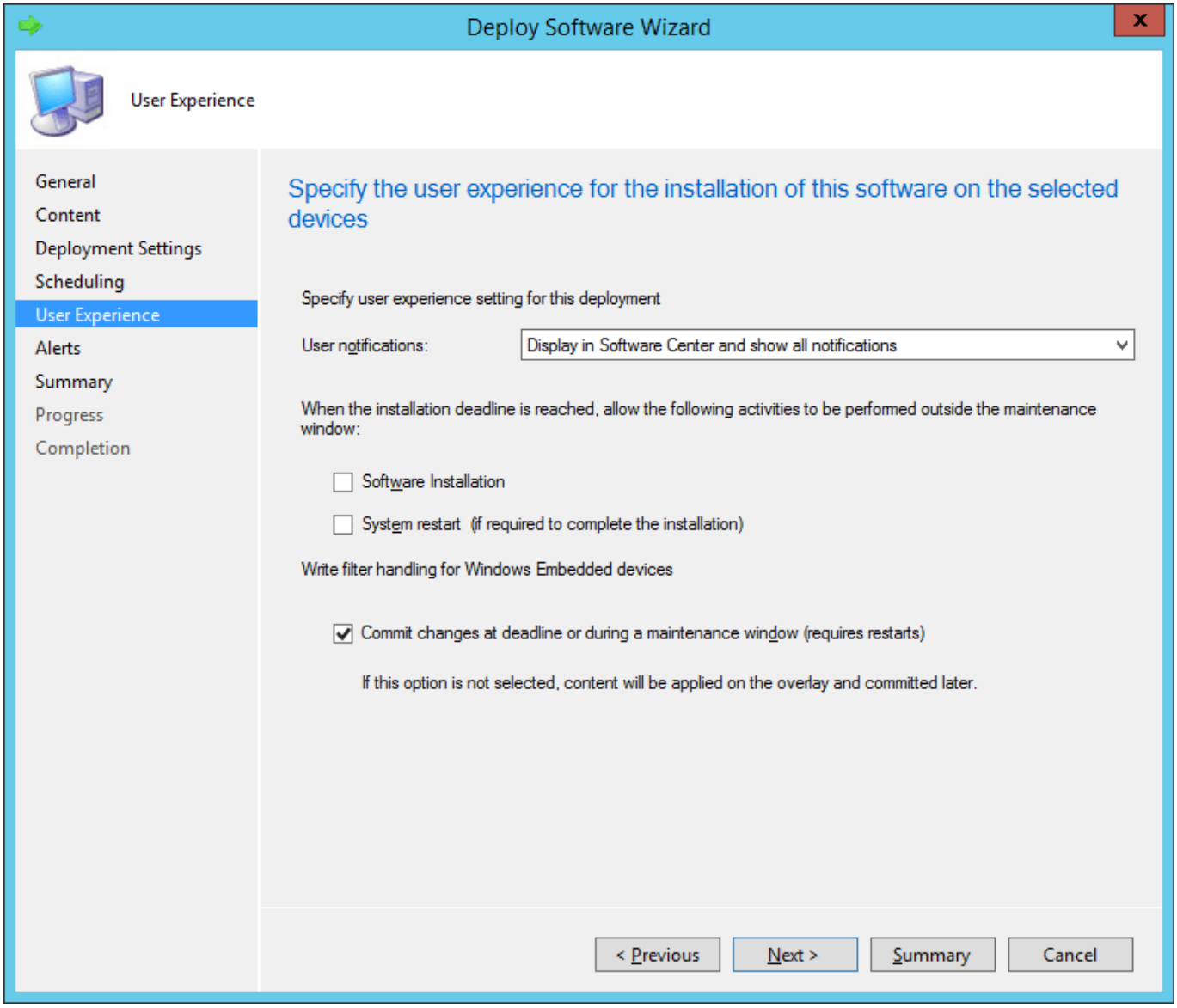

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with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

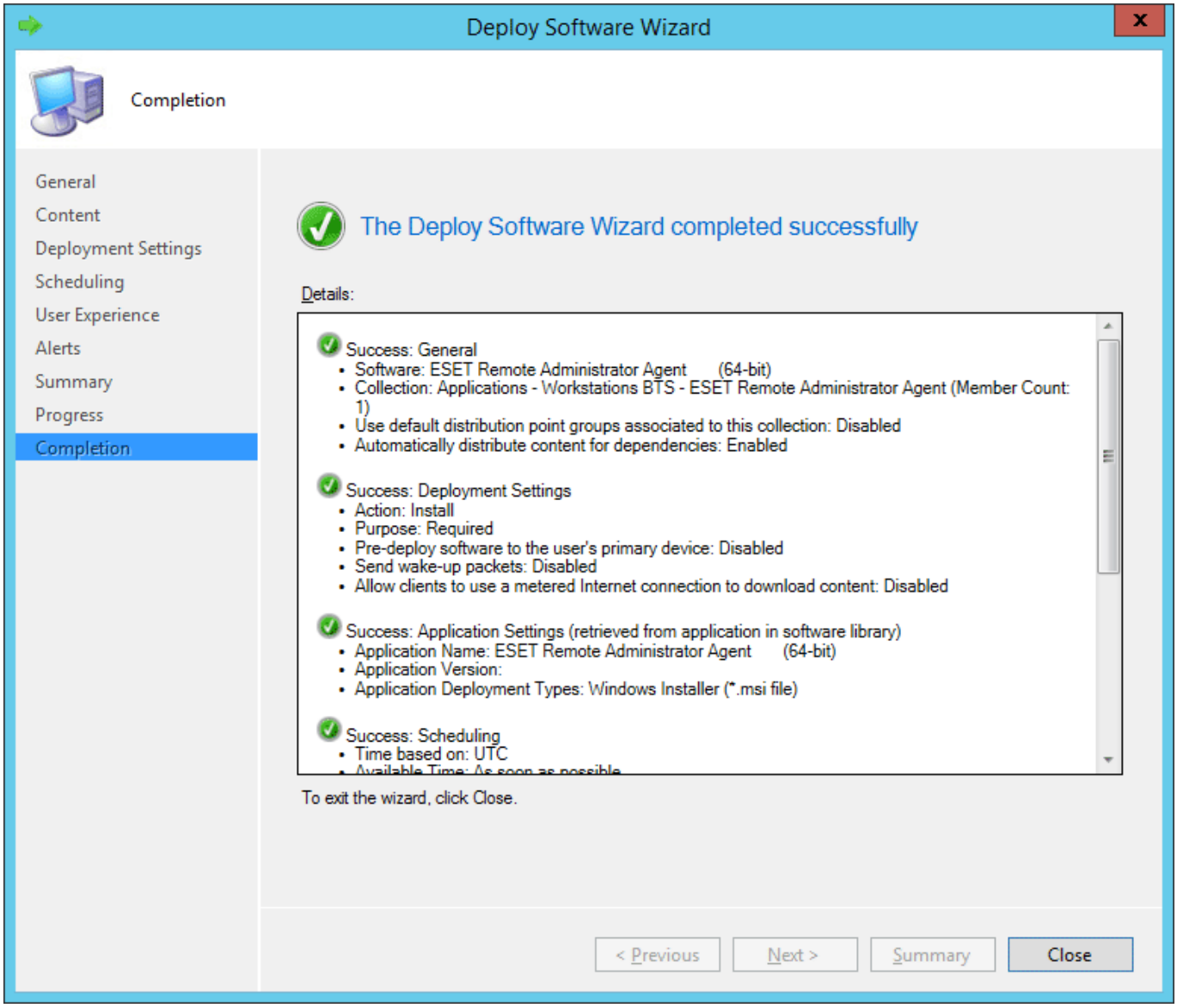

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution 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 para implementar ESET Management Agent y productos de seguridad de ESET de forma remota en los ordenadores de una red.

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

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

ESET Management Agent está preconfigurado para conectarse correctamente con ESET PROTECT, por lo que solo se puede realizar un número limitado de modificaciones en la configuración de ESET Management Agent a través de la política de ESET Management Agent.

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.

    • 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.

Requisitos previos de la Herramienta de implementación remota de ESET

En implementaciones remotas, compruebe que todos los ordenadores cliente disponen de conexión a Internet.

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

• La instancia de ESET PROTECT debe haberse creado y funcionar.

• Deben estar abiertos los puertos correspondientes. Consulte Puertos de ESET PROTECT Remote Deployment Tool.

• Una Live Installer debe crearse y descargarse en la unidad local del dispositivo desde el que va a realizar la implementación remota con la Herramienta de implementación.

La implementación puede fallar por diversos motivos. Si tiene cualquier problema con la implementación, lea el capítulo Resolución de problemas.

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.

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).

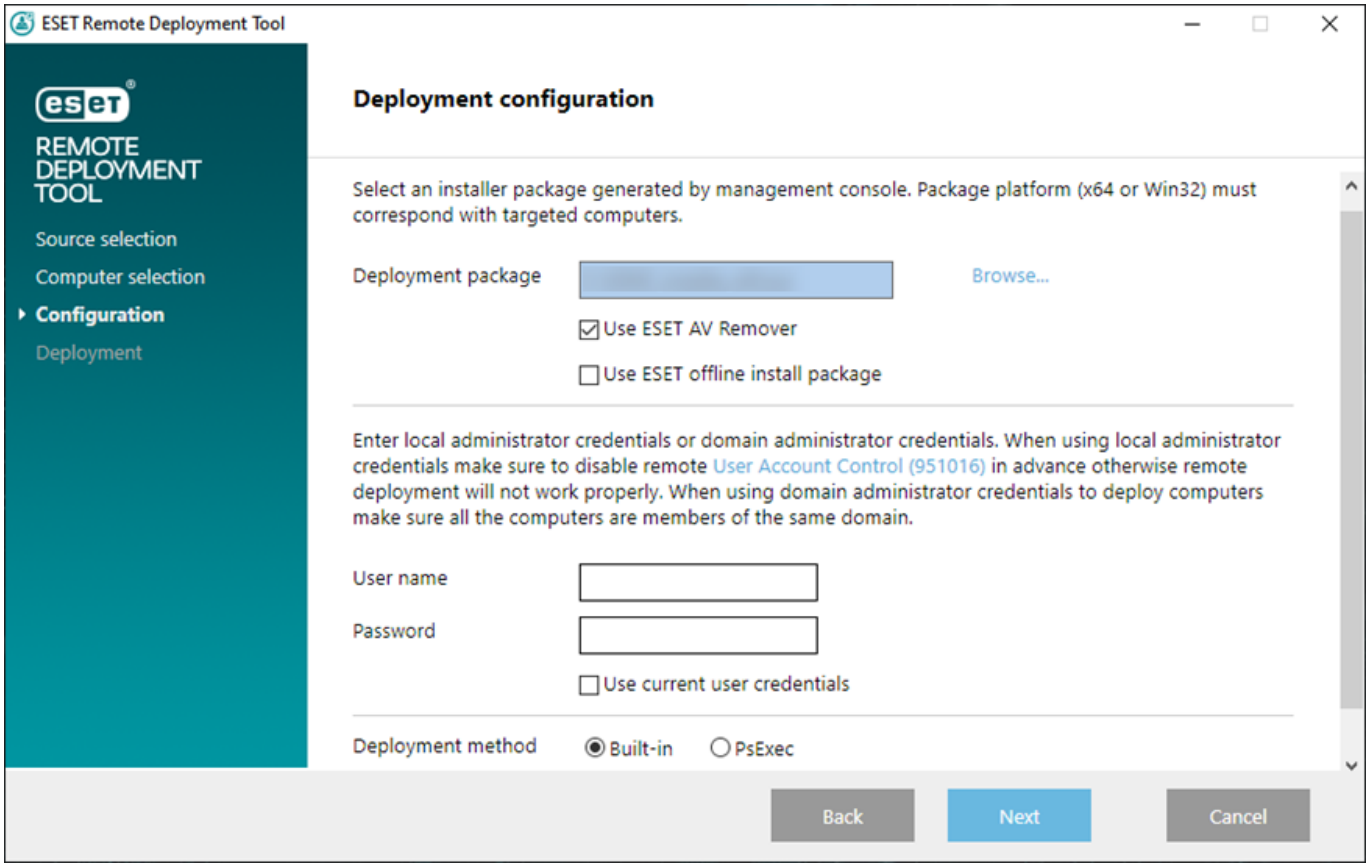
7. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

- 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.

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.

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).

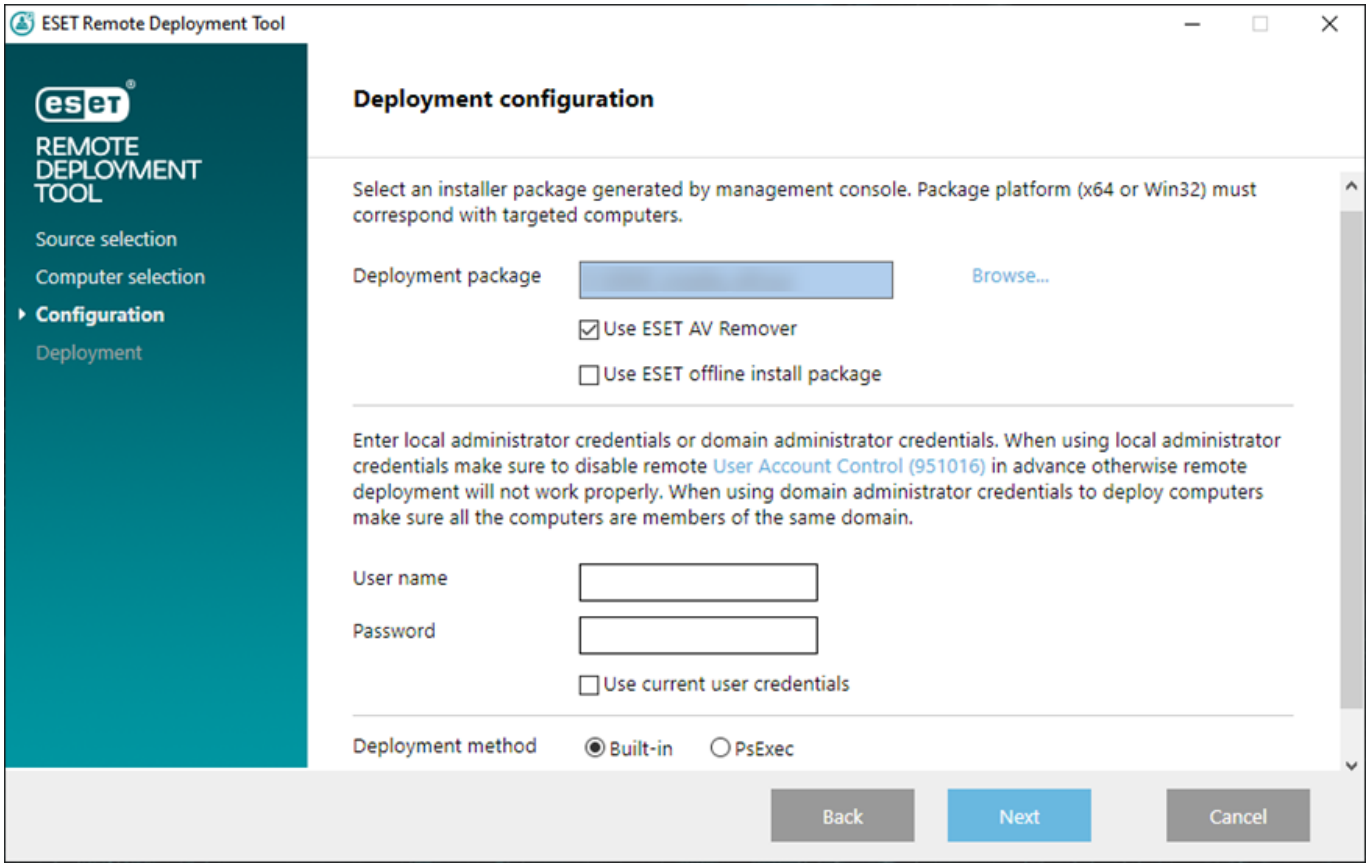
7. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

- 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.

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).

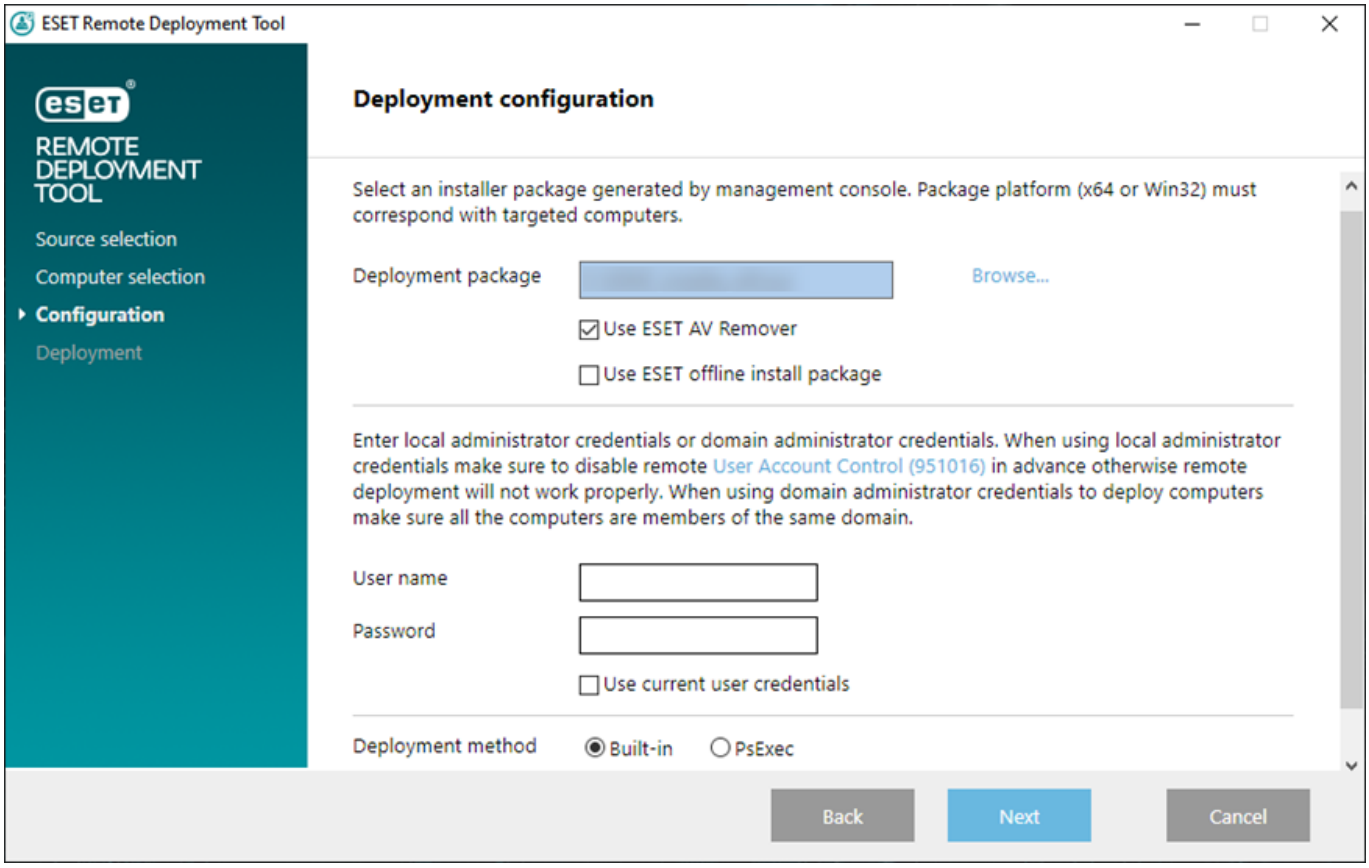
5. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

   • 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.

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**.

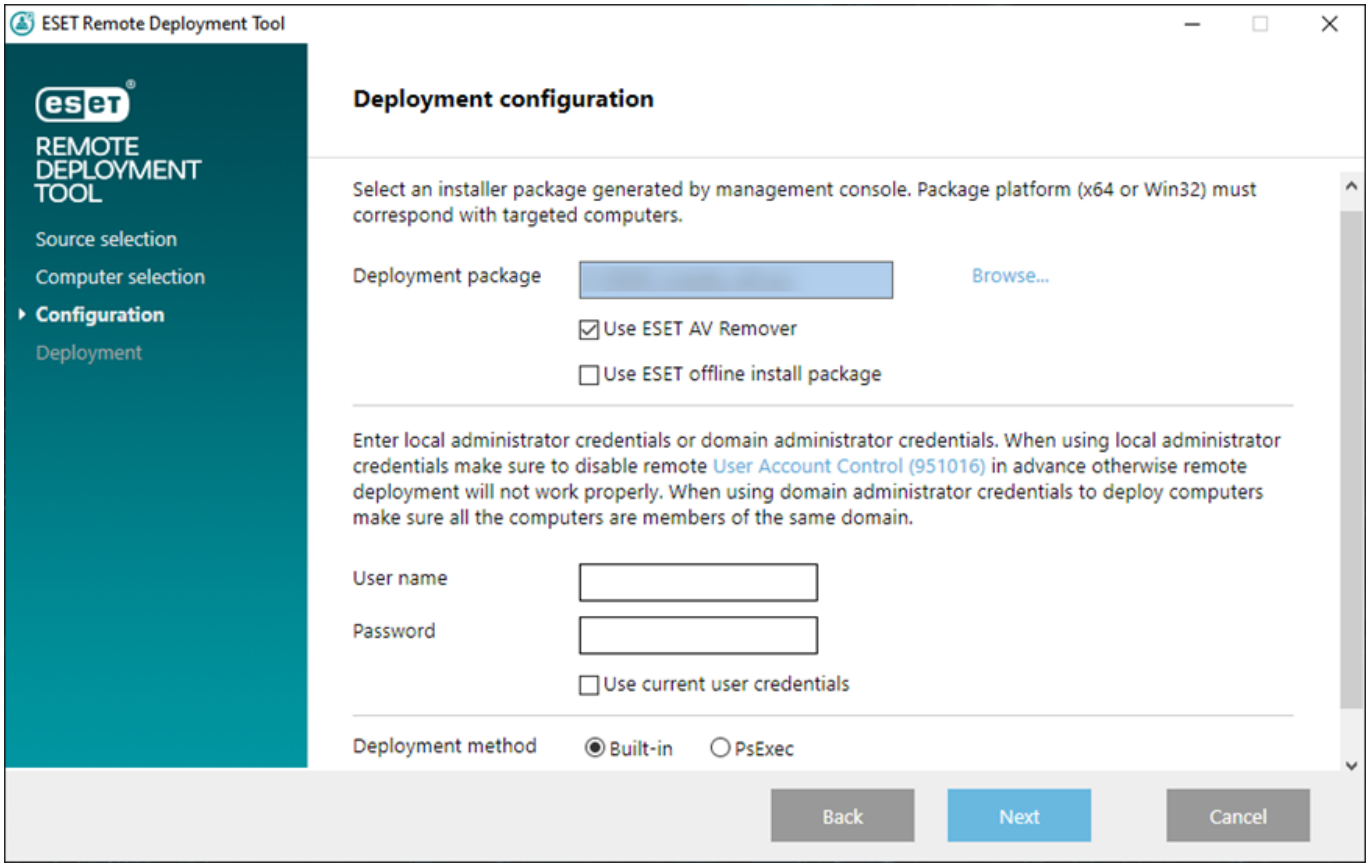
4. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en ESET PROTECT Web Console (local o en la nube).

- 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.

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 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.

No hay políticas predefinidas para ESET Management Agent. Para crear una política de ESET Management Agent, haga clic en **Políticas** > **Nueva política** y, en la sección **Configuración**, seleccione **ESET Management Agent**, donde podrá configurar los siguientes ajustes:

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 en su red. Marque o desmarque la casilla **Usar conexión directa si el proxy HTTP no está disponible** para activar o desactivar esta opción de reserva.
- **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.

• **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 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.

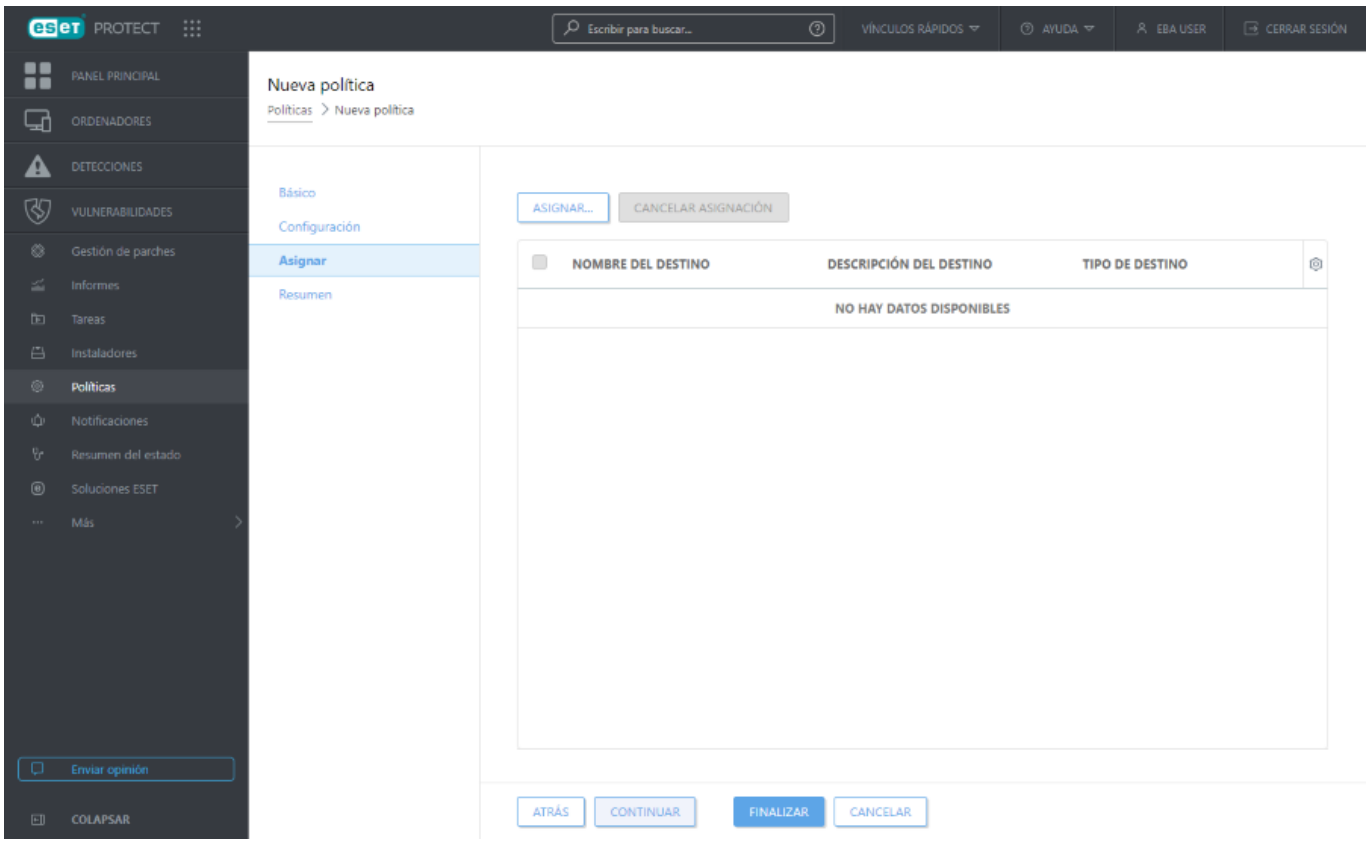
Configuración

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).

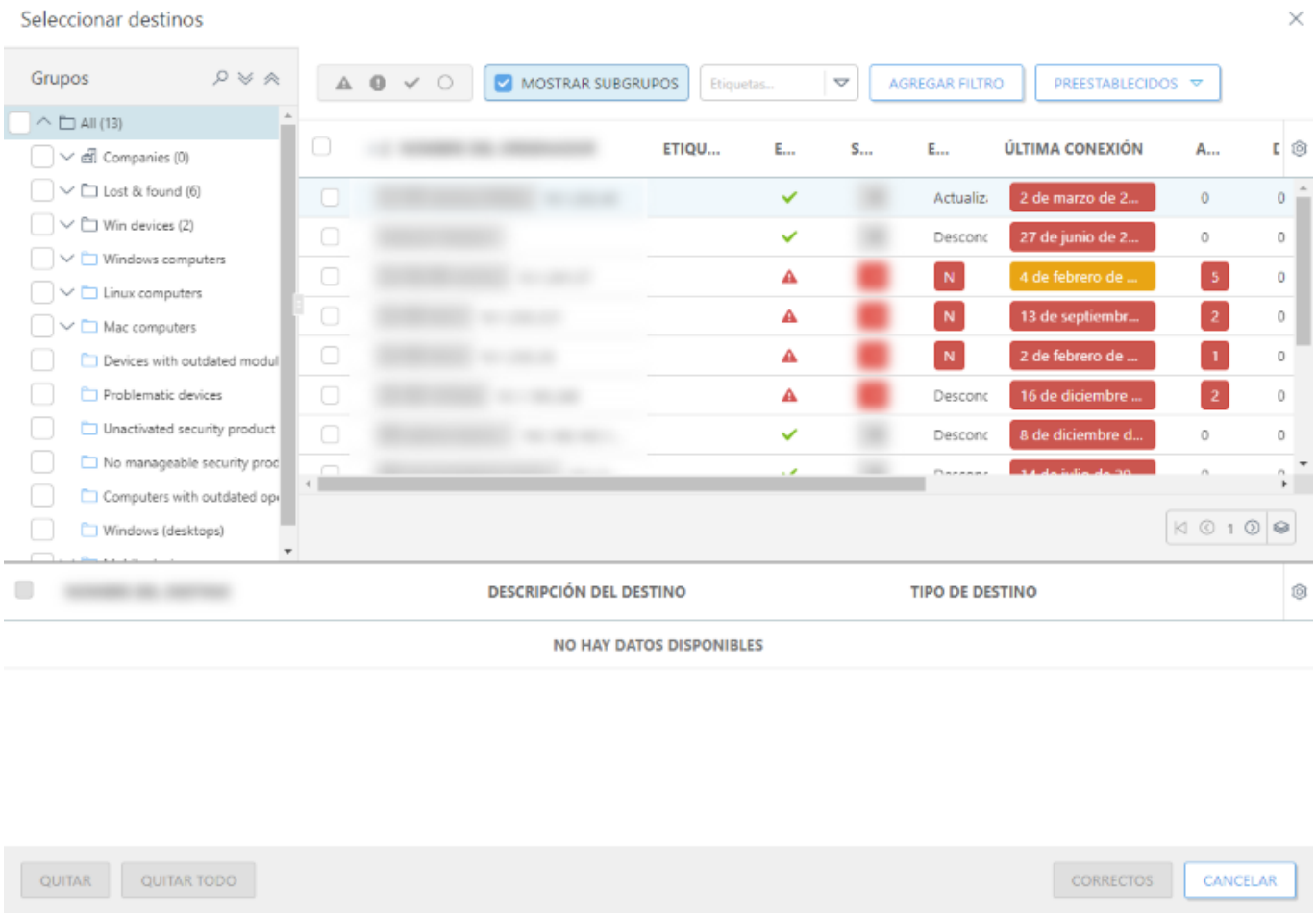
Asignar

Especifique los clientes (ordenadores individuales 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.

> 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 cada 10 minutos.

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.

Los problemas más común que puede impedir que ESET Management Agent se conecte al ESET PROTECT es que el DNS no funcione correctamente o que un firewall haya bloqueado los puertos (consulte nuestra lista de puertos que usa ESET PROTECT). Consultar nuestro artículo de la base de conocimiento para resolver la alerta **El dispositivo utiliza una conexión de conmutación por error**.

ESET PROTECT 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 y los siguientes elementos:

Panel
Clientes administrados
Ordenadores
Detecciones
Vulnerabilidades
Administración de parches
Informes
Tareas
Instaladores
Políticas
Notificaciones
Resumen del estado
Soluciones ESET
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 estos paneles predeterminados: **Resumen del estado, Resumen de la seguridad ESET LiveGuard** y **ESET Inspect**.

En ESET PROTECT 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 (a menos que establezca otra consola como predeterminada). Muestra información general sobre su red.

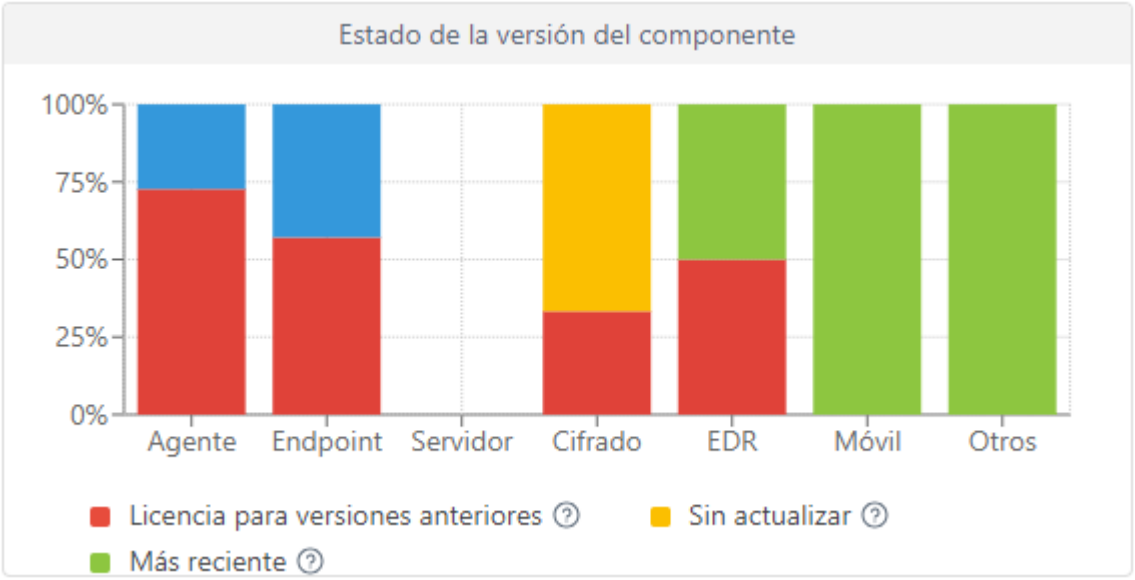
Filtros de dispositivos: muestra el número de dispositivos administrados basándose en el último estado del que se ha informado. Puede hacer clic en cada una de las 4 ventanas dinámicas para abrir una lista filtrada de dispositivos.

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 Actualizar agente 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 tiene constancia pero que no tienen instalado el agente) y **Rogue** (dispositivos cliente de los que ESET PROTECT 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.

ESET Inspect

Si utiliza ESET Inspect, este panel le ofrece una descripción general de datos estadísticos importantes de ESET Inspect. Haga clic en una ventana para abrir la consola de ESET Inspect y siga a partir de ahí. Haga clic en el icono del engranaje situado en la parte superior (junto a) y seleccione **Ocultar/Mostrar ESET Inspect** para ocultar o mostrar el panel.

Las ventanas de ESET Inspect muestran la siguiente información:

- **Detecciones sin resolver por gravedad**: el número total de detecciones sin resolver y las detecciones sin resolver por nivel de gravedad: Información, Advertencia o Crítico.
- **Detecciones de los últimos 7 días por gravedad**: un gráfico de líneas compuesto con el número de

detecciones por gravedad de los últimos siete días.

• **Los 10 ordenadores con más detecciones en los últimos 7 días**: el nombre del ordenador, el número de ordenadores por nivel de gravedad de la detección (rojo: Crítico; amarillo: Advertencia; azul: Información) y el número total de detecciones.

• **Ordenadores por gravedad de detección**: un gráfico de anillos con el número de ordenadores por nivel de gravedad de la detección: Crítico, Advertencia e Información.

• **Incidentes**: el número de incidentes (creados en ESET Inspect) por estado (**Abierto**, **En curso**, **En espera**, **Resuelto**, **Cerrado** y **No válido**). Haga clic en un número junto al estado de un incidente para ver más detalles en ESET Inspect. Cuando el representante del servicio de ESET edite el incidente en ESET Inspect, verá el incidente etiquetado como **Investigado por ESET**.

ESET Cloud Office Security

Si utiliza ESET Cloud Office Security, este panel proporciona un resumen de los datos estadísticos importantes de ESET Cloud Office Security. Haga clic en una ventana para abrir la consola de ESET Cloud Office Security y siga a partir de ahí. Haga clic en el ícono del engranaje situado en la parte superior (junto al ícono de actualización) y seleccione **Ocultar/Mostrar ESET Cloud Office Security** para ocultar/mostrar el dashboard.

Las ventanas dinámicas de ESET Cloud Office Security incluyen la siguiente información:

• **Usuarios protegidos**: el número de usuarios protegidos

• **Uso de licencias**: el número de licencias usadas y sin utilizar

• **Sitios** de **SharePoint protegidos**: el número de sitios de SharePoint protegidos.

• **Grupos** de **Teams protegidos**: el número de grupos de Teams protegidos.

• Los **10 usuarios con más detecciones en los últimos 30 días**: el nombre y el correo electrónico con el número de detecciones de correo electrónico y archivos para los 10 usuarios con más detecciones.

• **Detecciones en los últimos 30 días**: un gráfico de histograma con el número de detecciones en los servicios específicos (**Teams**, **SharePoint**, **correo electrónico**, **Drive**) durante los últimos 30 días. Haga clic en cualquier servicio en el gráfico de histograma para abrir la página de Detecciones en ESET Cloud Office Security.

• **Objetos en cuarentena**: el número de objetos en cuarentena en los servicios específicos en los últimos 7 y 30 días. Haga clic en cualquier fila de servicio para ver la página Cuarentena en ESET Cloud Office Security.

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.

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).

ESET MDR

ESET MDR proporciona un resumen de los incidentes y las detecciones de ESET Inspect. Para usar ESET MDR, necesita una licencia de ESET Inspect y el nivel de **ESET PROTECT MDR**.

> **Disponibilidad por país de ESET MDR**
> ESET MDR está disponible en los siguientes países: EE. UU., Canadá, Japón, Reino Unido, Países Bajos, Francia, Italia, Alemania, Austria, Suiza, Suecia, Noruega, Dinamarca, Finlandia, Islandia, Eslovaquia, República Checa y Ucrania.

El servicio de ESET MDR cubre todos los dispositivos administrados que ejecutan archivos de ESET Inspect. Siga los pasos que se indican a continuación para seleccionar los dispositivos donde desea administrar la seguridad, independientemente del servicio de ESET MDR:

1. Abra ESET PROTECT y vaya a **Equipos**.
2. Haga clic en el icono de engranaje situado junto al grupo primario estático existente y seleccione **Nuevo grupo estático**.
3. Escriba `exempt` en el campo **Nombre** y haga clic en **Finalizar**.
4. Seleccione el grupo principal y los dispositivos que desea incluir en el grupo exempt.
5. Haga clic en **Equipo** > **Administrar** > **Mover a grupo** y seleccione el grupo `exempt`.

Usted administra los dispositivos del grupo `exempt`: puede controlar los incidentes de forma manual sin las acciones de respuesta aplicadas automáticamente.

> Necesita los conjuntos de permisos siguientes para ver **ESET MDR** en el panel:
> • **Informes de ESET MDR** : usar
> • **Acceso de solo lectura a ESET Inspect** – Lectura
> Puede ver los datos en mosaicos según los conjuntos de permisos personalizados en ESET Inspect y ESET PROTECT.

Haga clic en un mosaico para abrir la consola web de ESET Inspect y siga a partir de ahí.

Las ventanas de **ESET MDR** muestran la siguiente información:

- **Incidentes**: número de incidentes por nivel de gravedad en los últimos siete días: **Total**, **Alto**, **Medio** y **Bajo**

- **Principales incidentes sin resolver**: lista con el mayor número de incidentes en los últimos siete días: **Nombre del incidente**, **Autor**, **Fecha de creación**, **Dispositivos afectados**, **Estado** y **Asignado a**

- **Estado del incidente**: gráfico de anillos con el número de incidentes por estado en los últimos siete días: **Abierto**, **En curso**, **En espera**, **Resuelto**, **Cerrado** y **No válido**

- **Dispositivos más afectados**: lista con el mayor número de dispositivos afectados según el nivel de gravedad en los últimos siete días:**Nombre del dispositivo**, **Incidentes** (nivel de gravedad: **Informativo**, **Advertencia** o **Crítico**), **Nombre del grupo** y **Visto por última vez**

- **Acciones de respuesta**: gráfico de anillos con el número de acciones de respuesta a un incidente en los últimos siete días: **Bloquear**, **Desinfectar y bloquear**, **Aislar** y **Eliminar proceso**

- **Pipeline de incidentes**: **Número de todas las detecciones**, **Número de detecciones relacionadas con incidentes** y **Número de incidentes creados** en los últimos siete días

- **Incidentes a tiempo**: gráfico de líneas con el número de incidentes detectados en los últimos siete días según el nivel de gravedad: **Alto**, **Medio** y **Bajo**

En cada mosaico, puede hacer clic en el botón ⋮ para:

- **Ver todo**: haga clic aquí para acceder a la consola web de ESET Inspect. Se le redirigirá a la página específica con el filtro configurado (Tiempo de creación: 7 días)

- **Actualizar**: haga clic aquí para actualizar el mosaico específico

Consulte también el informe de ESET MDR.

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:

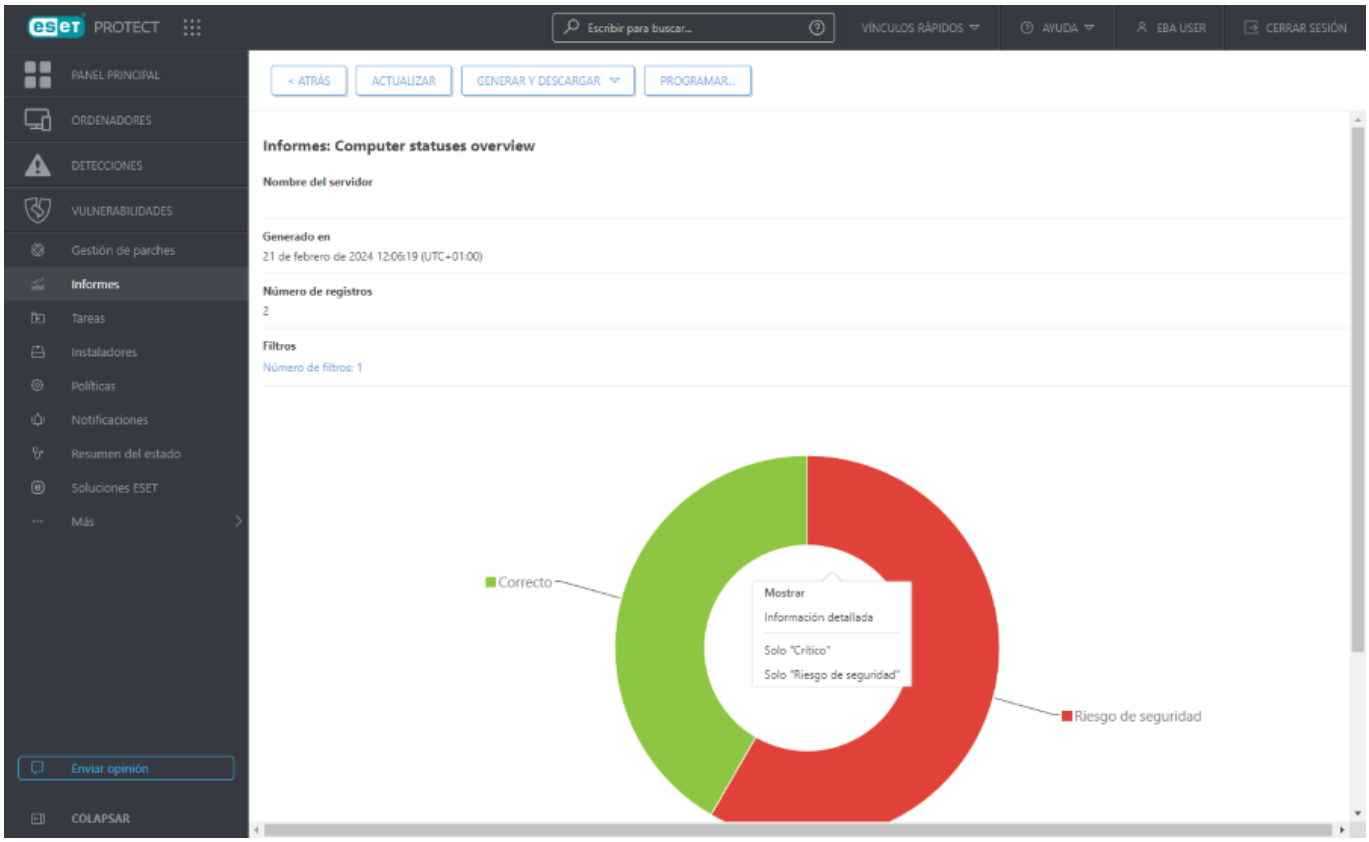
o Administrar políticas

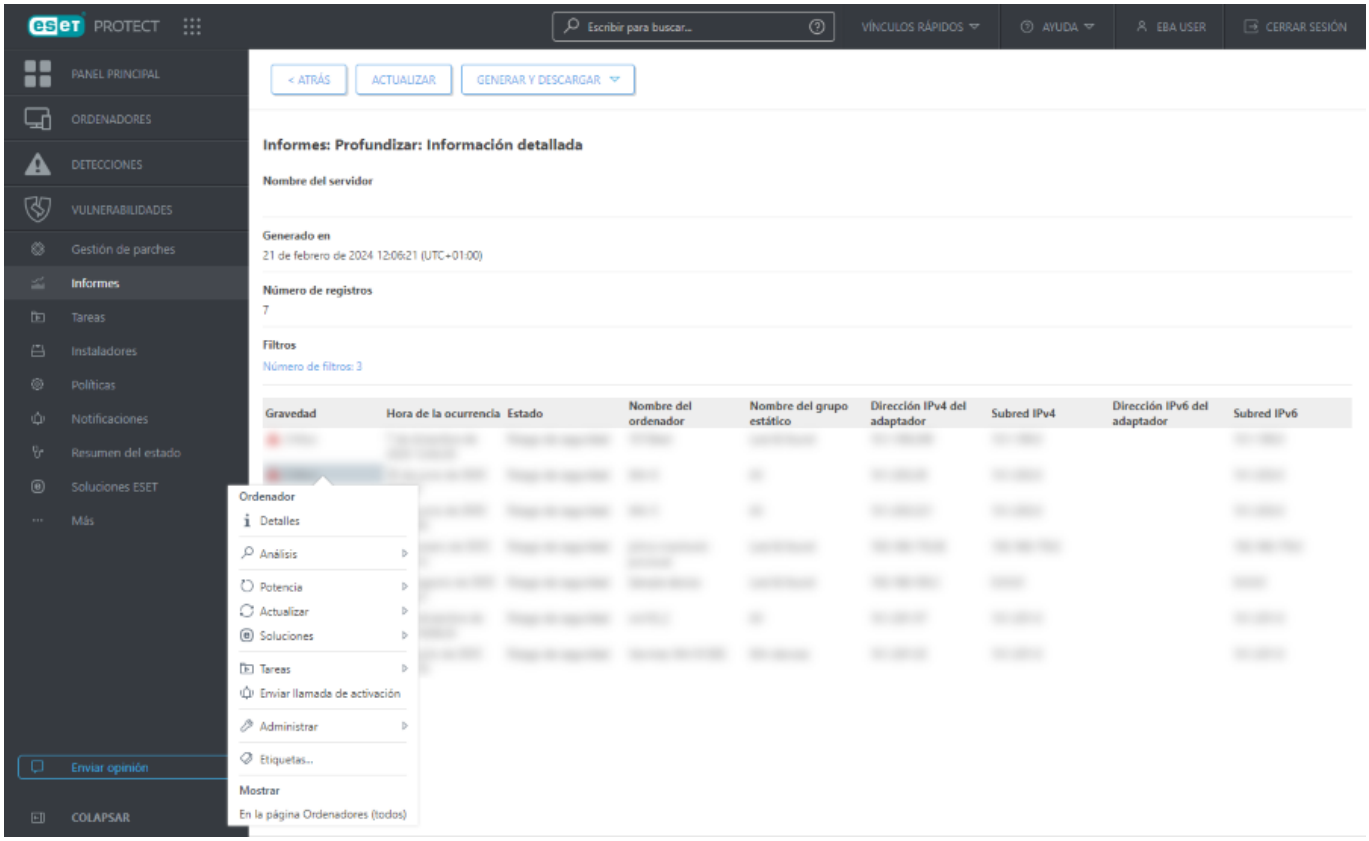
o**Nueva política**

• **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 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.
- 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 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.

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.

> Los dispositivos móviles inscritos deben conectarse a ESET PROTECT cada 120 días para evitar problemas de conexión. Puede ver esta información en el vínculo del correo electrónico o el código QR de inscripción. No inscriba un dispositivo de repuesto por adelantado. Recomendamos inscribir solo un dispositivo de repuesto, que se utilizará antes de 120 días.

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

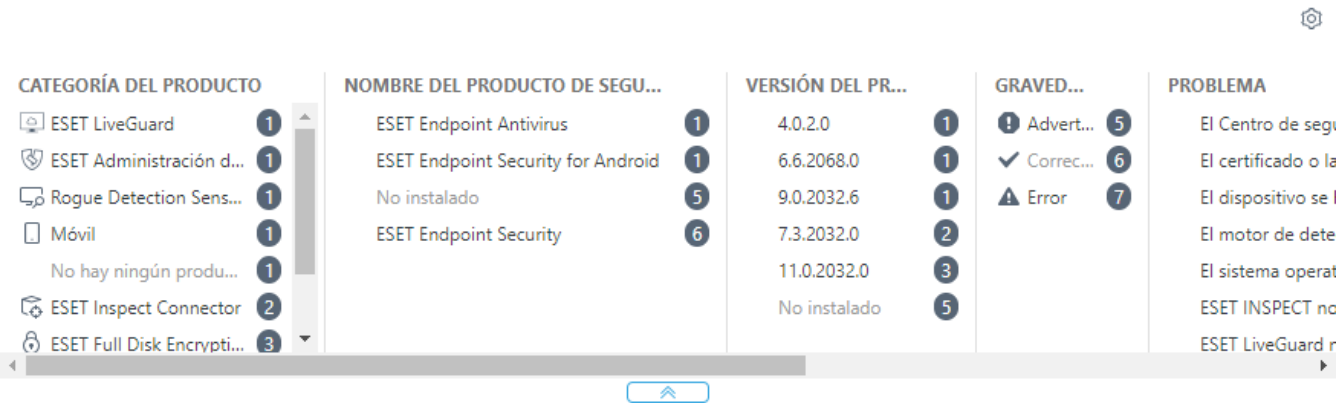
  - **Protegido por ESET** (protegido por un producto ESET): Escritorio, Móvil, Servidor, Servidor de correo electrónico, Servidor de puerta de enlace, Servidor de colaboración, Servidor de archivos.

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

  - **Otros**: ESET LiveGuard, ESET Inspect Connector, ESET Full Disk Encryption, ESET Bridge, ESET Vulnerability & Patch Management.

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

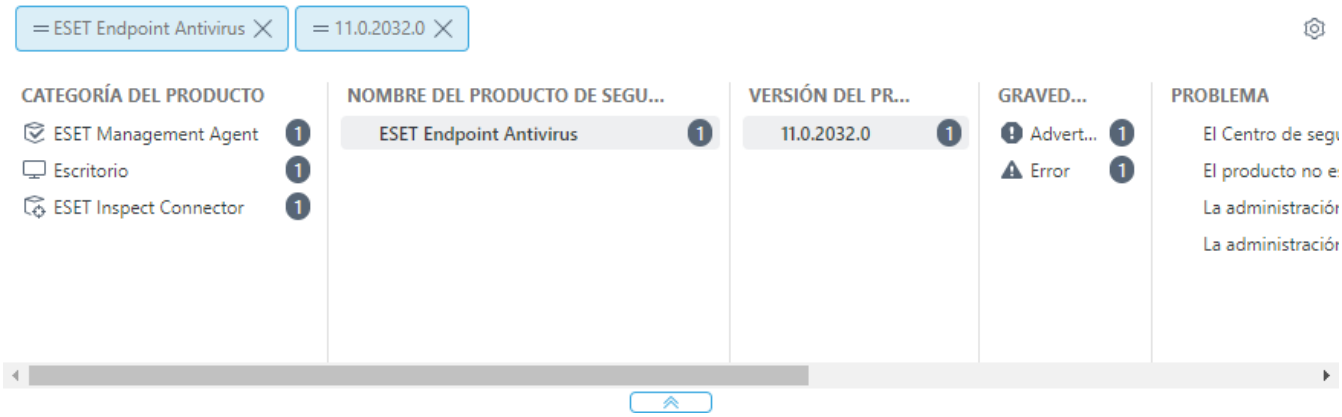
- Puede ver los **Filtros avanzados** como un panel de filtros expansible en la pantalla **Ordenadores**.



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 Web Console. El ESET Inspect solo está disponible cuando tiene la licencia de ESET Inspect y ESET Inspect está conectado a ESET PROTECT. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a 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
- **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**:
  - **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**
  - Haga 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.

  - Haga clic en el icono de la papelera para cancelar la asignación del usuario actual.
  - Haga 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:
  - Aislar de la red
  - 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.
  - Marcar como maestro para clonación
  - **Desactivar la detección de hardware**: desactive la detección de los cambios de hardware de forma permanente. Esta acción es irreversible.
  - **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** > **Desactivar** para detener el modo de diagnóstico.

El límite de tamaño de archivo para la entrega de registro por dispositivo es de 15 MB. Puede acceder a los registros desde Web Console en **Detalles** > sección **Registros**. Si los registros que ha recopilado la tarea superan los 15 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 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 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 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**, **Firewall**, **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:

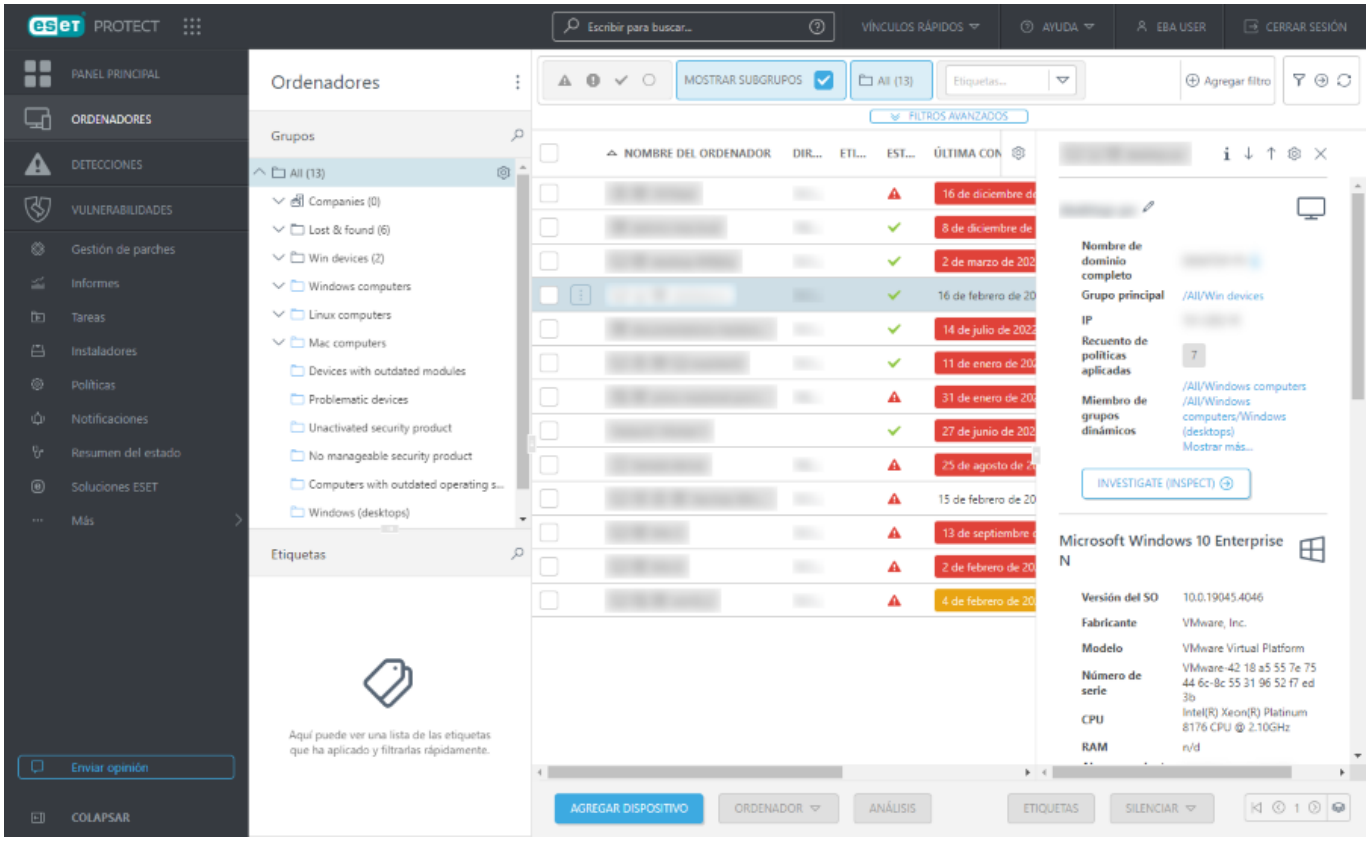
- **Mostrar detalles**: abra el menú Detalles del ordenador

- **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.

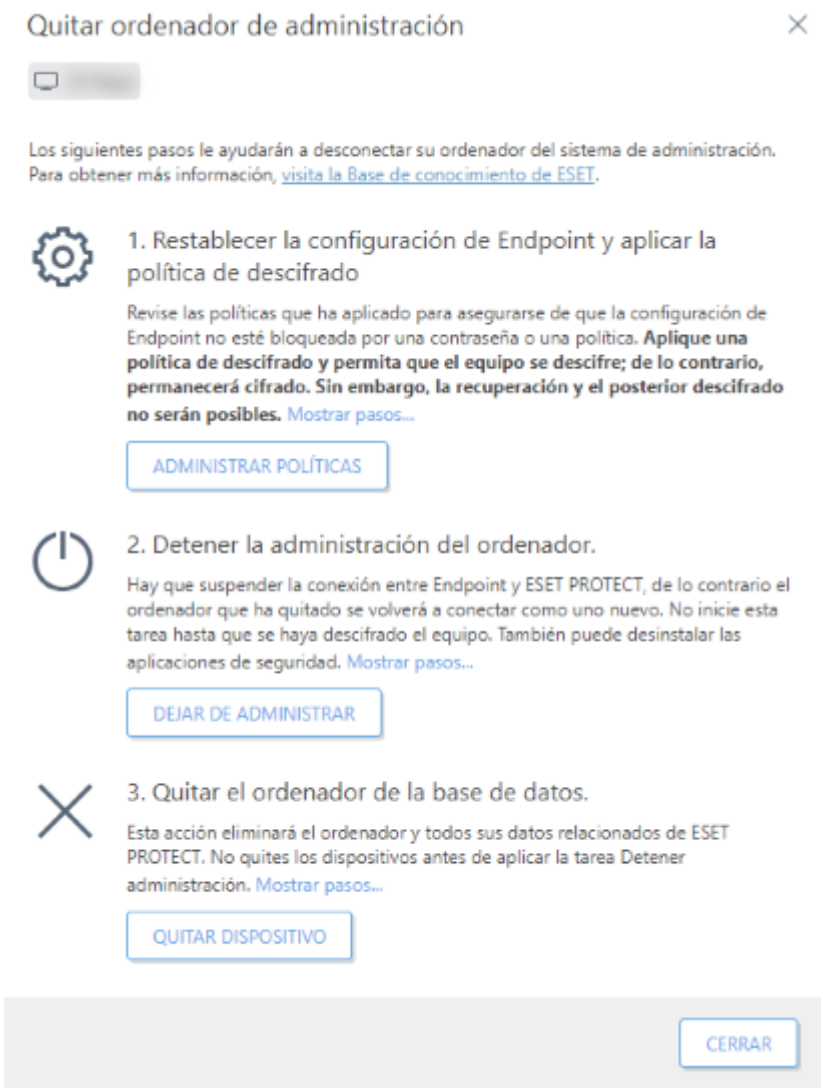
- **Administrar el contenido de Detalles del ordenador**: puede gestionar qué secciones del panel lateral de vista previa del ordenador se muestran y en qué orden.

- **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, haga clic en **Desactivar contraseña** para asignar la política **Desactivar protección por contraseña** al ordenador seleccionado. También puede crear una nueva política para quitar la contraseña (seleccione establecer una contraseña, pero no escriba ninguna contraseña) y asignarla al ordenador. Para ordenadores cifrados con ESET Full Disk Encryption, siga los pasos de descifrado.

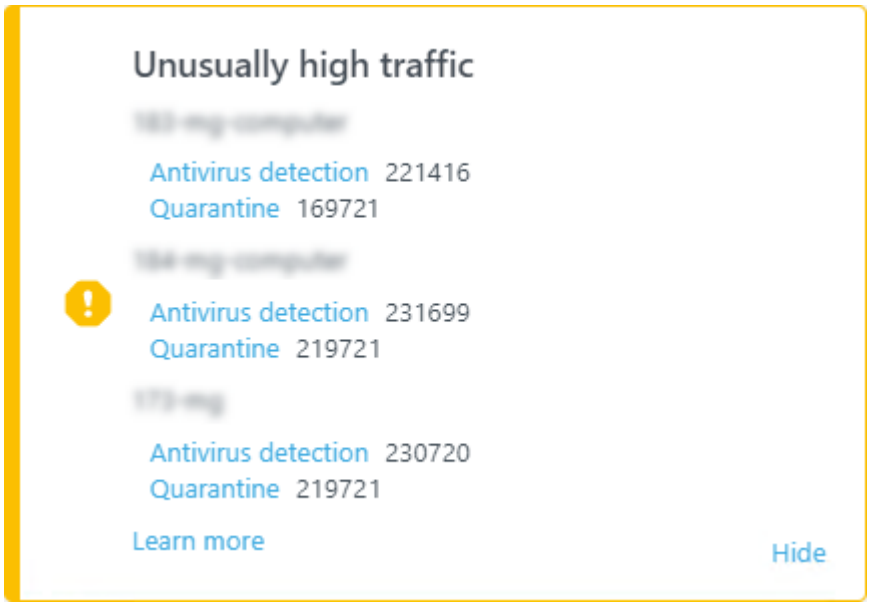
2. **Detener administración del ordenador**: ejecuta una tarea Detener administración o desinstale ESET Management Agent o el producto de seguridad ESET localmente en el ordenador. De esta forma se suspende la conexión entre el ordenador y ESET PROTECT.

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, 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.

Tráfico inusualmente elevado desde ordenadores administrados

Cuando el administrador de Web Console inicia sesión, puede ver una ventana en la que se advierte de un tráfico inusualmente elevado desde los ordenadores administrados.



La sobrecarga de registro ralentiza la red entre los ordenadores administrados y ESET PROTECT:

- Los datos de los ordenadores administrados tardan más en cargarse en ESET PROTECT.
- Web Console podría no mostrar el estado actual de los ordenadores administrados afectados.

El administrador de Web Console debe resolver registros de tráfico poco comunes (por ejemplo, un archivo en la cuarentena detectado en Endpoint o ESET PROTECT).

La ventana desaparece cuando se reduce el número de registros de tráfico poco comunes.

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	✔
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**: haga clic en junto a un grupo estático y seleccione **Soluciones** > **Activar ESET Inspect** para activar y habilitar ESET Inspect 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
Active Directory Scanner	Utilice el token de acceso generado para autenticar ESET Active Directory Scanner para conectarse a ESET PROTECT y sincronizar Active Directory con el grupo estático seleccionado.	✔	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:

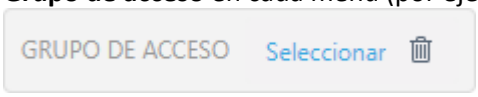
- **Todo**: este es un grupo principal para todos los dispositivos de la red de ESET PROTECT Server. Todos los objetos creados por el administrador están (de forma predeterminada) en este grupo. Siempre se muestra, y su nombre no puede cambiarse. El acceso a este grupo otorga a los usuarios acceso a 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

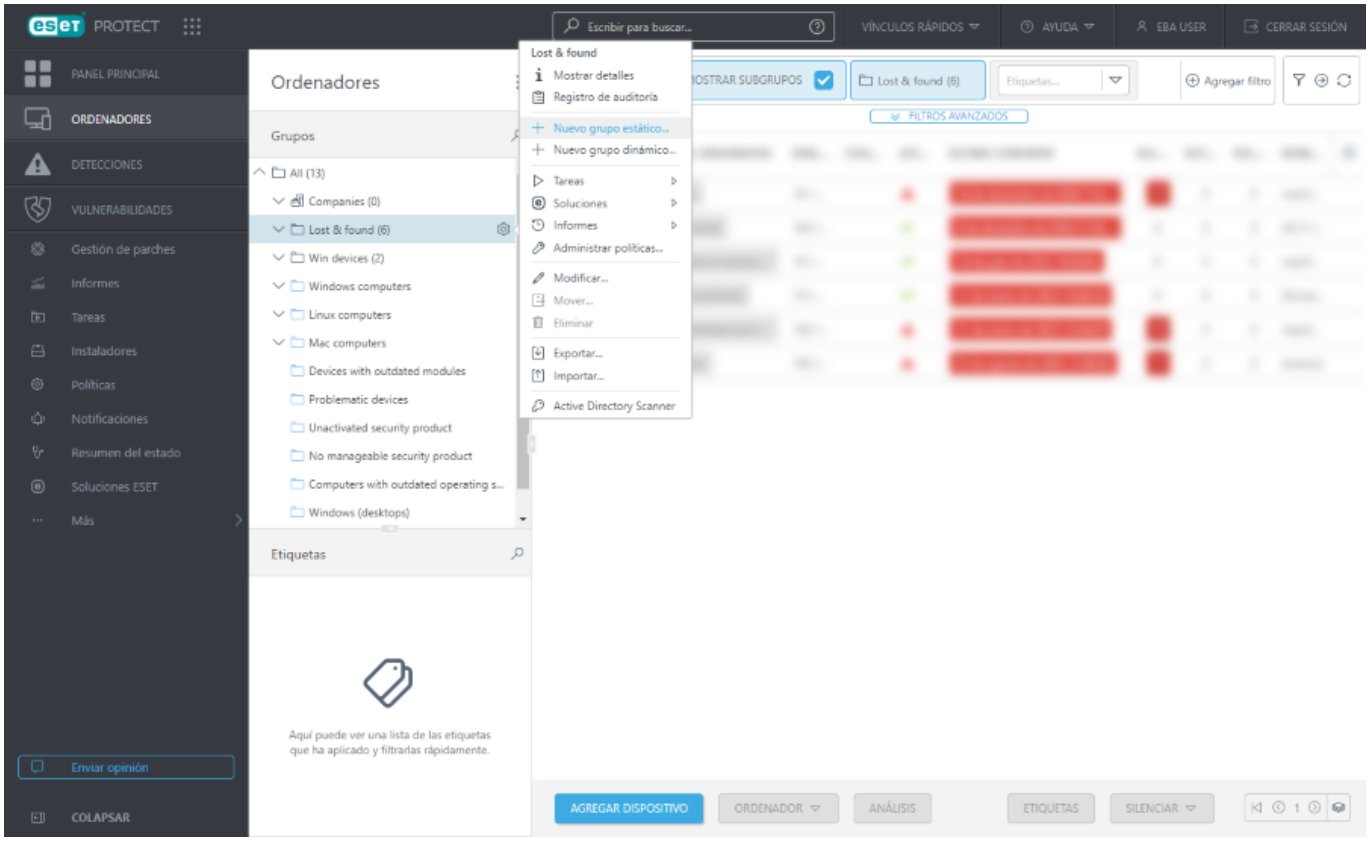
Si quedan objetos en el grupo estático, la operación de eliminación fallará. Hay un botón de filtrado de **Grupo de acceso** en cada menú (por ejemplo, **Instaladores**) con objetos.



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**.



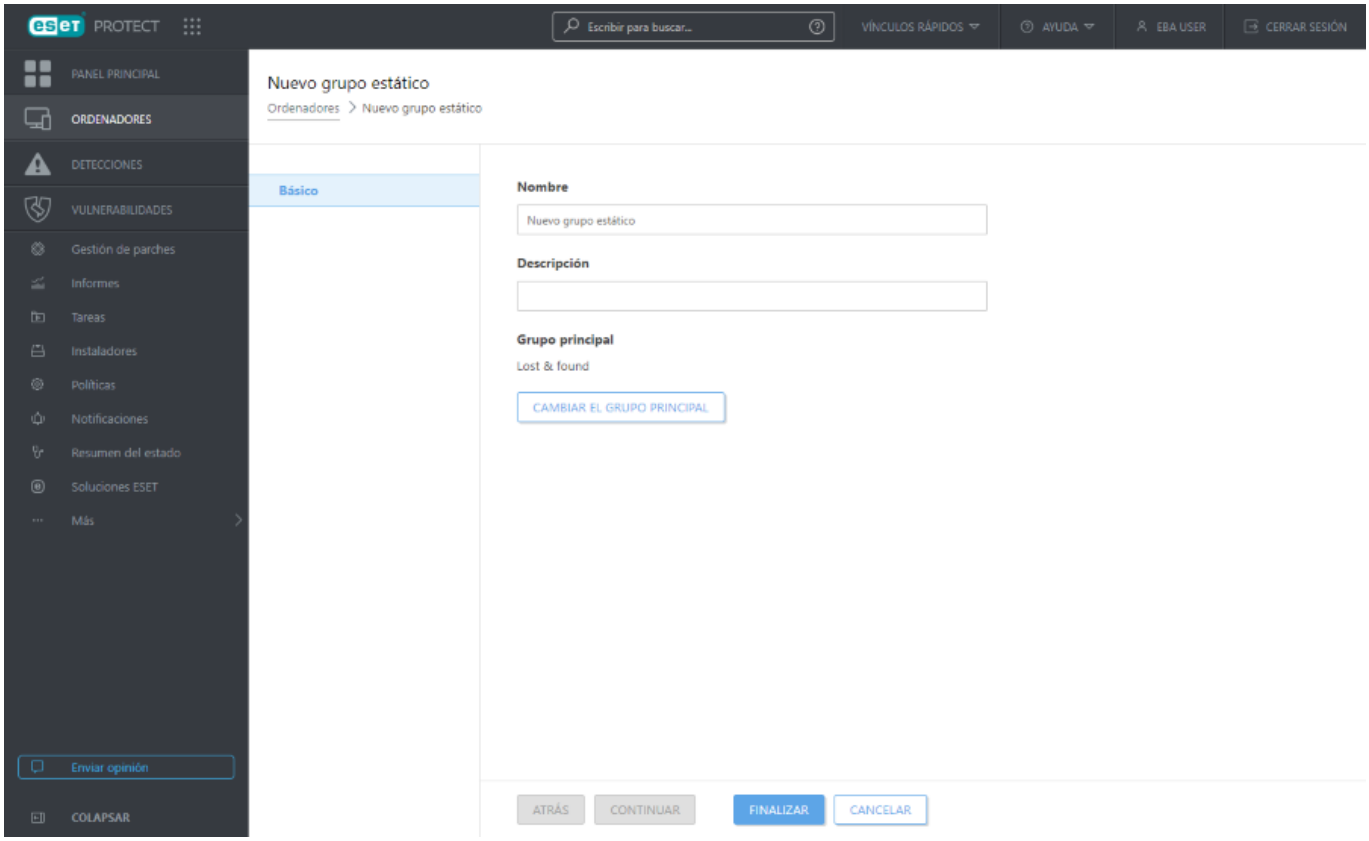
Básico

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.

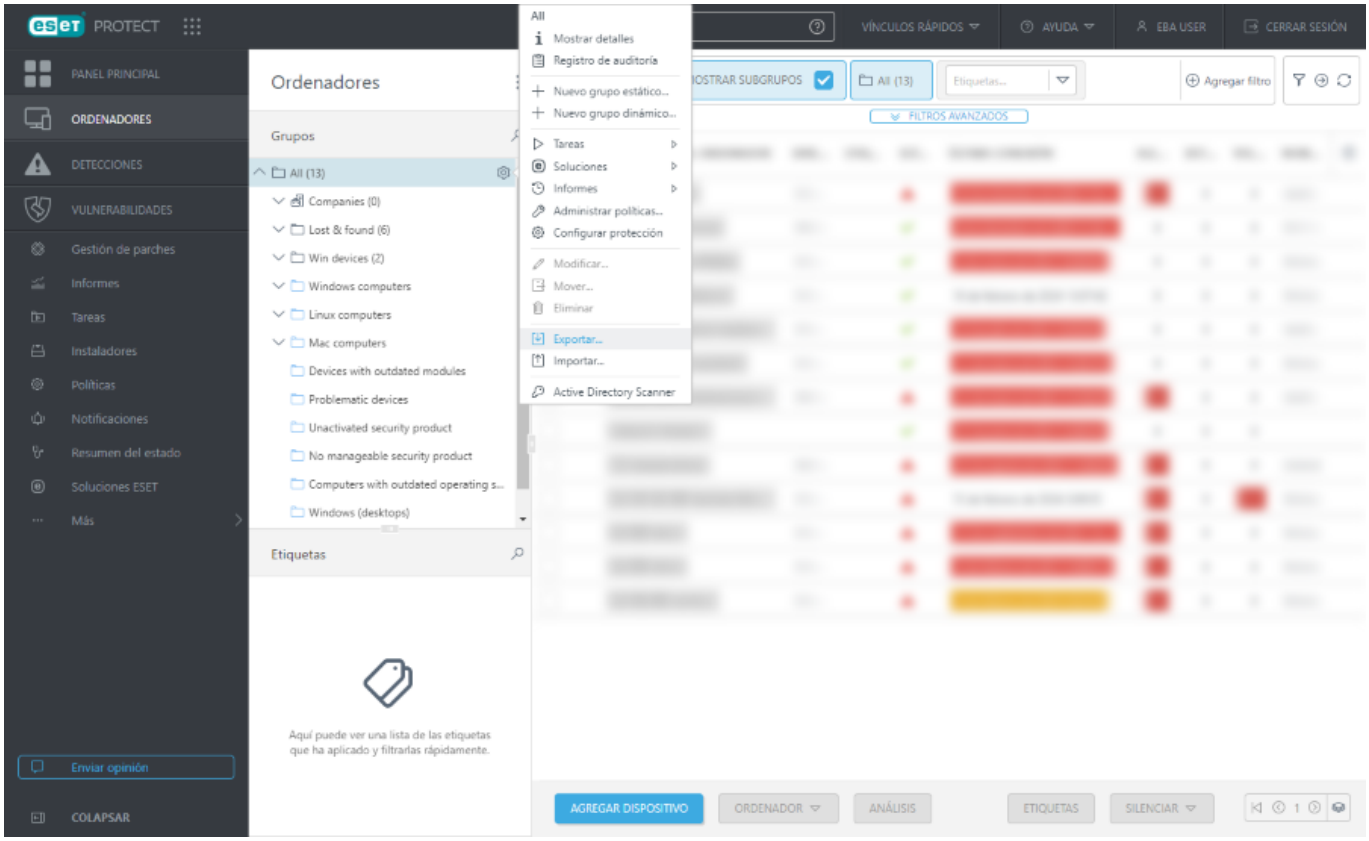


Exportar grupos estáticos

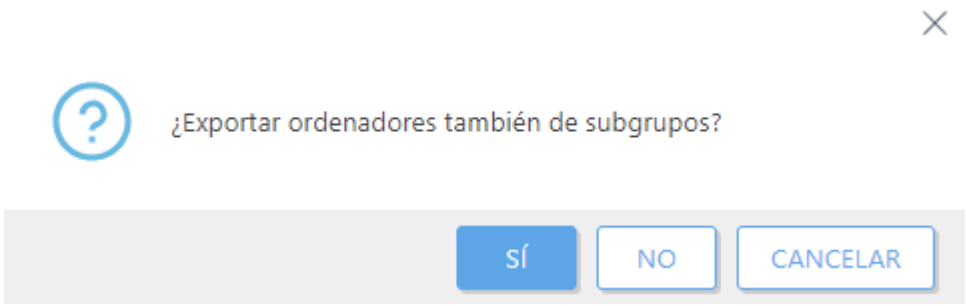
Exportar una lista de ordenadores que estén en la estructura de ESET PROTECT es sencillo. Puede exportar la lista y almacenarla como una copia de seguridad para poder importarla de nuevo en el futuro, por ejemplo, si desea restaurar la estructura del grupo.

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.

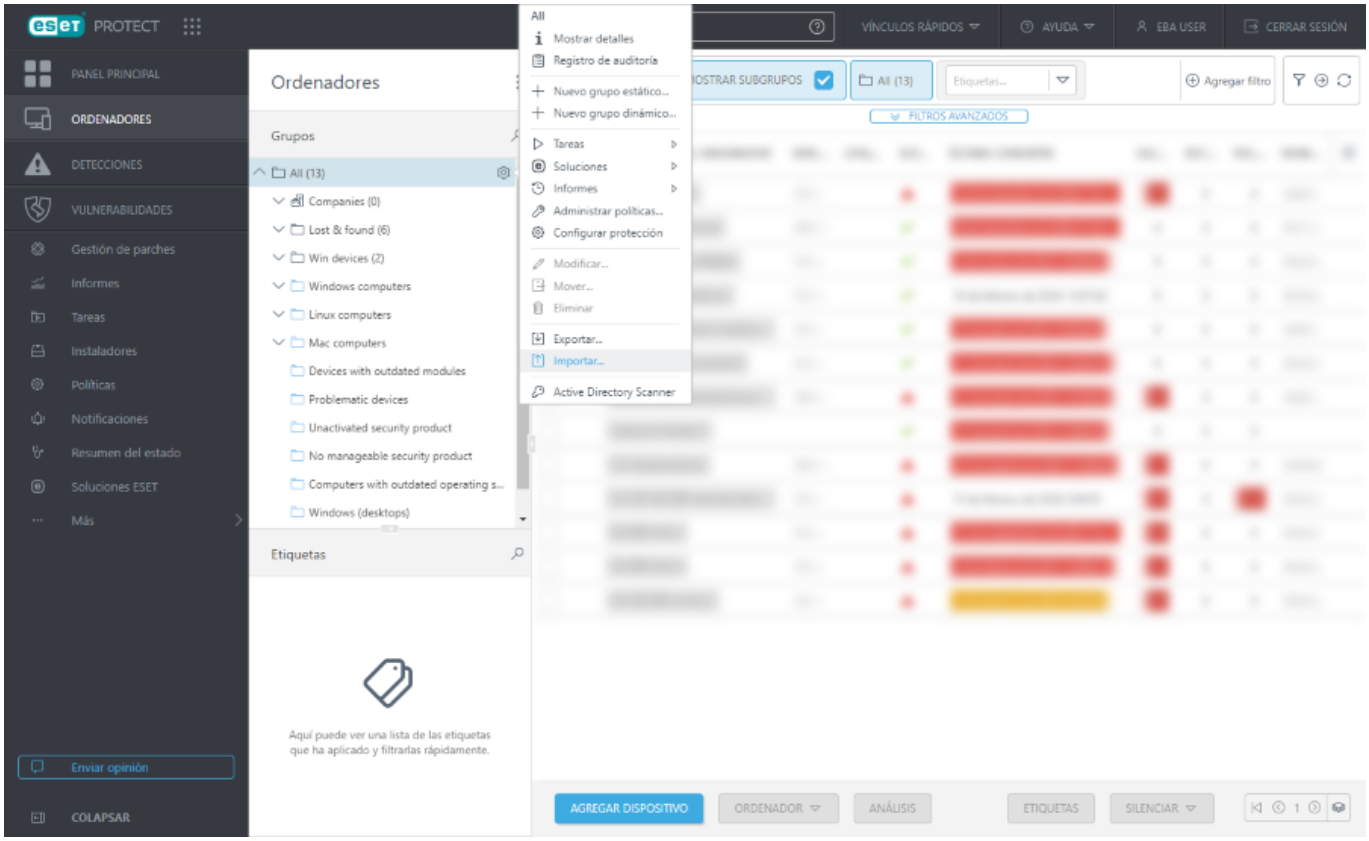


4. El archivo se guardará en formato *.txt*.

> 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 **Elegir archivo** 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.

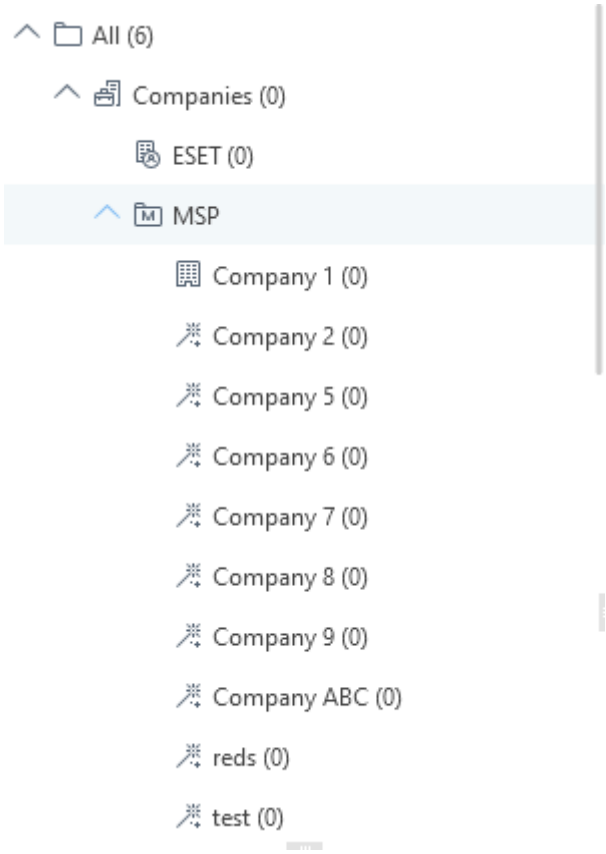
Árbol de grupos estáticos para ESET Business Account/ESET MSP Administrator

Si ha implementado ESET PROTECT 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 3.4 de ESET PROTECT).

Si ha implementado ESET PROTECT desde ESET MSP Administrator, la estructura ESET MSP Administrator aparece en el árbol de grupo estático. Más información sobre ESET PROTECT 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**.



En **Empresas**, puede ver:

- Empresa de ESET Business Account: si implementó ESET PROTECT desde ESET Business Account.
- Árbol de ESET MSP Administrator: si implementó ESET PROTECT desde ESET MSP Administrator.

- Ambos árboles: si implementó ESET PROTECT desde una cuenta mixta.

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 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 con acceso **personalizado** a ESET PROTECT 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.

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 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. 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.

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 crear ESET PROTECT, tendrá a su disposición varios grupos dinámicos predefinidos para sus ordenadores y sus dispositivos móviles. 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. Es posible asignarles políticas (consulte cómo se aplican las políticas) o preparar una tarea para todos los ordenadores del grupo.

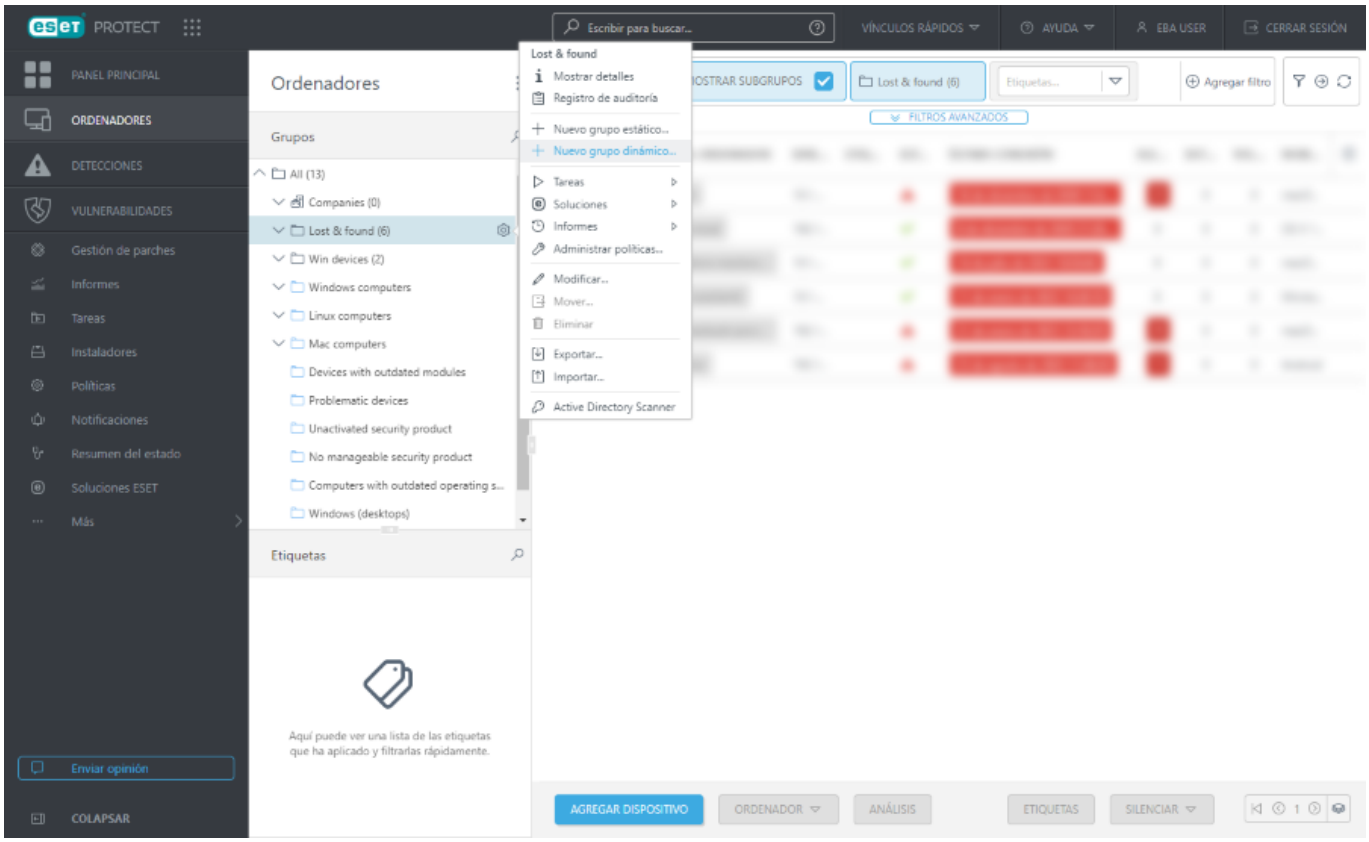
Los grupos dinámicos pueden estar dentro (bajo) de grupos estáticos o en grupos dinámicos. Sin embargo, el grupo estático no puede estar dentro de un grupo dinámico. Todos los grupos dinámicos que estén debajo de un determinado grupo estático solo filtran los dispositivos de ese grupo estático. Si un 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

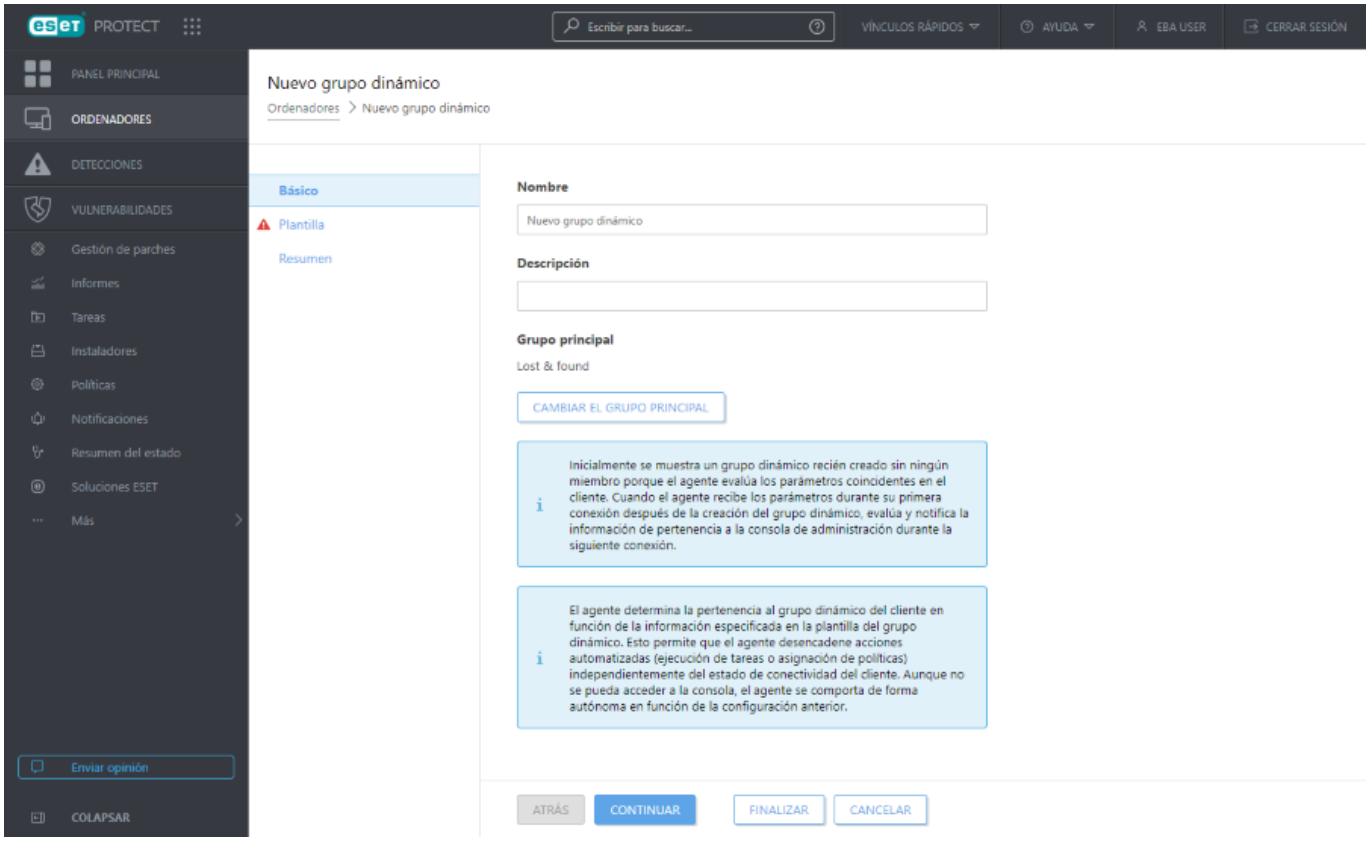
Siga estos pasos para crear un grupo dinámico nuevo.

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**.



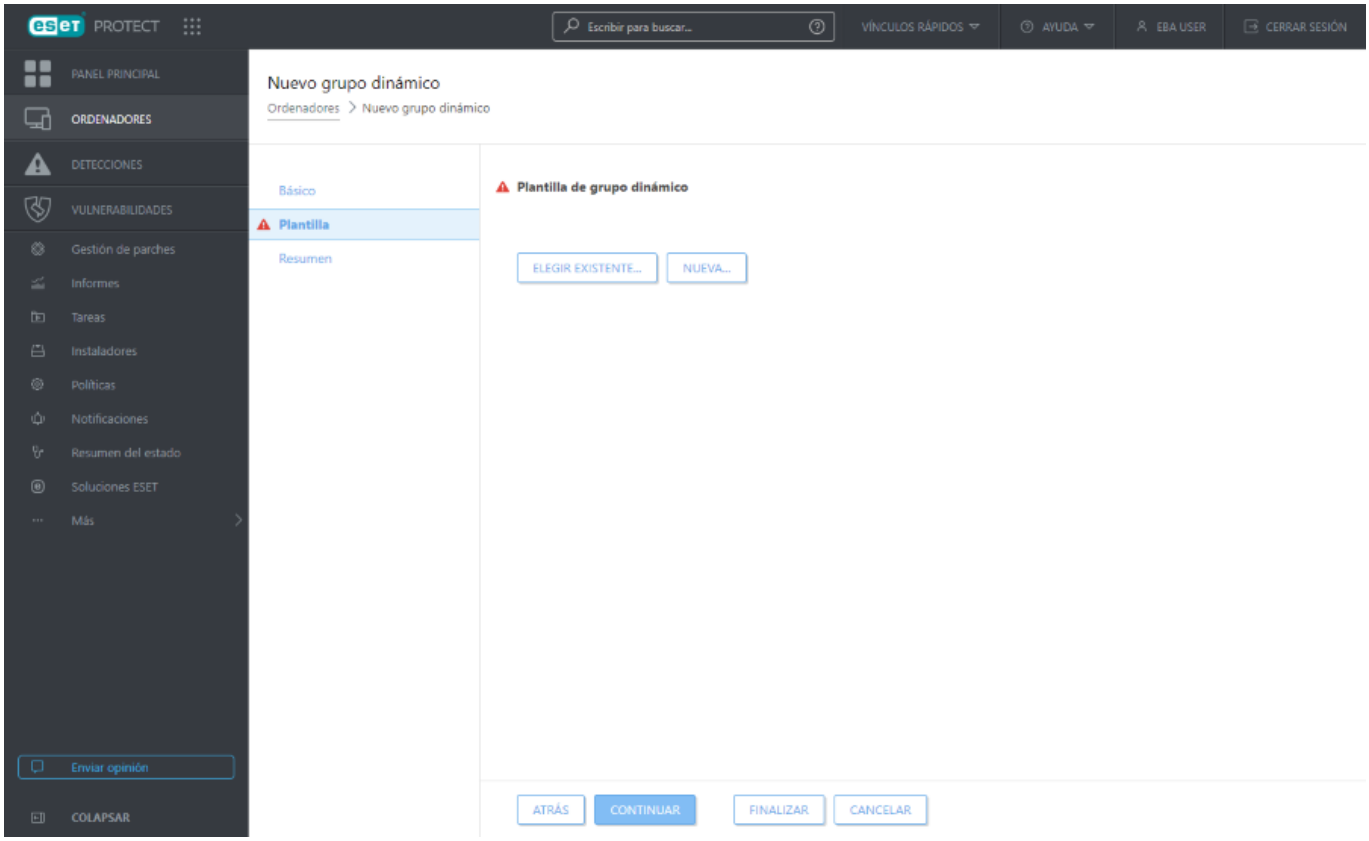
4. Haga clic en **Plantilla**. Todos los grupos dinámicos se crean a partir de una plantilla que define la forma en la que el grupo filtra los ordenadores cliente. A partir de una plantilla se puede crear un número de grupos dinámicos ilimitado.

> 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

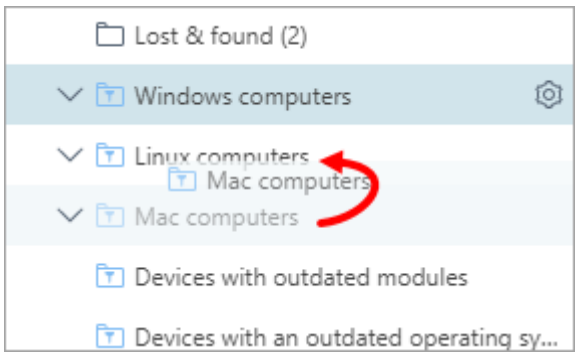
Un grupo dinámico puede ser miembro de cualquier otro grupo, incluidos los estáticos. Un grupo estático no se puede mover a un grupo dinámico. Tampoco es posible mover grupos estáticos predefinidos (por ejemplo, el grupo estático **Perdidos y encontrados**) a ningún otro grupo. Los demás grupos se pueden 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.

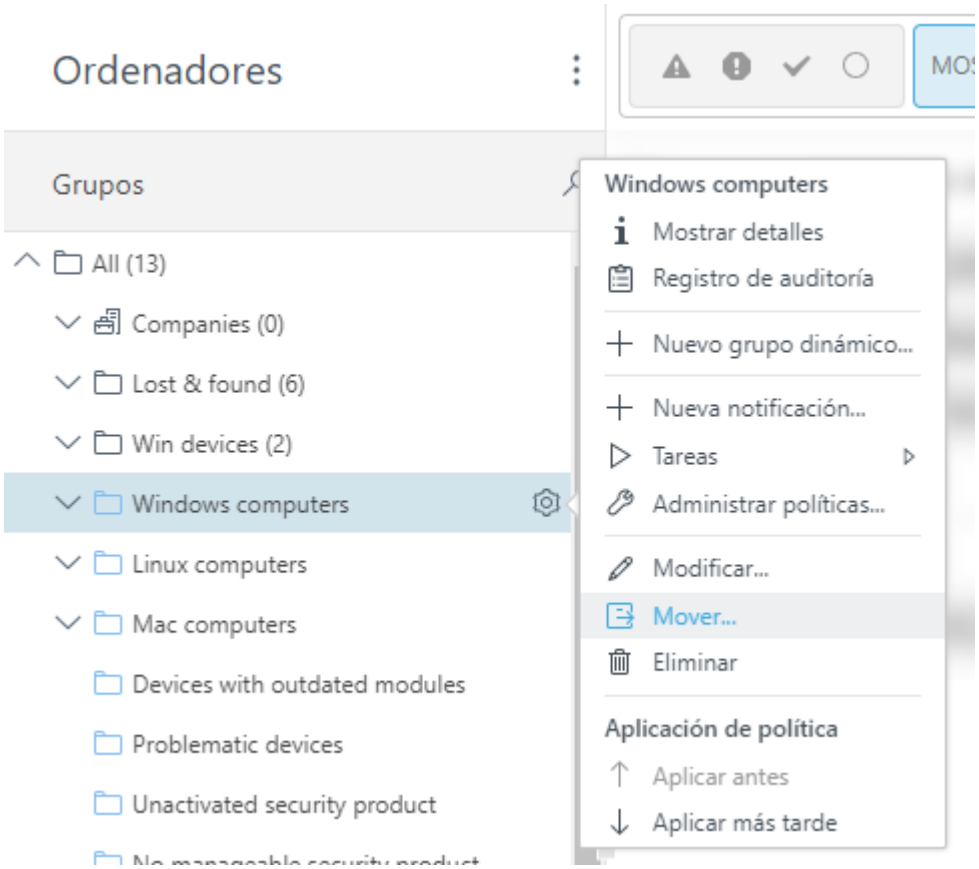
El grupo dinámico en una nueva posición comienza a filtrar los ordenadores (según la plantilla) sin ninguna relación con su ubicación anterior.

Un grupo se puede mover de tres formas:

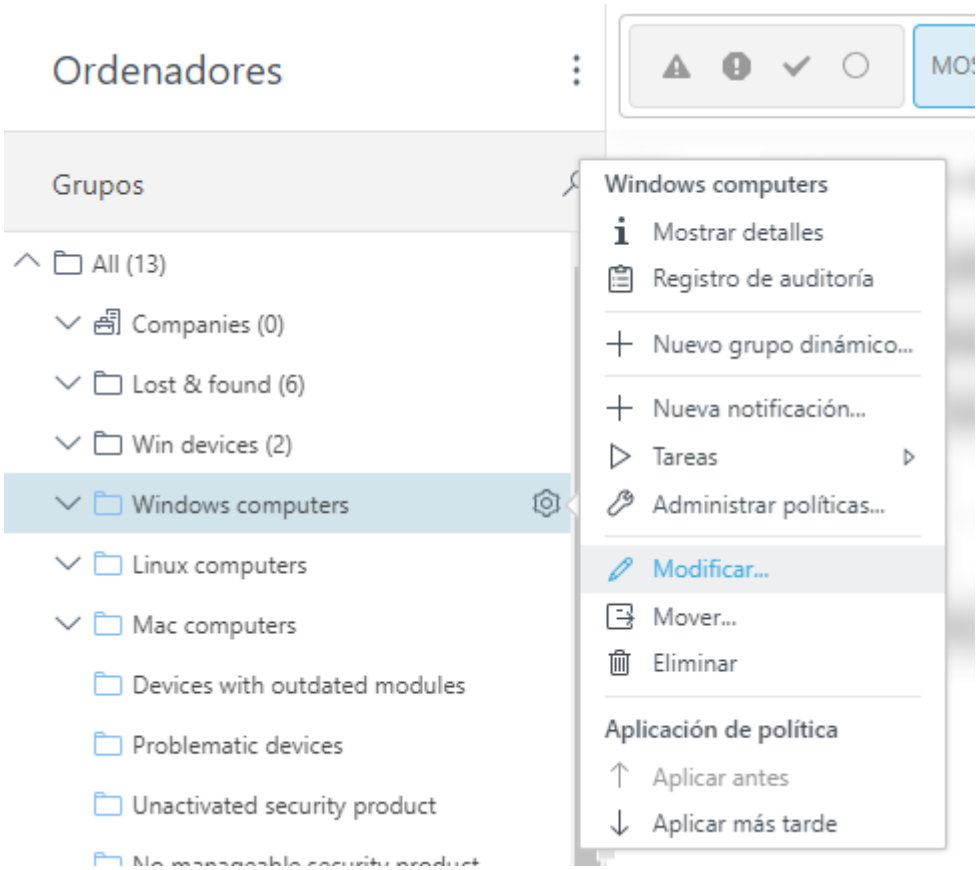
- **Arrastrar y soltar**: haga clic y mantenga pulsado el grupo que desea mover y suéltelo encima del grupo principal nuevo.



- Haga clic en el icono del engranaje > **Mover** > seleccione un grupo principal nuevo de la lista y haga clic en **Aceptar**.

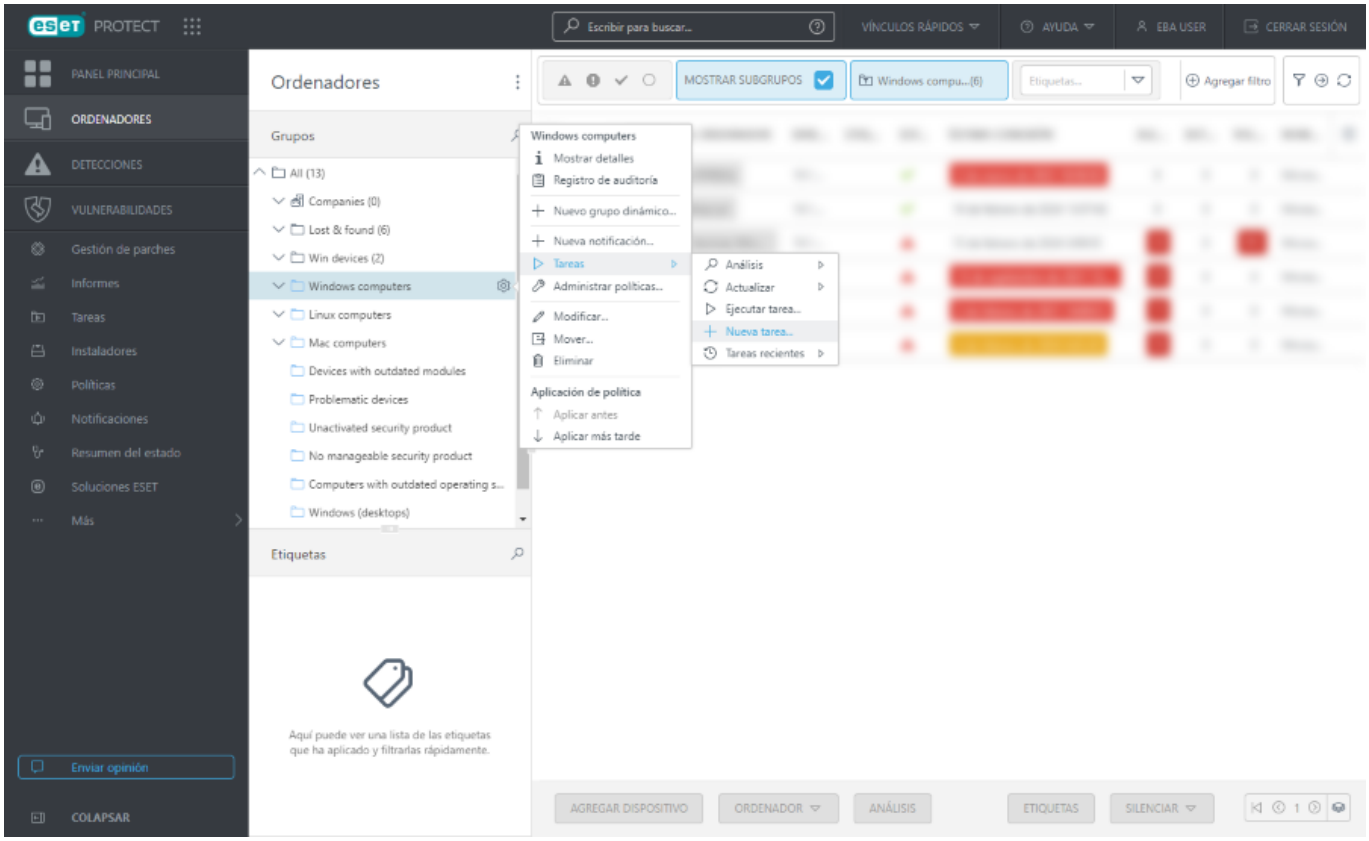


- Haga clic en el icono del engranaje > **Modificar >** seleccione **Cambiar el grupo principal**. Seleccione un grupo principal nuevo de la lista y haga clic en **Aceptar**.



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.

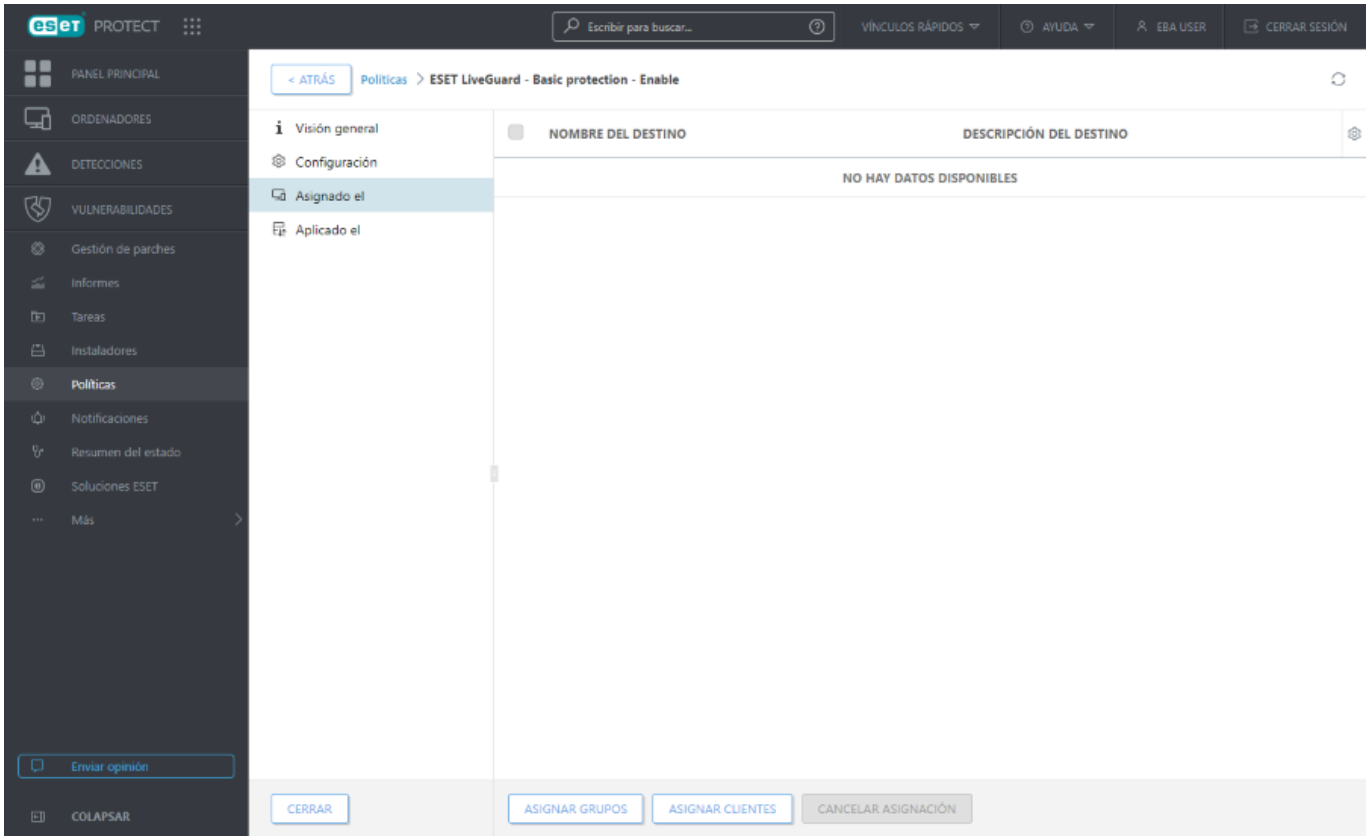


Asignar una política a un grupo

Después de crear una política, puede asignarla a un **grupo estático** o **dinámico**. Hay dos formas de asignar una política:

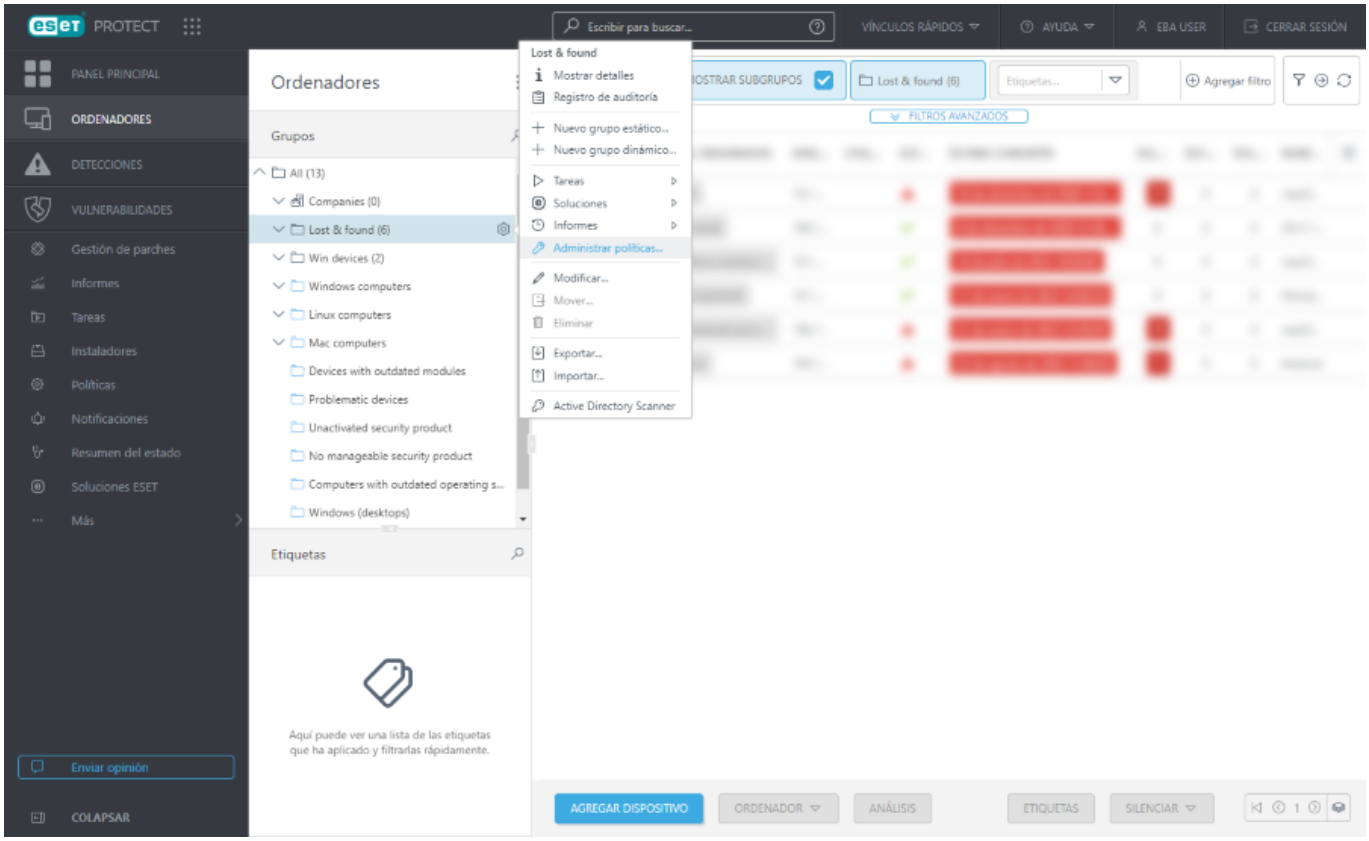
Método I.

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.

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**, **Firewall**, **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:
  - **desinfectado**: se ha desinfectado la detección.
  - **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.

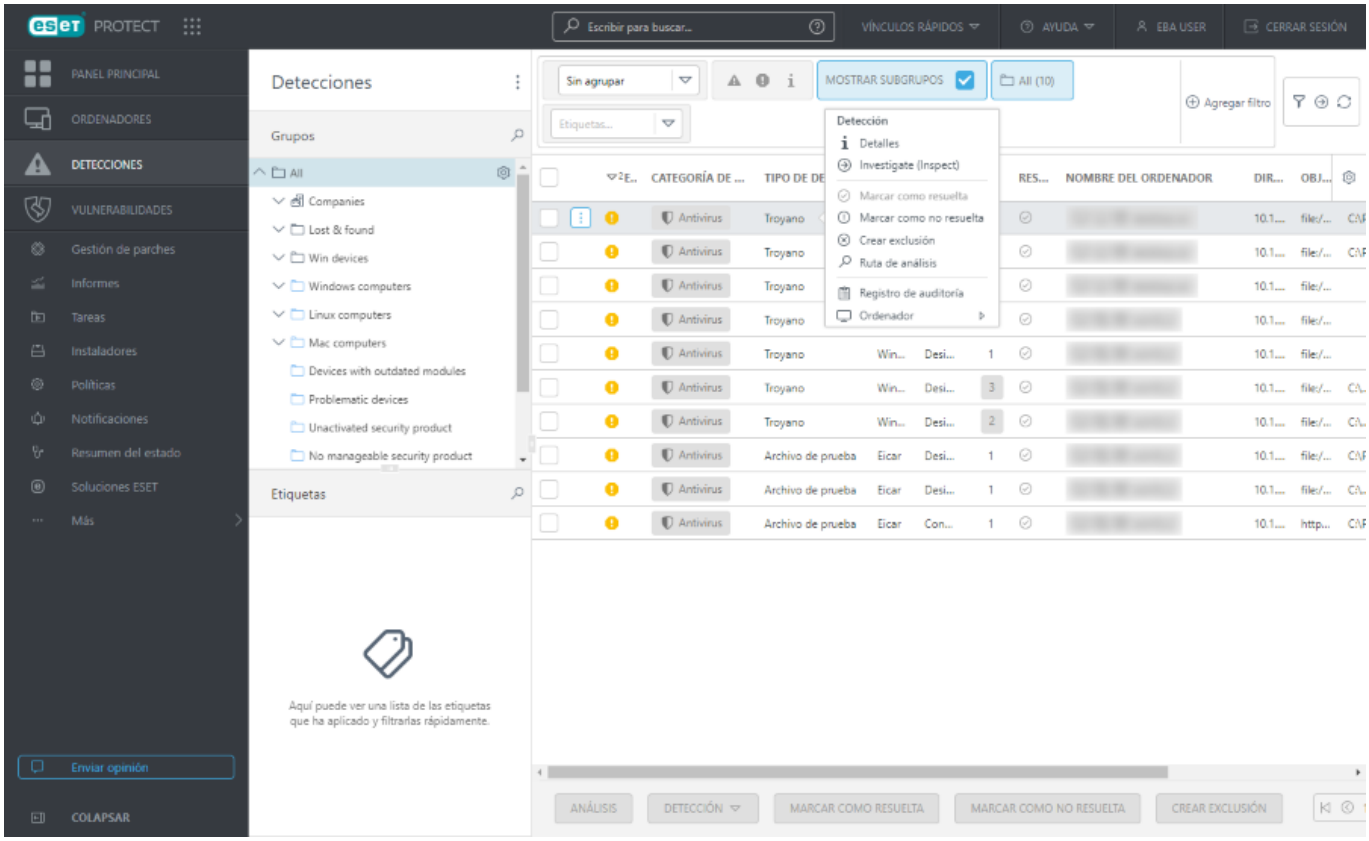
➢ En la configuración del motor de detección del producto de seguridad de ESET, el nivel de **Protección** de la categoría de detección está establecido en un valor inferior al nivel de **Informe**.

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:

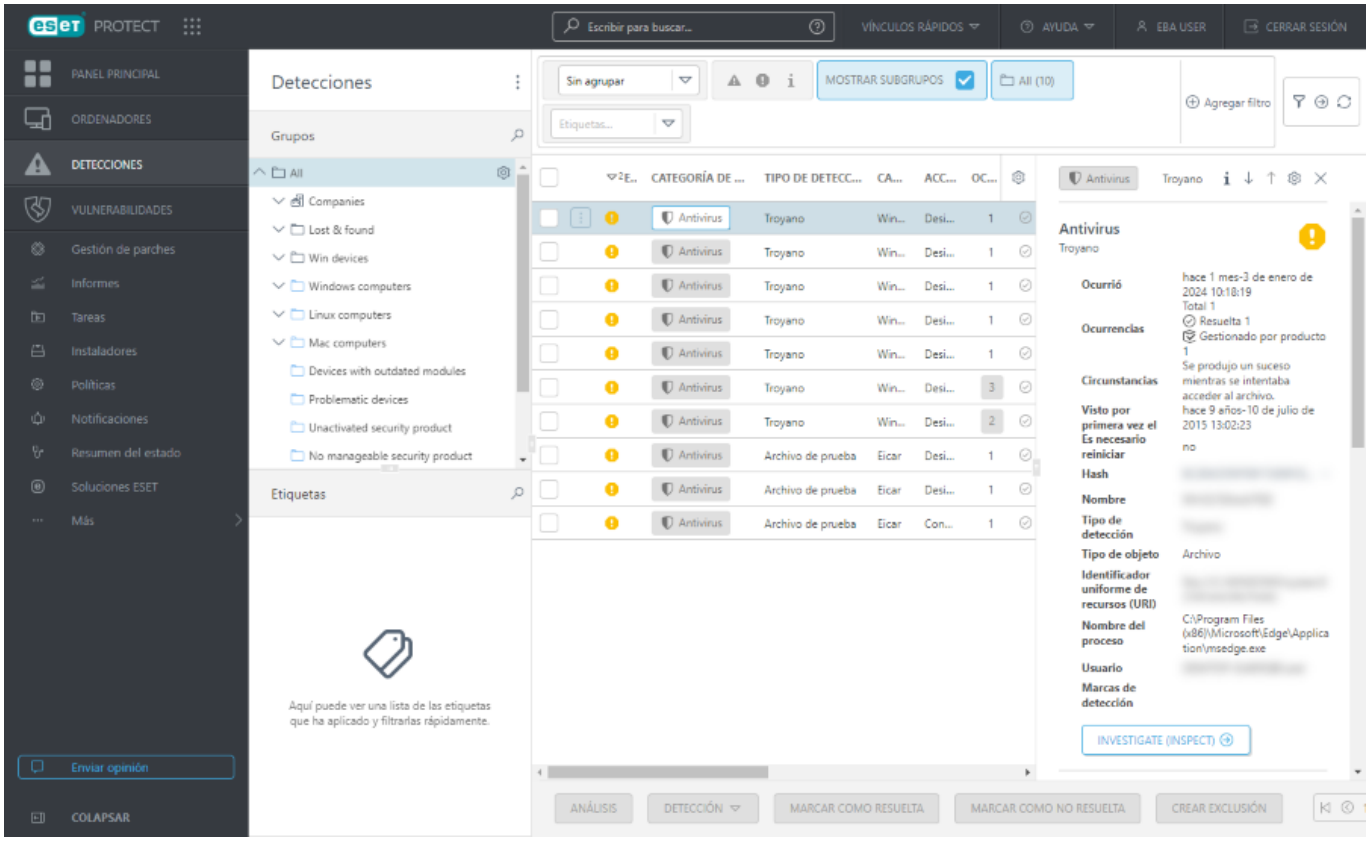
- **Análisis**: ejecuta la tarea Análisis a petición en el dispositivo desde el que se haya informado de la detección seleccionada.
- **Detalles**: vea los Detalles de la detección.
- **Ordenador**: una lista de acciones que puede realizar en el ordenador en el que se detectó la detección. Esta lista 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 Web Console. El icono **Inspect** de la parte superior derecha abre la ESET Inspect sección Detecciones de Web Console. El ESET Inspect solo está disponible cuando tiene la licencia de ESET Inspect y ESET Inspect está conectado a ESET PROTECT. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a 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.

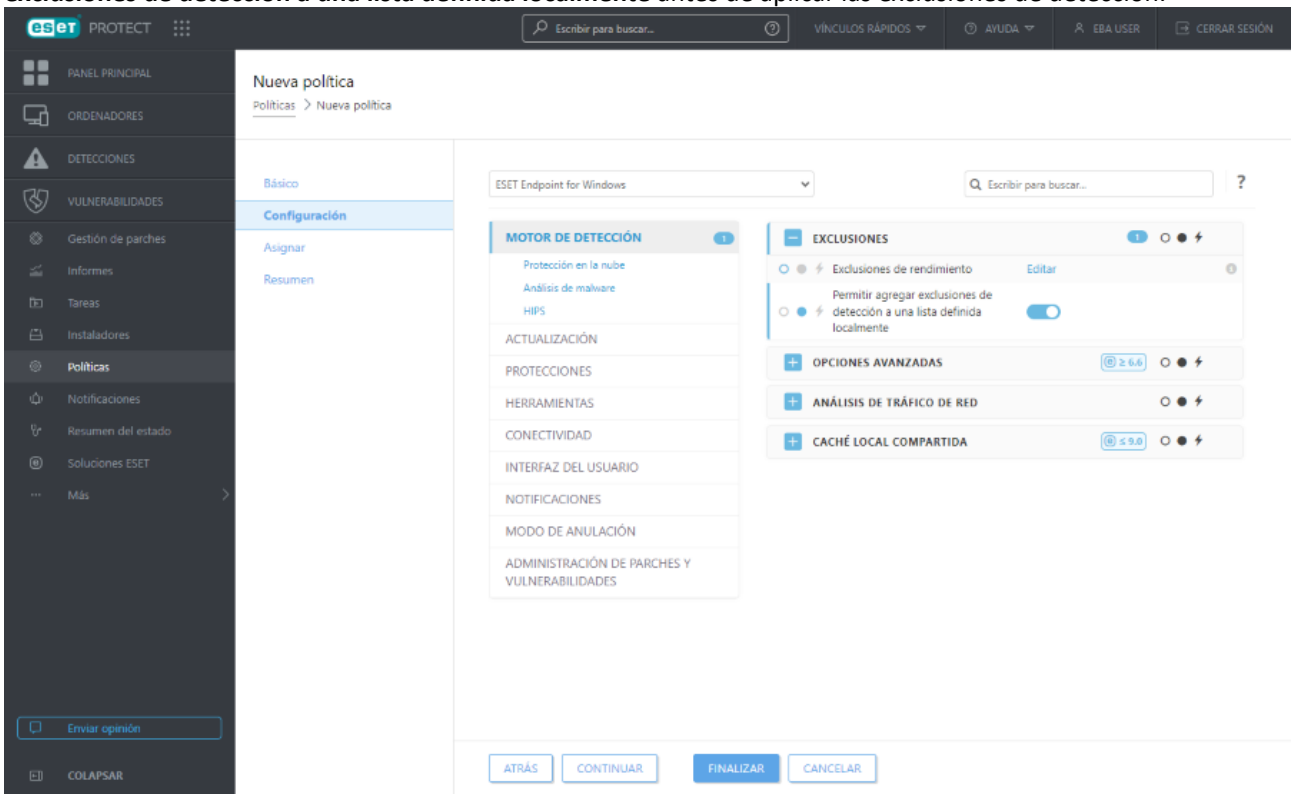
En ESET PROTECT hay dos categorías de exclusión de **Antivirus**:

- **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 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

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

ESET Inspect 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, su instalación y sus funciones, consulte la ayuda de ESET Inspect.

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

Puede activar ESET Inspect desde ESET Business Account. Necesita una licencia de ESET Inspect para activar ESET Inspect.

El ESET Inspect solo está disponible cuando tiene la licencia de ESET Inspect y ESET Inspect está conectado a ESET PROTECT. Un usuario de Web Console necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect**.

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** para implementar ESET Inspect Connector en los ordenadores Windows/Linux/macOS administrados.

Informes de detecciones de ESET Inspect en ESET PROTECT

ESET PROTECT no almacena ni muestra detecciones de ESET Inspect en Detecciones. Puede ver las estadísticas de las detecciones de ESET Inspect en **ESET PROTECT** > **Panel** > **ESET Inspect**.

Otro tipo de detecciones notificadas por ESET Inspect son **Archivos bloqueados**: los intentos bloqueados de iniciar ejecutables bloqueados en ESET Inspect (hashes bloqueados).

Haga clic en la detección y seleccione **Investigar (Inspect)** para ver los detalles de la detección en ESET Inspect Web Console.

Vulnerabilidades

La sección **Vulnerabilidades** proporciona una descripción general de las vulnerabilidades detectadas en los ordenadores. El ordenador se analiza para detectar cualquier software instalado vulnerable a riesgos de seguridad. El análisis automatizado con informes instantáneos para la consola le permite priorizar las vulnerabilidades en función de la gravedad, administrar los riesgos de seguridad y asignar recursos de manera eficaz. Una amplia gama de opciones de filtrado le permite identificar y afrontar los problemas de seguridad críticos.

Requisitos previos

Para ver y activar ESET Administración de revisiones y vulnerabilidades, asegúrese de que tiene uno de los siguientes niveles:

- ESET PROTECT Elite
- ESET PROTECT Complete
- ESET PROTECT MDR

Puede activar ESET Administración de revisiones y vulnerabilidades solo en equipos Windows que ejecuten:

- ESET Management Agent versión 10.1 o posteriores
- ESET Endpoint Security para Windows versión 10.1 o posteriores
- ESET Endpoint Antivirus para Windows versión 10.1 o posteriores
- ESET Server Security para Microsoft Windows Server versión 11.0 o posteriores

ESET Vulnerability & Patch Management no es compatible con los procesadores ARM.

Activar administración de parches y vulnerabilidades

1. Haga clic en **Ordenadores**.

2. Seleccione el ordenador o el grupo en los que desea activar la administración de vulnerabilidades y revisiones.

3. Seleccione **Soluciones** y haga clic en **Activar administración de vulnerabilidades y revisiones**.

4. En la ventana **Activar administración de vulnerabilidades y revisiones**:

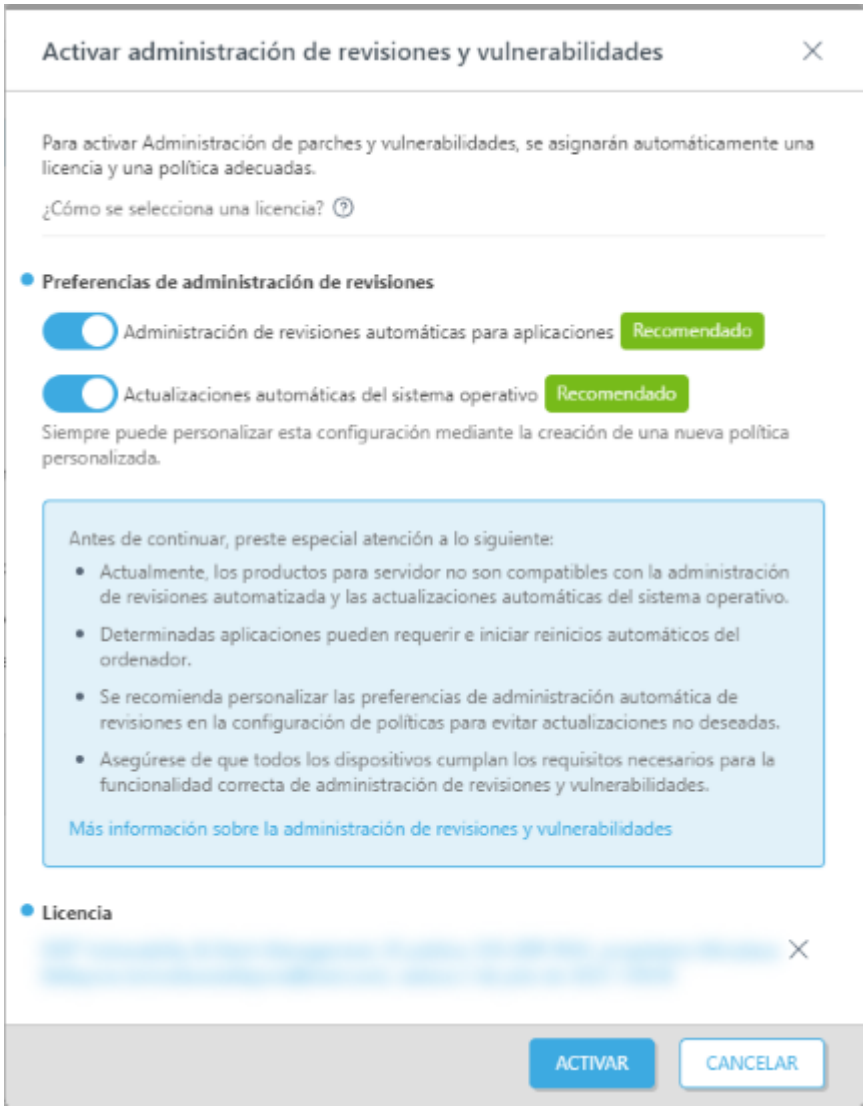
   a.Compruebe que el botón de alternancia **Administración de revisiones automáticas para aplicaciones** esté habilitado para aplicar automáticamente las revisiones que faltan a los ordenadores seleccionados.

   b.Compruebe que el botón de alternancia **Actualizaciones automáticas del sistema operativo** esté habilitado para aplicar automáticamente las actualizaciones del sistema operativo a los ordenadores seleccionados.

Las actualizaciones automáticas del sistema operativo solo están disponibles para ESET Endpoint para Windows 11.0 y versiones posteriores.

   c.La licencia está preseleccionada.

   d.Haga clic en el botón **Activar**.



Cuando la administración de vulnerabilidades y revisiones está activada:

- El icono de vulnerabilidades aparece junto al nombre del ordenador.
- Puede ver la ventana dinámica **Administración de vulnerabilidades y revisiones** con el estado **Activa** en los detalles del ordenador.

> Después de una actualización, algunas aplicaciones requieren reiniciar el ordenador y pueden reiniciar los ordenadores automáticamente.

> En el caso de algunas aplicaciones (por ejemplo, TeamViewer), se pueden ofrecer licencias para versiones específicas. Revise sus aplicaciones. Para evitar una actualización innecesaria, configure **Estrategia de aplicación automática de parches** > **Parchear todas las aplicaciones excepto las excluidas** cuando cree una política.

Ver Vulnerabilidades

Puede ver **Vulnerabilidades** desde varios lugares:

- Haga clic en **Vulnerabilidades** en el menú principal para abrir la sección **Vulnerabilidades** y ver una lista de vulnerabilidades.

- Haga clic en **Ordenadores** > haga clic en el ordenador y, a continuación, haga clic en **Detalles** > en la ventana dinámica **Administración de vulnerabilidades y revisiones**, haga clic en **Mostrar vulnerabilidades** para abrir la sección **Vulnerabilidades**.

- Haga clic en **Ordenadores** > en la columna **Vulnerabilidades**, y haga clic en el número de vulnerabilidades del ordenador seleccionado para abrir la sección **Vulnerabilidades**.

Agrupación de vulnerabilidades

Para agrupar las vulnerabilidades, seleccione en el menú desplegable:

- **Sin agrupar**: vista predeterminada

- **Agrupar por nombre de la aplicación**: las vulnerabilidades se agrupan por el nombre de la aplicación vulnerable, con números en **Dispositivos afectados** y **Vulnerabilidades**. Cuando se agrupen, haga clic en la fila de una aplicación y, a continuación, haga clic en **Mostrar vulnerabilidades** para mostrar las vulnerabilidades de la aplicación seleccionada.

- **Agrupar por CVE**: las vulnerabilidades se agrupan por el número CVE (Common Vulnerabilities and Exposure). Un CVE es un número de identificación de una vulnerabilidad. Cuando se agrupen, haga clic en la fila de un CVE y, a continuación, haga clic en **Mostrar dispositivos** para mostrar los dispositivos (ordenadores) con la vulnerabilidad.

Filtrado de la vista

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.

- **Nombre de la aplicación**: el nombre de la aplicación con la vulnerabilidad

- **Versión de la aplicación**: la versión de la aplicación

- **Proveedor de la aplicación**: el proveedor de la aplicación con la vulnerabilidad

- **Puntuación de riesgo**: puntuación de riesgo de la vulnerabilidad de 0 a 100

- **CVE**: un número CVE (Common Vulnerabilities and Exposure), que es un número de identificación de una vulnerabilidad

- **Nombre del ordenador**: el nombre del ordenador afectado; haga clic en el nombre del ordenador para ver los detalles del ordenador con la vulnerabilidad

- **Categoría**: categoría de la vulnerabilidad.

  - Vulnerabilidad de la aplicación

  - Vulnerabilidad del sistema operativo

- **Visto por primera vez**: la fecha y la hora de la primera detección de la vulnerabilidad en el dispositivo

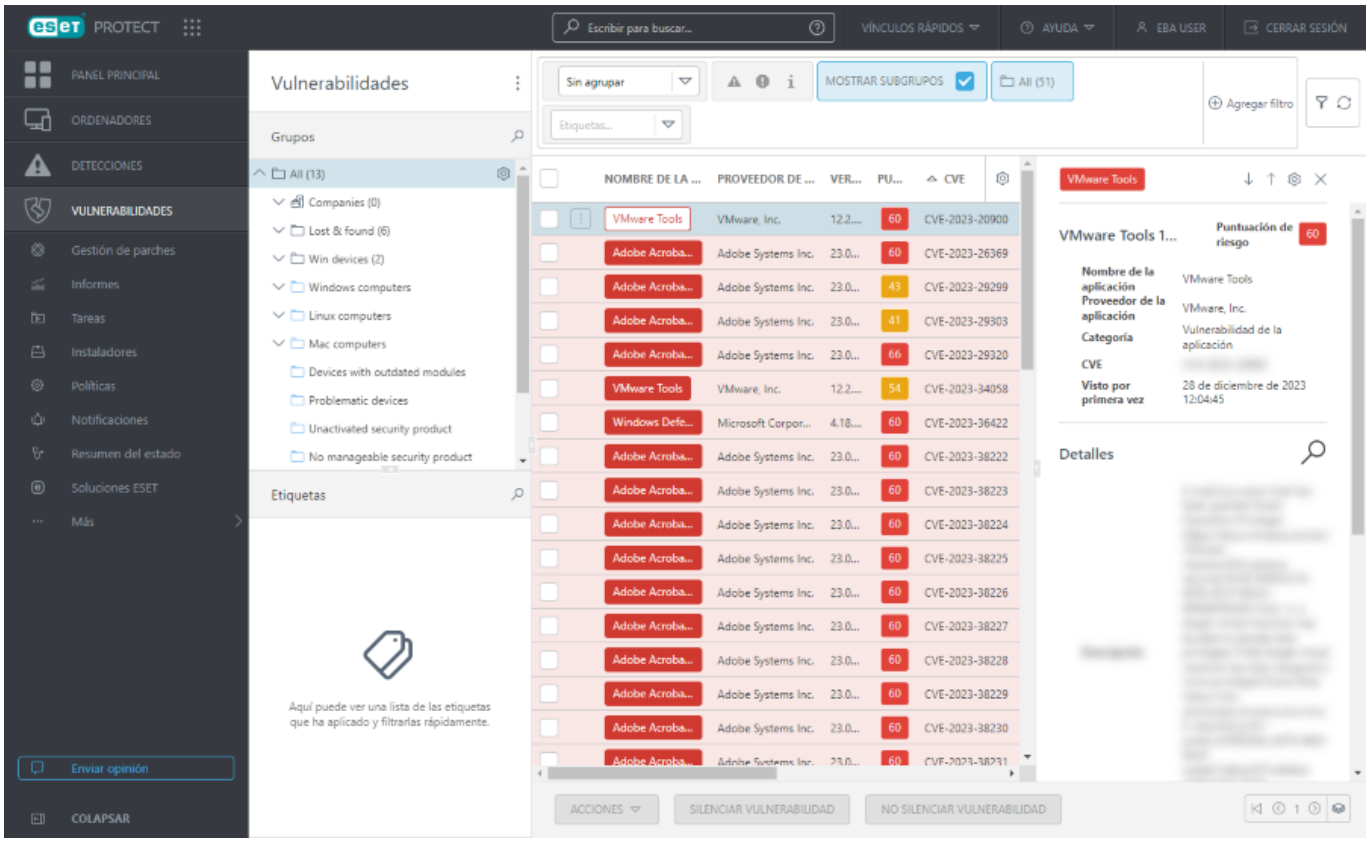
Puntuación de riesgo: evalúa la gravedad de las vulnerabilidades de seguridad del sistema informático. La puntuación de riesgo se calcula de la siguiente manera:
- CVSSv2/CVSSv3
- Popularidad de CVE: indica el nivel de actividad de vulnerabilidad.
- Tasa de riesgo comprometida: indica el número de dispositivos con vulnerabilidad confirmada.
- Ciclo de vida de CVE: indica el tiempo transcurrido desde que se notificó la vulnerabilidad por primera vez.

La puntuación de riesgo se indica con el siguiente código de colores:
- Gris (0–29): gravedad baja
- Amarillo (30–59): gravedad media
- Rojo (60–100): gravedad crítica

Vista previa de la vulnerabilidad

Haga clic en el nombre de una aplicación para ver los detalles de la vulnerabilidad en un panel lateral. La manipulación de la vista previa de la vulnerabilidad incluye:

- **Siguiente**: muestra la siguiente vulnerabilidad en el panel lateral de vista previa de la vulnerabilidad
- **Anterior**: muestra la anterior vulnerabilidad en el panel lateral de vista previa de la vulnerabilidad
- **Administrar el contenido de Detalles de vulnerabilidad**: administra cómo se muestran las secciones del panel lateral de vista previa de la vulnerabilidad y en qué orden
- **Cerrar**: cierra el panel lateral de vista previa de la vulnerabilidad



Para obtener más información, consulte la lista de aplicaciones cubiertas en Vulnerabilidades.

Silenciar vulnerabilidad/anular silenciamiento de vulnerabilidad

Puede silenciar la vulnerabilidad o anular el silenciamiento de la vulnerabilidad en los dispositivos:

- Haga clic en la fila del ordenador y, a continuación, haga clic en **Silenciar vulnerabilidad/Anular silenciamiento de vulnerabilidad**
- Seleccione el ordenador y haga clic en el botón **Silenciar vulnerabilidad/Anular silenciamiento de vulnerabilidad** en la parte inferior de la página
- Seleccione el ordenador, haga clic en el botón **Acciones** y, a continuación, seleccione **Silenciar vulnerabilidad/Anular silenciamiento de vulnerabilidad**

Análisis de vulnerabilidades

Puede iniciar un análisis inmediato de vulnerabilidades y falta de parches en un dispositivo específico:

- Haga clic en la fila del equipo y seleccione **Equipo** > **Análisis** > **Análisis de vulnerabilidades**
- Seleccione el equipo y haga clic en el botón **Acciones**. A continuación, seleccione **Equipo** > **Análisis** > **Análisis de vulnerabilidades**
- Seleccione cualquier grupo y haga clic en . A continuación, seleccione **Tareas** > **Análisis** > **Análisis de vulnerabilidades**

La tarea **Iniciar análisis de vulnerabilidades** se programa para ejecutarse lo antes posible.

La tarea puede exigir más recursos del dispositivo durante un máximo de 10 minutos.

Puede crear una plantilla de informe con datos de vulnerabilidad y, a continuación, agregar el informe al panel.

Para obtener más información, consulte Preguntas frecuentes sobre la administración de revisiones y vulnerabilidades.

Aplicaciones cubiertas por Vulnerabilidades

La lista de aplicaciones cubiertas por Vulnerabilidades solo está disponible en inglés.

Administración de revisiones

La administración de revisiones ayuda a garantizar que los sistemas y las aplicaciones estén protegidos contra vulnerabilidades conocidas. La sección Administración de revisiones muestra todas las revisiones disponibles para eliminar las vulnerabilidades detectadas y facilita el proceso de corrección mediante actualizaciones de software automatizadas. Con las opciones de administración de revisiones, puede asegurarse rápidamente de que sus puntos de acceso estén actualizados con las revisiones de seguridad más recientes.

Requisitos previos

Para ver y activar ESET Administración de revisiones y vulnerabilidades, asegúrese de que tiene uno de los siguientes niveles:

- ESET PROTECT Elite
- ESET PROTECT Complete
- ESET PROTECT MDR

Puede activar ESET Administración de revisiones y vulnerabilidades solo en equipos Windows que ejecuten:

- ESET Management Agent versión 10.1 o posteriores
- ESET Endpoint Security para Windows versión 10.1 o posteriores
- ESET Endpoint Antivirus para Windows versión 10.1 o posteriores
- ESET Server Security para Microsoft Windows Server versión 11.0 o posteriores

ESET Vulnerability & Patch Management no es compatible con los procesadores ARM.

ESET Bridge usuarios

De forma predeterminada, ESET Bridge bloquea el tráfico de red de Administración de revisiones. ESET Bridge no afecta a la notificación de vulnerabilidades.

Para habilitar el tráfico de red de Administración de revisiones, deshabilite las reglas de la Lista de control de acceso (ACL) en el archivo de configuración de ESET Bridge:

1.Abra el archivo *restrict.conf.template* de configuración de ESET Bridge en un editor de texto:
*o*Windows: *C:\ProgramData\ESET\Bridge\Proxies\Nginx\Conf\restrict.conf.template*
*o*Linux: */var/opt/eset/bridge/nginx/conf/restrict.conf.template*
2.Cambie `set $valid_host 0;` a `set $valid_host 1;`.
3.Guarde el archivo *restrict.conf.template*.
4.Reinicie el servicio ESET Bridge.

Deshabilitar las reglas de la ACL permite redirigir todo el tráfico de red a través de ESET Bridge (ESET Bridge se convierte en un proxy abierto).

Administración de revisiones se activa durante la activación de la administración de vulnerabilidades y revisiones.

Ver Administración de revisiones

Puede ver Administración de revisiones desde varios lugares:

- Haga clic en **Administración de revisiones** en el menú principal para abrir la sección **Administración de revisiones** y ver una lista de revisiones

- Haga clic en **Ordenadores** > seleccione **Detalles** > en la ventana dinámica **Administración de vulnerabilidades y revisiones**, haga clic en **Mostrar revisiones** para abrir la sección **Administración de revisiones**

Agrupar la vista

Para agrupar las revisiones, seleccione en el menú desplegable:

- **Sin agrupar**: vista predeterminada

- **Agrupar por nombre de la aplicación**: cuando se agrupen, haga clic en la fila de una aplicación y, a continuación, haga clic en **Mostrar dispositivos** para mostrar los dispositivos (ordenadores) en los que se aplicará una revisión

Filtrado de la vista

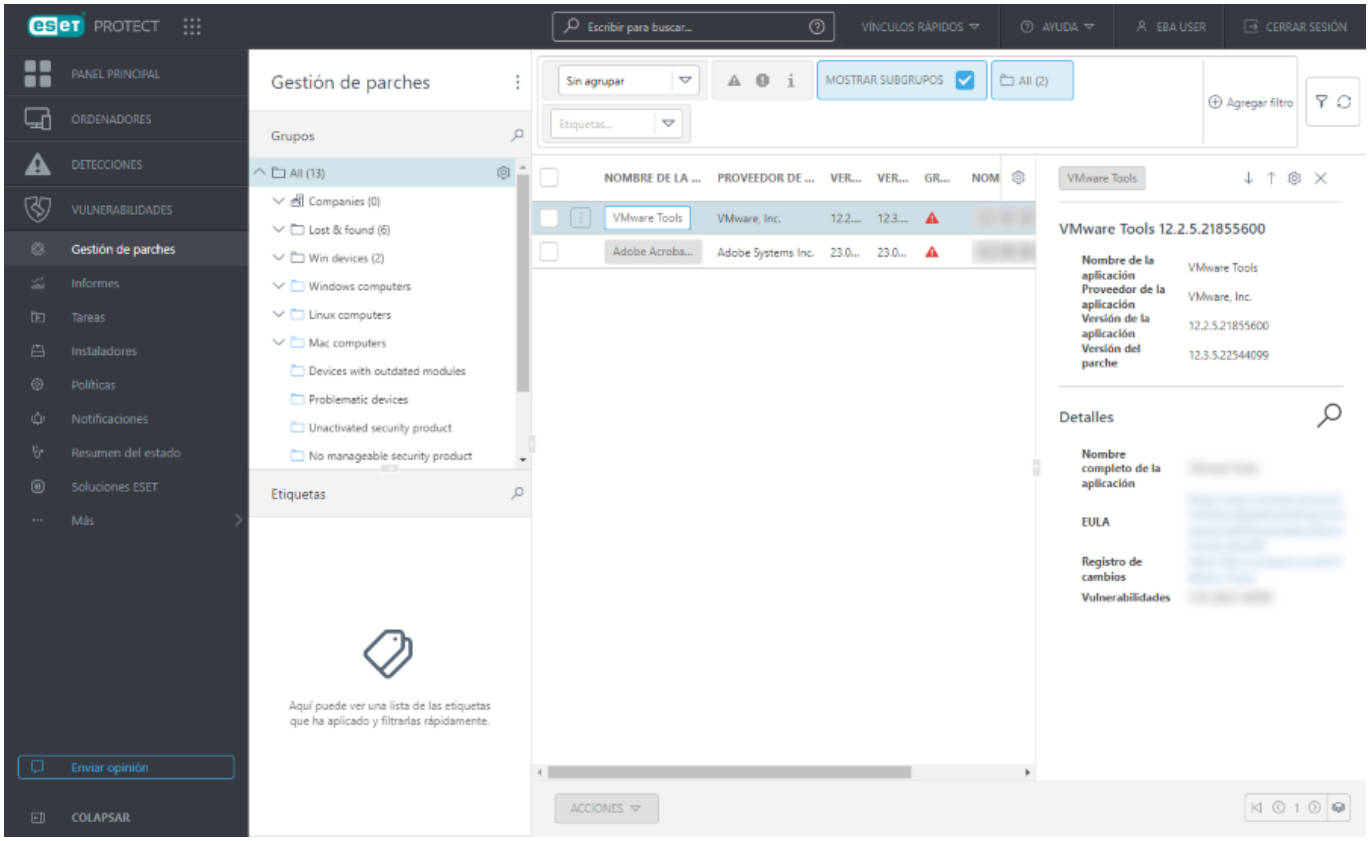
Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Entrar**. Los filtros activos aparecen resaltados en color azul.

- **Nombre de la aplicación**: el nombre de la aplicación con la vulnerabilidad
- **Versión de la aplicación**: la versión de la aplicación que causa la vulnerabilidad
- **Versión de la revisión**: la versión de la revisión
- **Gravedad**: nivel de gravedad, incluidos el informativo, el de advertencia o el crítico
- **Nombre del ordenador**: el nombre del ordenador afectado
- **Proveedor de la aplicación**: el nombre del proveedor de la aplicación

Panel lateral con detalles

Haga clic en el nombre de una aplicación para ver los detalles de la aplicación en un panel lateral. Manipulación de la vista previa del Aplicación:

- **Siguiente**: muestra los detalles de la siguiente aplicación en el panel lateral
- **Anterior**: muestra los detalles de la anterior aplicación en el panel lateral
- **Administrar el contenido de Detalles de revisión**: administra cómo se muestran las secciones del panel lateral y en qué orden
- **Cerrar**: cierra el panel lateral



Implementar revisiones

Solo puede aplicar revisiones en las aplicaciones seleccionadas.

Le recomendamos que active la administración de revisiones automática mediante una política.

Puede activar las actualizaciones automáticas del sistema operativo y seleccionar los niveles de gravedad para aplicar las actualizaciones del sistema operativo mediante una política.
Las actualizaciones automáticas del sistema operativo solo están disponibles para ESET Endpoint para Windows 11.0 y versiones posteriores.

Cuando se configura la administración de revisiones automática, la solución administrará automáticamente las revisiones de las aplicaciones durante el mantenimiento.

Después de una actualización, algunas aplicaciones requieren reiniciar el ordenador y pueden reiniciar los ordenadores automáticamente.

En el caso de algunas aplicaciones (por ejemplo, TeamViewer), se pueden ofrecer licencias para versiones específicas. Revise sus aplicaciones. Para evitar una actualización innecesaria, configure **Estrategia de aplicación automática de parches** > **Parchear todas las aplicaciones excepto las excluidas** cuando cree una política.

Otra opción es implementar las revisiones mediante:

- Seleccione las aplicaciones en las que desea implementar las revisiones > haga clic en el botón **Acciones** y, a continuación, haga clic en **Actualizar**.

- Para administrar las revisiones de una aplicación en todos los dispositivos afectados, aplique la vista **Agrupar por nombre de la aplicación**, seleccione la fila del nombre de la aplicación, haga clic en ⋮ y, a

continuación, haga clic en **Actualizar**.

Al implementar actualizaciones con el botón **Actualizar**, se creará automáticamente la nueva tarea de cliente **Aplicar revisión de aplicación** en Tareas. Para los equipos, las revisiones se aplicarán en función del planificador de Administración de revisiones y vulnerabilidades configurado en Políticas. Para los servidores, las revisiones se instalarán después de una cuenta atrás de 60 segundos sin opción de posponerlas.

Para obtener más información, consulte Preguntas frecuentes sobre la administración de revisiones y vulnerabilidades.

Aplicaciones cubiertas por Administración de revisiones

La lista de aplicaciones cubiertas por Administración de revisiones solo está disponible en inglés.

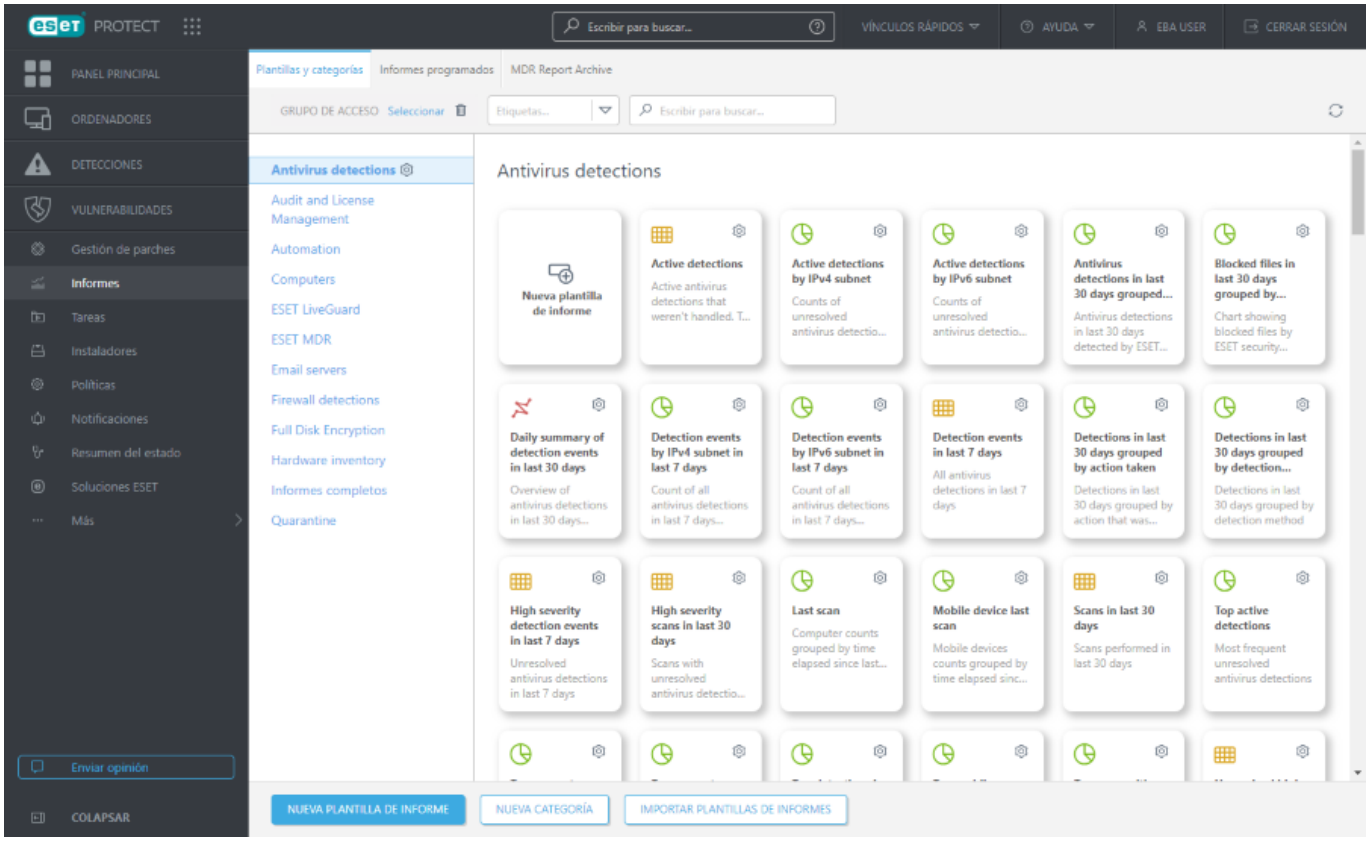
Informes

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.

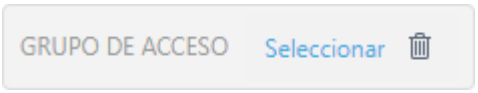
- **Archivo de informes de MDR**: esta pestaña muestra un resumen de los informes de ESET MDR.



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**

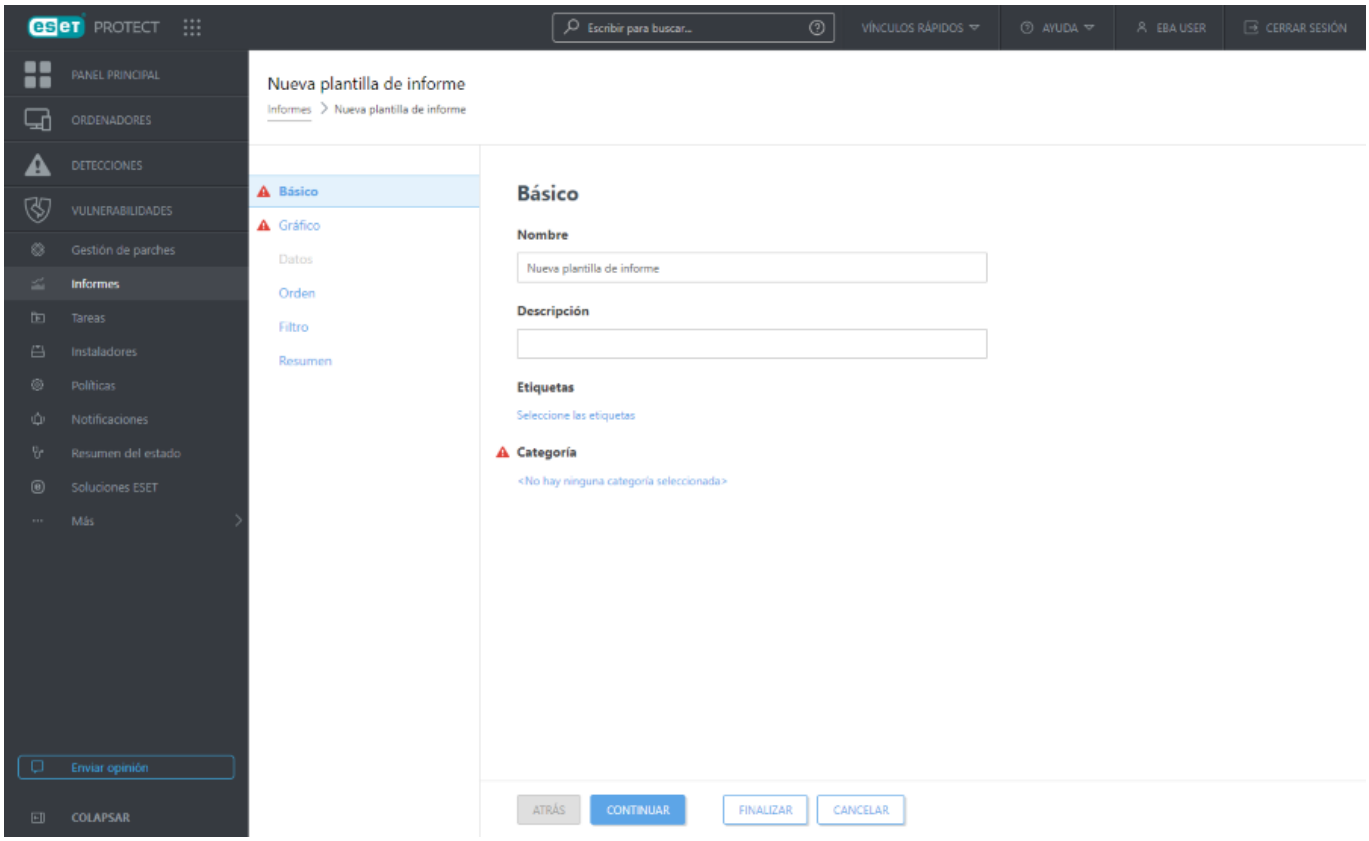
estados del ordenador, solo habrá datos de los ordenadores de los que tenga permiso de **Lectura**.

- **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**.

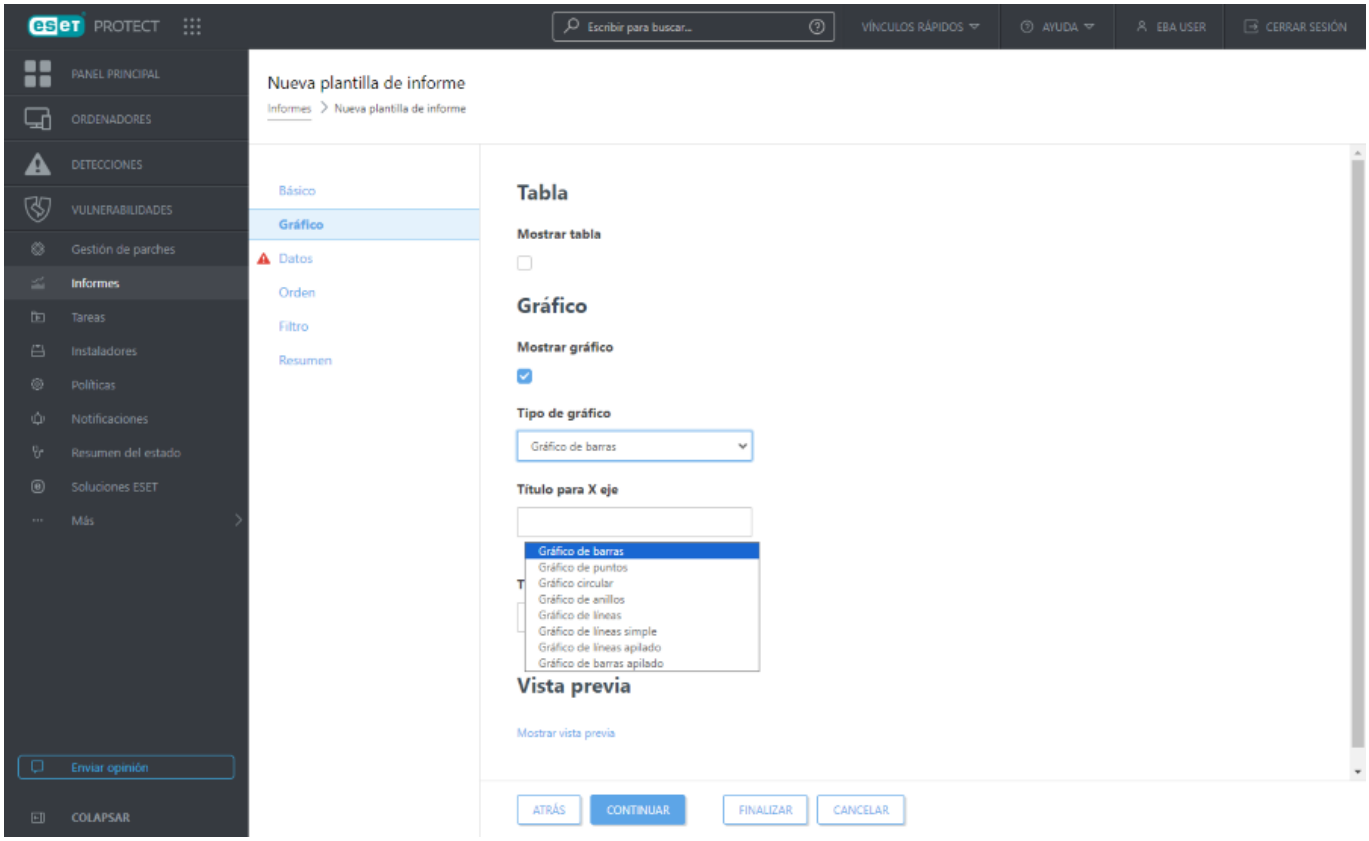
Crear una nueva plantilla de informe

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.

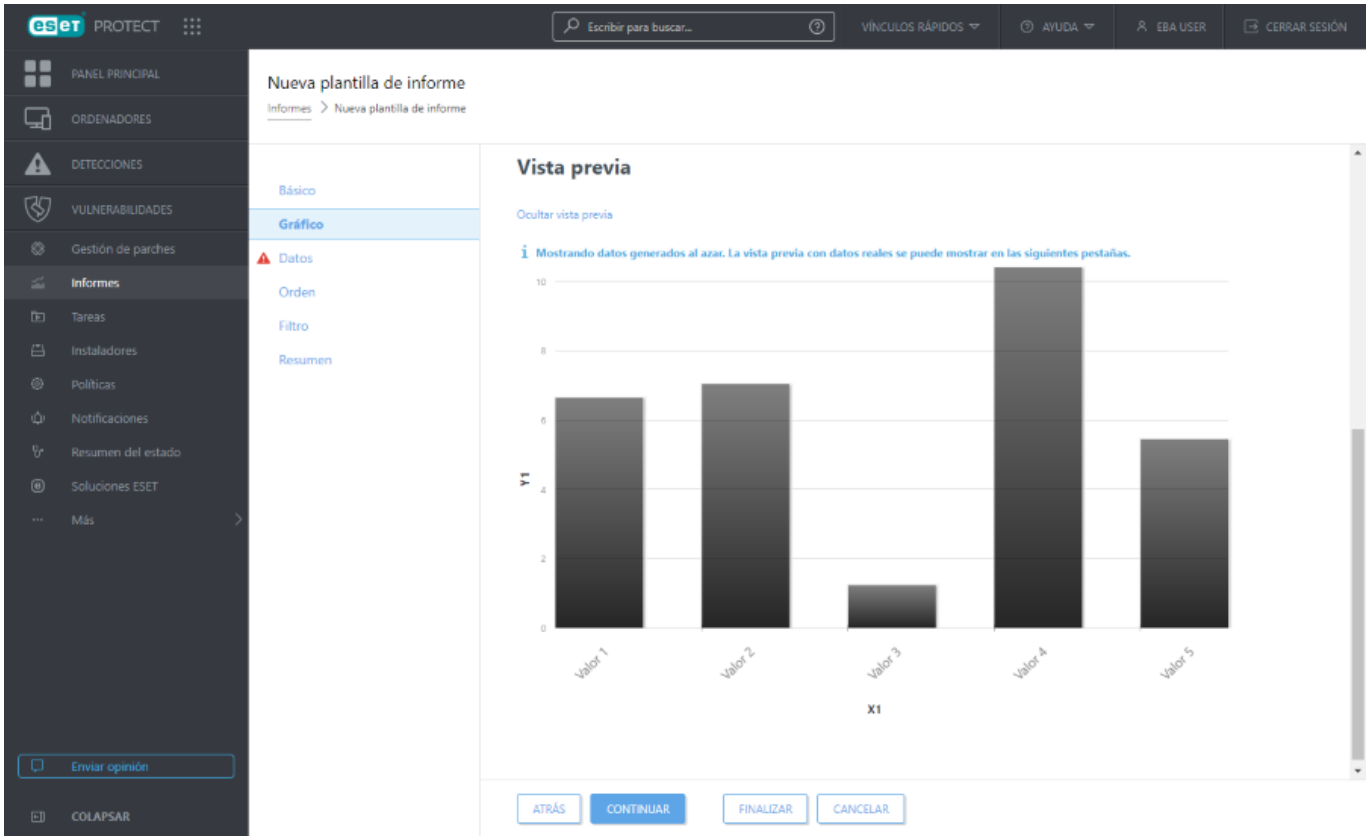
el tipo de gráfico seleccionado se mostrará en la sección **Vista previa**. De esta forma puede ver el aspecto del informe en tiempo real.

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:

- 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.

  - Configure 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.

Necesita una licencia de ESET Inspect para generar el informe de MDR. 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.

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 mensaje de correo electrónico.
- Si lo desea, defina los parámetros de desencadenadores y límites.

El tamaño máximo de correo electrónico permitido por la infraestructura de ESET PROTECT es 30 MB.

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.

ESET MDR

ESET MDR proporciona un resumen de los incidentes y las detecciones de ESET Inspect. Para usar ESET MDR, necesita una licencia de ESET Inspect y el nivel de **ESET PROTECT MDR**.

> **Disponibilidad por país de ESET MDR**
> ESET MDR está disponible en los siguientes países: EE. UU., Canadá, Japón, Reino Unido, Países Bajos, Francia, Italia, Alemania, Austria, Suiza, Suecia, Noruega, Dinamarca, Finlandia, Islandia, Eslovaquia, República Checa y Ucrania.

El servicio de ESET MDR cubre todos los dispositivos administrados que ejecutan archivos de ESET Inspect. Siga los pasos que se indican a continuación para seleccionar los dispositivos donde desea administrar la seguridad, independientemente del servicio de ESET MDR:

1. Abra ESET PROTECT y vaya a **Equipos**.
2. Haga clic en el icono de engranaje situado junto al grupo primario estático existente y seleccione **Nuevo grupo estático**.
3. Escriba `exempt` en el campo **Nombre** y haga clic en **Finalizar**.
4. Seleccione el grupo principal y los dispositivos que desea incluir en el grupo exempt.
5. Haga clic en **Equipo** > **Administrar** > **Mover a grupo** y seleccione el grupo `exempt`.

Usted administra los dispositivos del grupo `exempt`: puede controlar los incidentes de forma manual sin las acciones de respuesta aplicadas automáticamente.

Consulte también el panel de ESET MDR.

ESET MDR informe

El informe de **ESET MDR** es un resumen semanal de información relevante para la seguridad de distintas fuentes de la red.

Necesita los siguientes conjuntos de permisos para programar el informe de ESET MDR:
- **Informes de ESET MDR**: escribir
- **Tareas y desencadenadores de servidor**. **Generar informe**: usar, escribir

Tras activar la licencia de ESET PROTECT MDR, se programa automáticamente una tarea del servidor con el correo electrónico asignado al administrador.

Los destinatarios recibirán el **informe semanal de ESET MDR** automáticamente.

1. Haga clic en **Informes** y selecciona la pestaña **Categorías y plantillas** > **ESET MDR**.
2. Haga clic en el icono de engranaje **Acciones** en **Informe semanal de ESET MDR** y haga clic en **Programar**.
3. Haga clic en **Seleccionar etiquetas** para asignar etiquetas al informe. Haga clic en **Continuar**.
4. Seleccione el idioma del informe en el menú desplegable **Configuración regional** y la zona horaria en el menú desplegable **Zona horaria**. El menú desplegable**Tipo de desencadenador** está desactivado. La opción Semanal (todos los lunes) se selecciona automáticamente.
5. Escriba la dirección de correo electrónico del destinatario en el campo **Enviar a**.
6. También puede seleccionar **Personalizar mensaje** y escribir el **asunto** y el cuerpo del **mensaje**.
7. Haga clic en **Finalizar**.

También puede crear el **informe semanal de ESET MDR** tras ejecutar la tarea del servidor Generar informe:

1. Seleccione **Tareas** > **Nueva** > **Tarea del servidor**.
2. Seleccione **Generar informe** en el menú desplegable **Tarea** y haga clic en **Continuar**.
3. Haga clic en **Agregar plantilla de informe** y seleccione **Informe semanal de ESET MDR**.
4. Escriba la dirección de correo electrónico del destinatario en el campo **Enviar a**.
5. También puede seleccionar **Personalizar mensaje** y escribir el **asunto** y el cuerpo del **mensaje**.
6. Haga clic en **Continuar**.
7. Seleccione el idioma del informe en el menú desplegable **Configuración regional** y la zona horaria en el menú desplegable **Zona horaria**. El menú desplegable**Tipo de desencadenador** está desactivado. La opción Semanal (todos los lunes) se selecciona automáticamente.
8. Haga clic en **Continuar**.

9. Compruebe la configuración en **Resumen** y haga clic en **Finalizar**.

Recibirá el informe semanal de ESET MDR como un archivo .pdf.
El informe semanal de ESET MDR se genera todos los lunes con un nivel de ESET PROTECT MDR activo.

Archivo de informe MDR

El **archivo de informes de MDR** contiene todos los informes de ESET MDR enviados por correo electrónico. Recibirá un correo electrónico con un enlace al informe y podrá volver a consultar cualquier informe de ESET MDR generado en el último año.

Puede ver el archivo de informes de ESET MDR en la pestaña **Informes** > **Archivo de informes de MDR**.

Requisitos previos
Puede ver el archivo de informes tras configurar un derecho de **uso** en los conjuntos de permisos para **Informes de ESET MDR** y:
- haber activado la licencia de ESET PROTECT MDR y ESET Inspect
- su licencia de ESET PROTECT MDR ha caducado, pero tiene al menos un informe programado y entregado en el último año

Diseño del panel lateral

Haga clic en el icono ⋮ situado junto al nombre del **archivo de informes de MDR** y ajuste el diseño del panel lateral con el menú contextual:

- **Ocultar panel lateral**
- **Etiquetas**

Filtro del archivo de informes de MDR

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 agregar:

- **Período desde**: haga clic en el campo para seleccionar la fecha de inicio del filtro
- **Período hasta**: haga clic en el campo para seleccionar la fecha de cierre del filtro

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.

Administración del archivo de informes de MDR

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

Para clasificar por una sola columna (**Hora de creación**/**Período desde**/**Período hasta**), 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.

Haga clic en el icono del engranaje para administrar el archivo de informes:

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 de creación** y pase el ratón por encima de los datos de **Hora de creación** para ver el tiempo relativo/absoluto.

Clasificación de tablas

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

Columnas del archivo de informes de MDR

El archivo de informes de MDR contiene las siguientes columnas:

Tipo de informe: el tipo de informe (semanal)

Usuarios notificados: la dirección de correo electrónico del usuario que recibió el informe de ESET MDR

Configuración regional: el idioma del informe de ESET MDR

Hora de creación: la fecha en que se generó el informe de ESET MDR

Período desde: la fecha de inicio de los datos registrados en el informe de ESET MDR

Período hasta: la fecha de cierre de los datos registrados en el informe de ESET MDR

Zona horaria: la zona horaria del informe de ESET MDR

Acciones del archivo de informes

Haga clic en el informe para seleccionar una de las acciones:

- **Descargar**: descargue el informe como un archivo *.pdf*
- **Enviar por correo electrónico**: envíe el informe como archivo adjunto en un correo electrónico. Puede seleccionar el **idioma de correo electrónico** en el menú desplegable y hacer clic en el botón **Agregar** para agregar las **direcciones de correo electrónico** y elegir los destinatarios. También puede hacer clic en el botón **Más** para **agregar usuarios** (agregue la dirección de los usuarios del equipo), **importar CSV** (importe una lista personalizada de direcciones de un archivo *.csv* estructurado con delimitadores) o **pegar desde el portapapeles** (importe una lista personalizada de direcciones separadas con delimitadores personalizados; esta función es similar a la importación de CSV). Tras hacer clic en **Enviar**, el informe se enviará como un archivo adjunto a la dirección de correo electrónico seleccionada.

> **Registros en el archivo de informes de MDR**
> Los informes de ESET MDR se conservan en el archivo de informes de MDR durante un año.

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 Actualizar agente para actualizar ESET Management Agent.
- 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**.

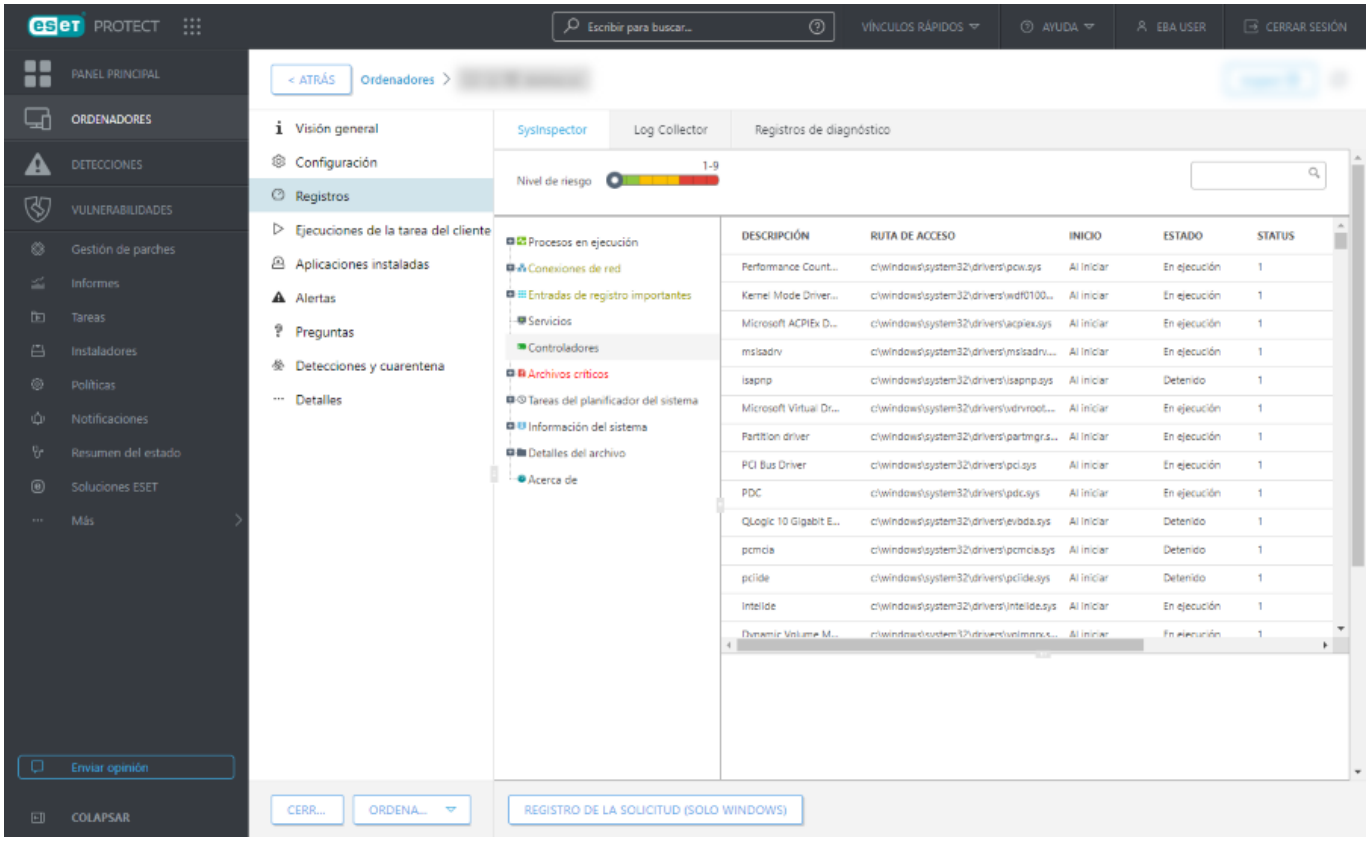
3.Abra el informe, seleccione un ordenador y, a continuación, seleccione **Abrir vista del registro de SysInspector** en el menú desplegable.

Desde el menú Ordenadores

1.Desplácese hasta Ordenadores.

2.Seleccione un ordenador en un grupo estático o dinámico, y haga clic en **Mostrar detalles**.

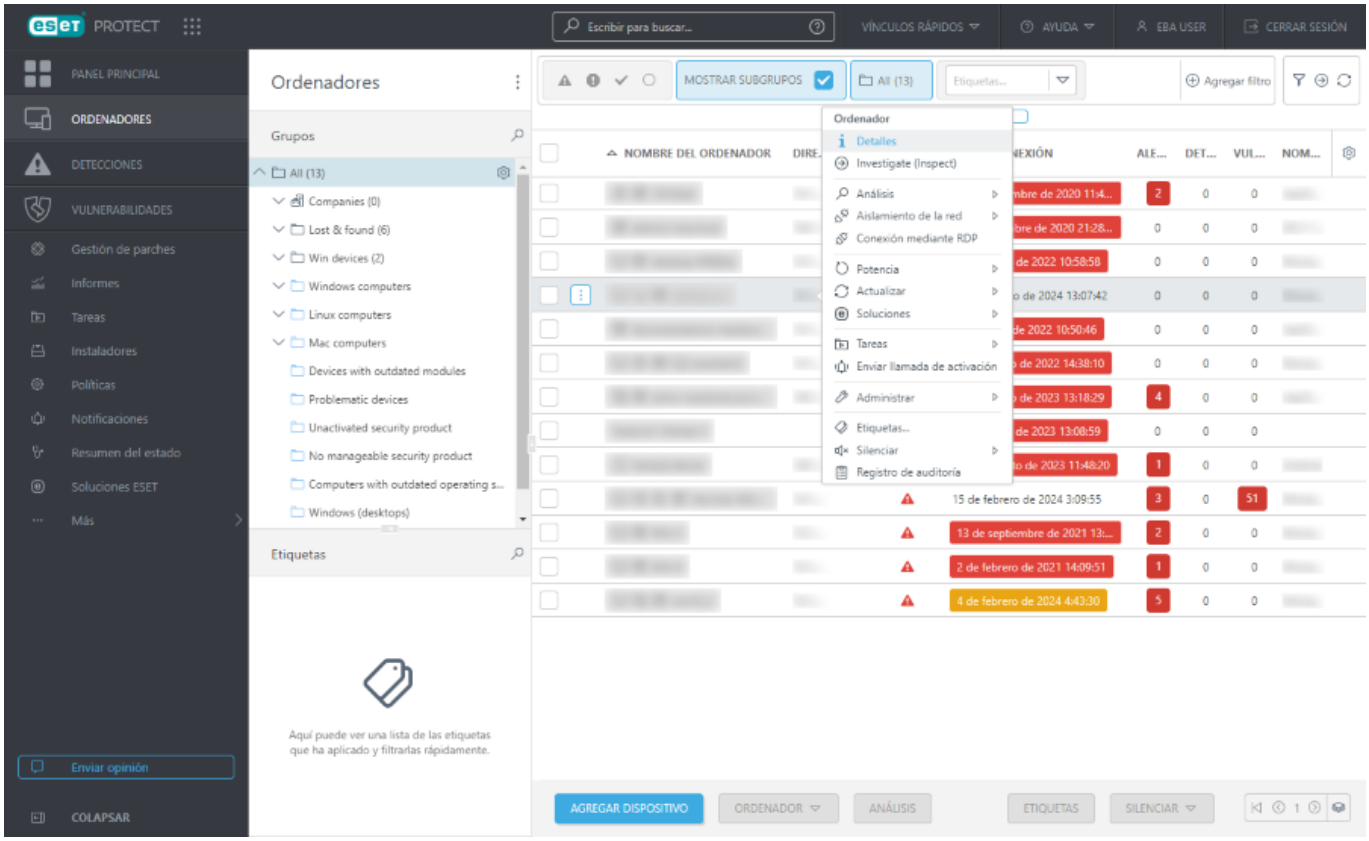
3.Diríjase hasta la sección **Registros** > ficha **SysInspector**, haga clic en una entrada de la lista y seleccione **Abrir visor de registros de SysInspector**.



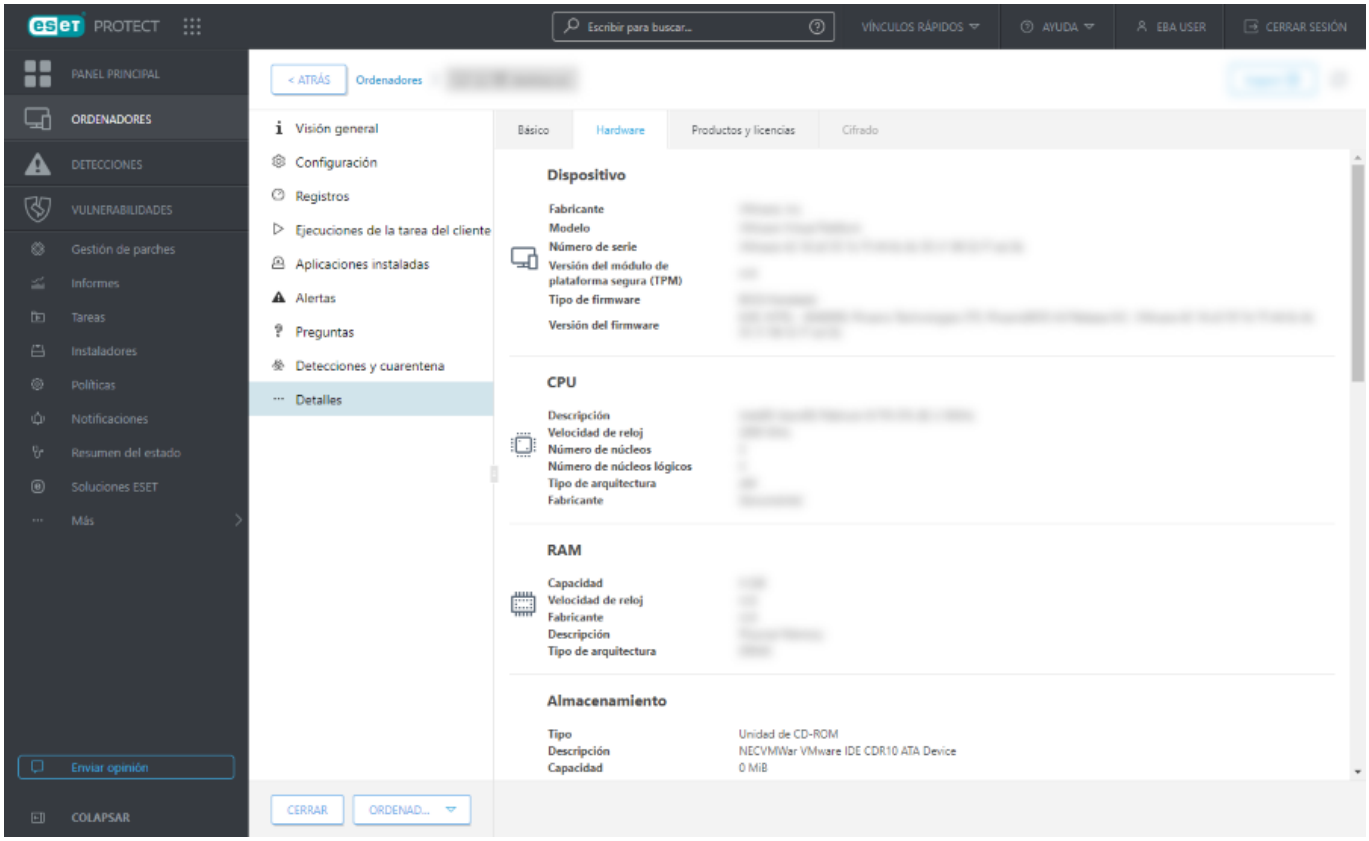
Inventario de hardware

ESET PROTECT 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.

- 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
Detener administración (desinstalar ESET Management Agent)
Actualizar agente

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)

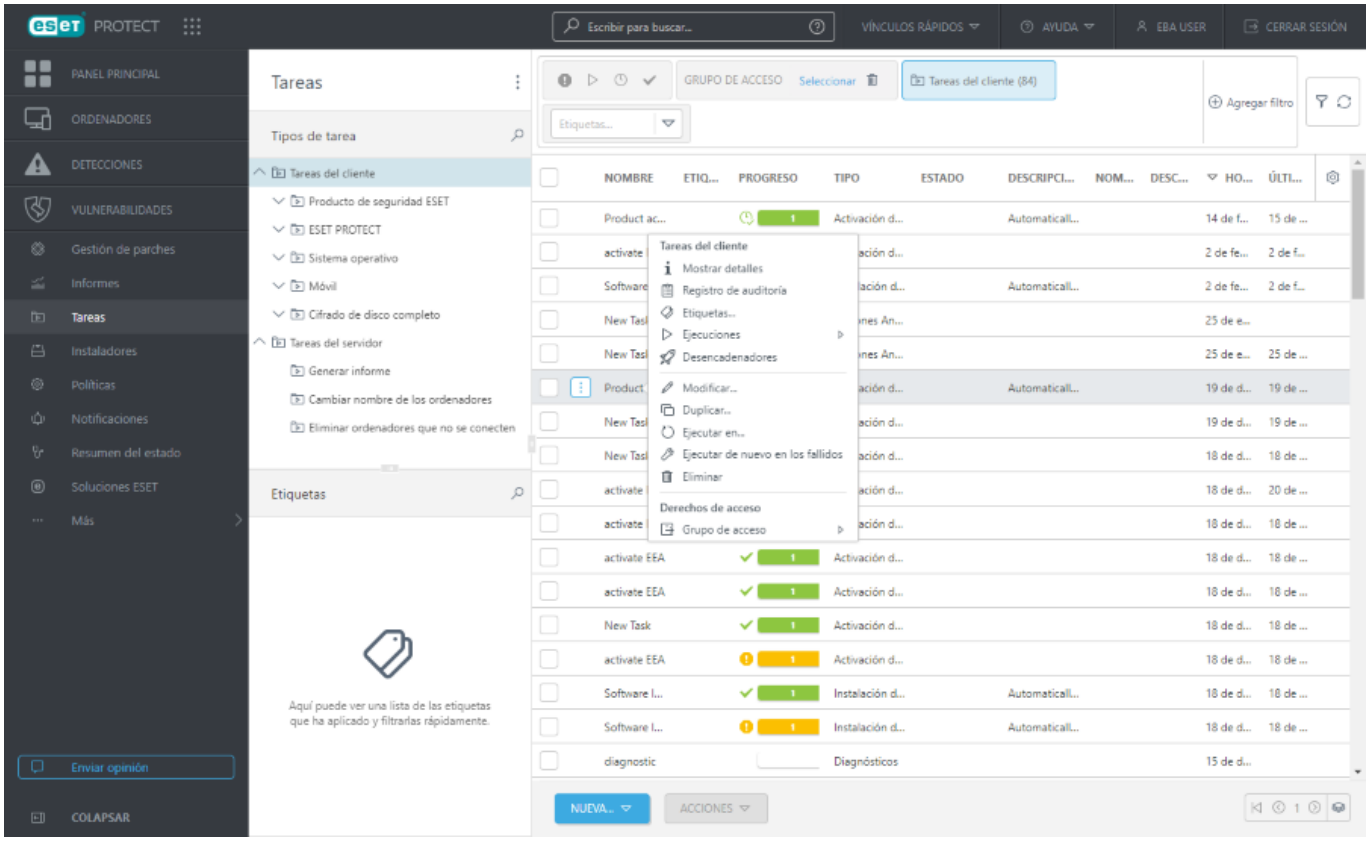
Tareas del servidor

Eliminar ordenadores que no se conecten: elimina clientes que ya no se conectan a ESET PROTECT 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.

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:

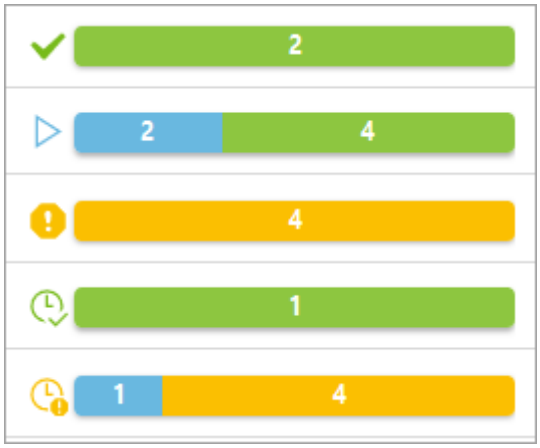
En ejecución (azul)

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**.

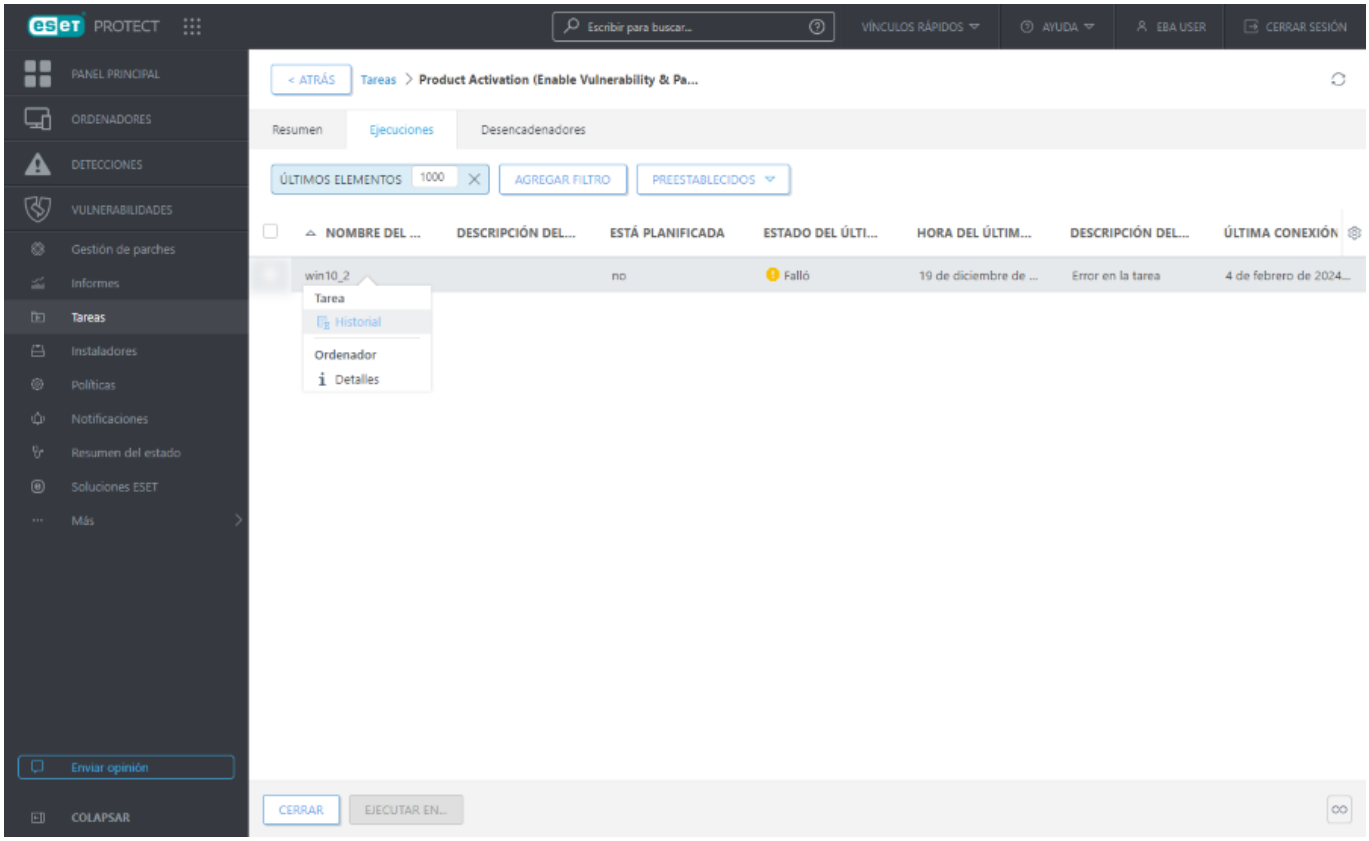
Puede modificar el filtro o desactivarlo para ver todos los ordenadores, sea cual sea su estado.

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**.

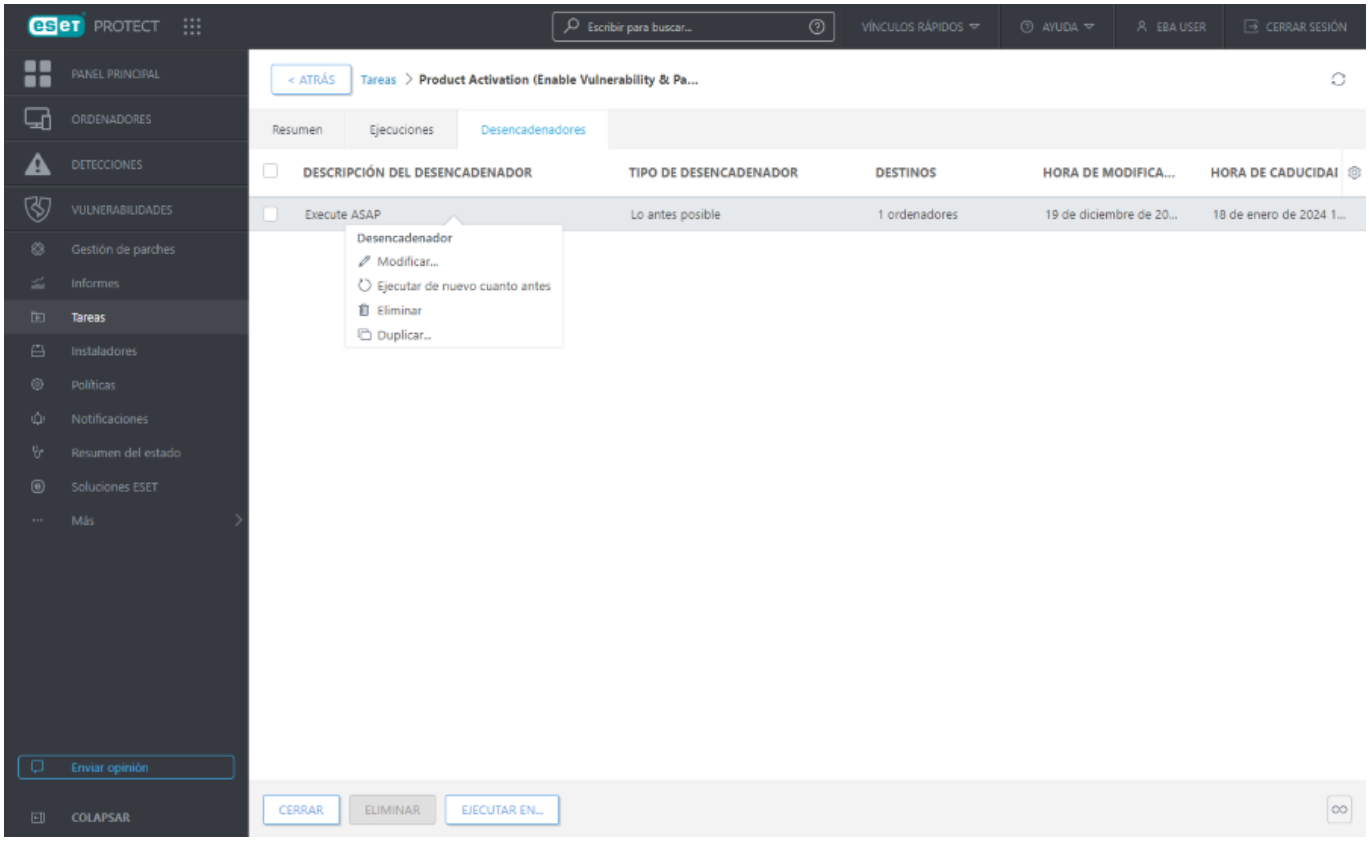
- **Detalles**: consulte los detalles del ordenador seleccionado.



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:

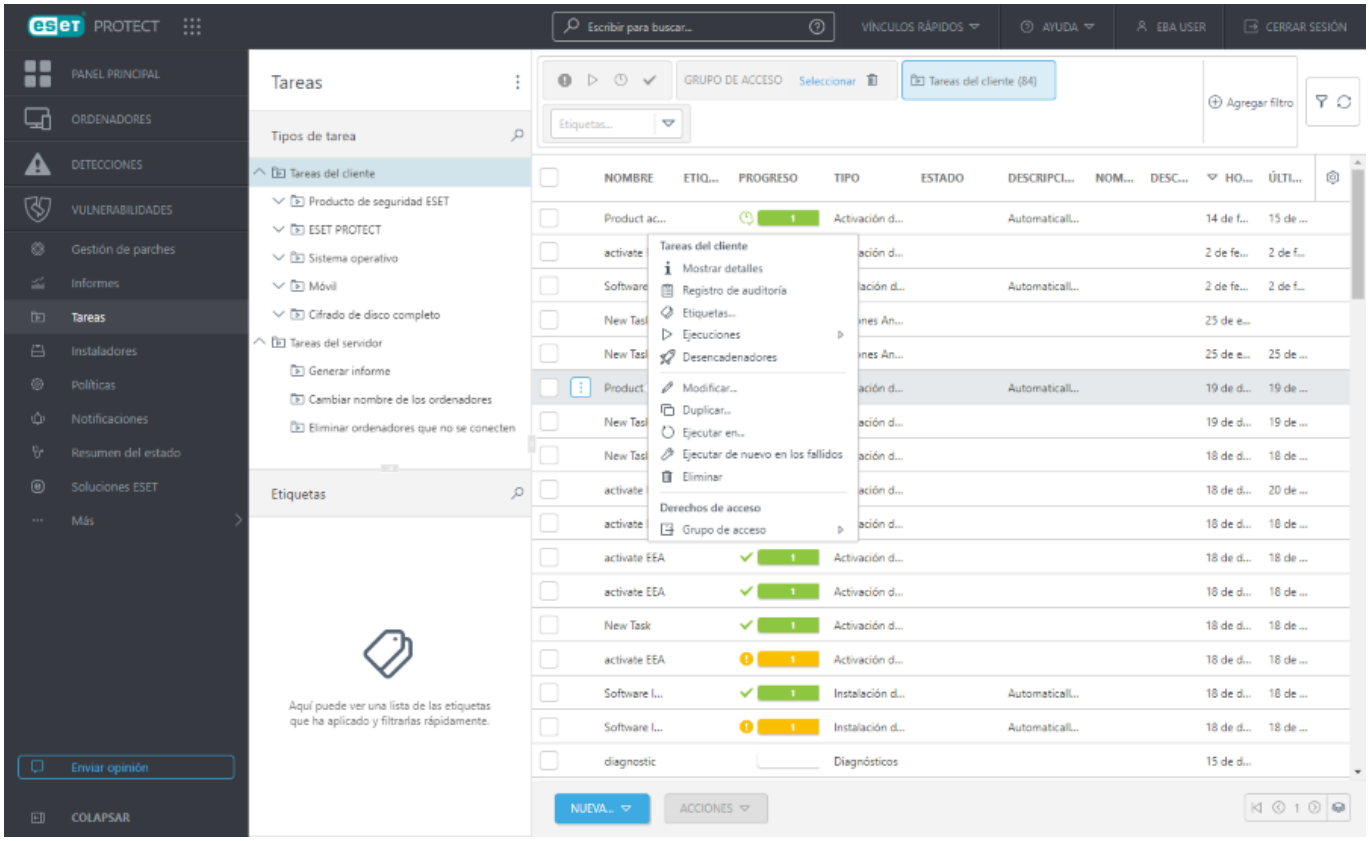
Modificar...	Permite realizar modificaciones en el desencadenador seleccionado.
Ejecutar de nuevo cuanto antes	Ejecute la tarea del cliente de nuevo (lo antes posible) con un desencadenador existente sin modificación.
Eliminar	Elimina el desencadenador seleccionado por completo. Para eliminar varios 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 ver la barra indicadora de progreso, el icono de estado y los detalles de cada **tarea** creada.



Encuentre más información sobre las tareas de cliente (Eliminar proceso) creadas en ESET Connect. Puede ver los resúmenes de tareas del cliente, sin embargo, no puede editarlos ni crearlos.

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.

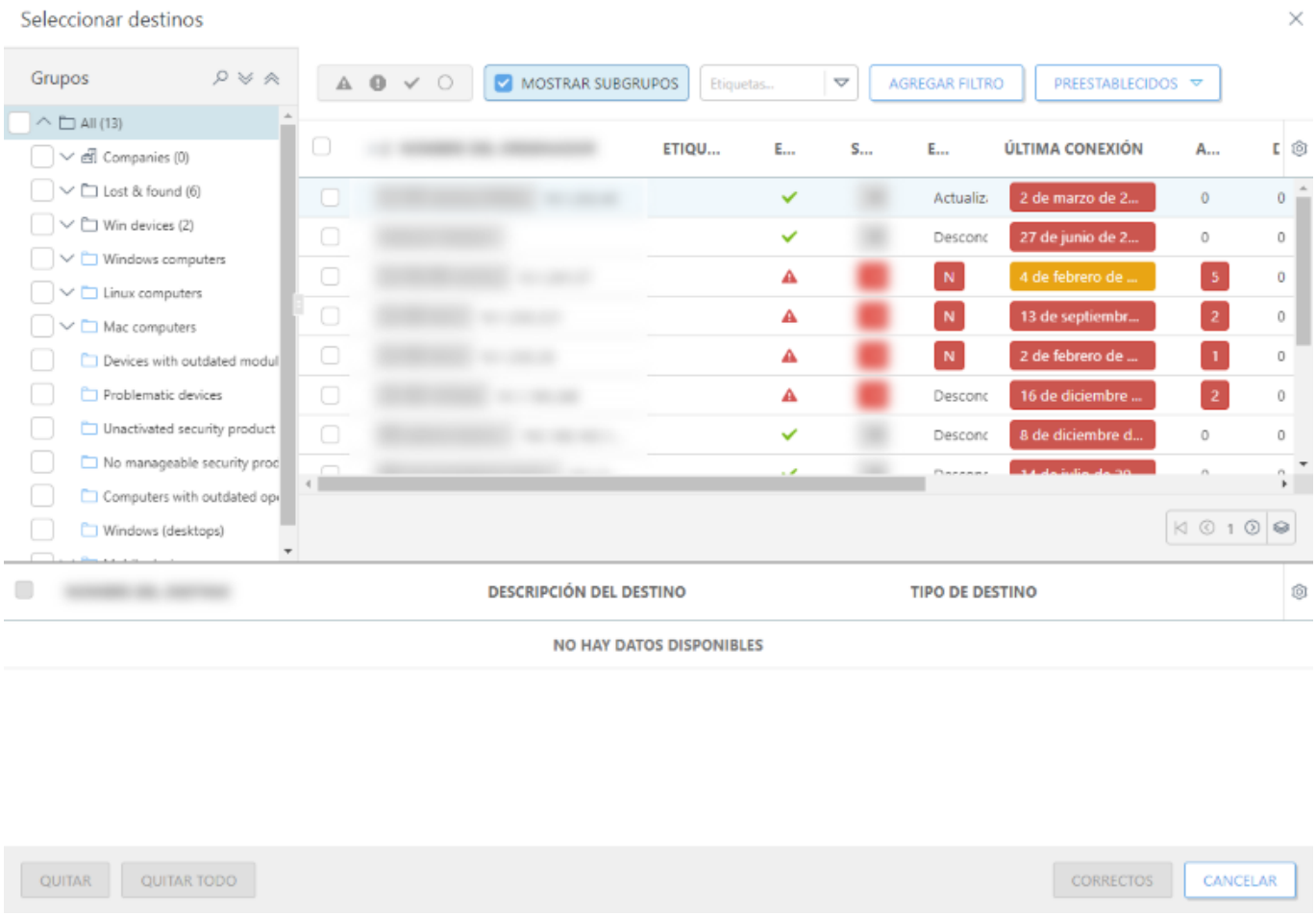
Básico

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 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. Puede establecer la fecha de caducidad hasta en 6 meses a partir de la fecha actual.
- **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.

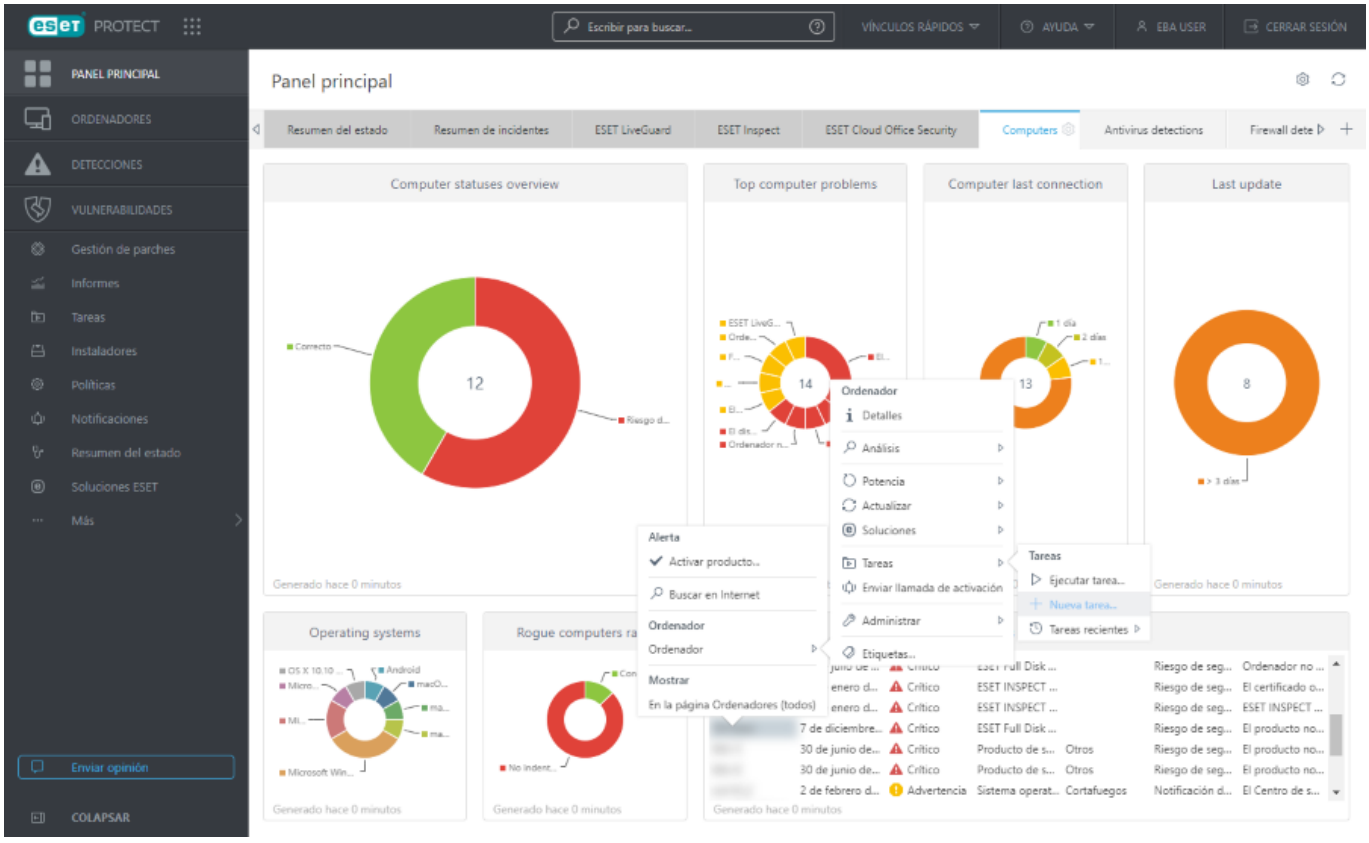
Haga clic en **Finalizar** cuando haya definido los destinatarios de esta tarea y los desencadenadores que la ejecutan.

Asignar una tarea del cliente a grupos u ordenadores

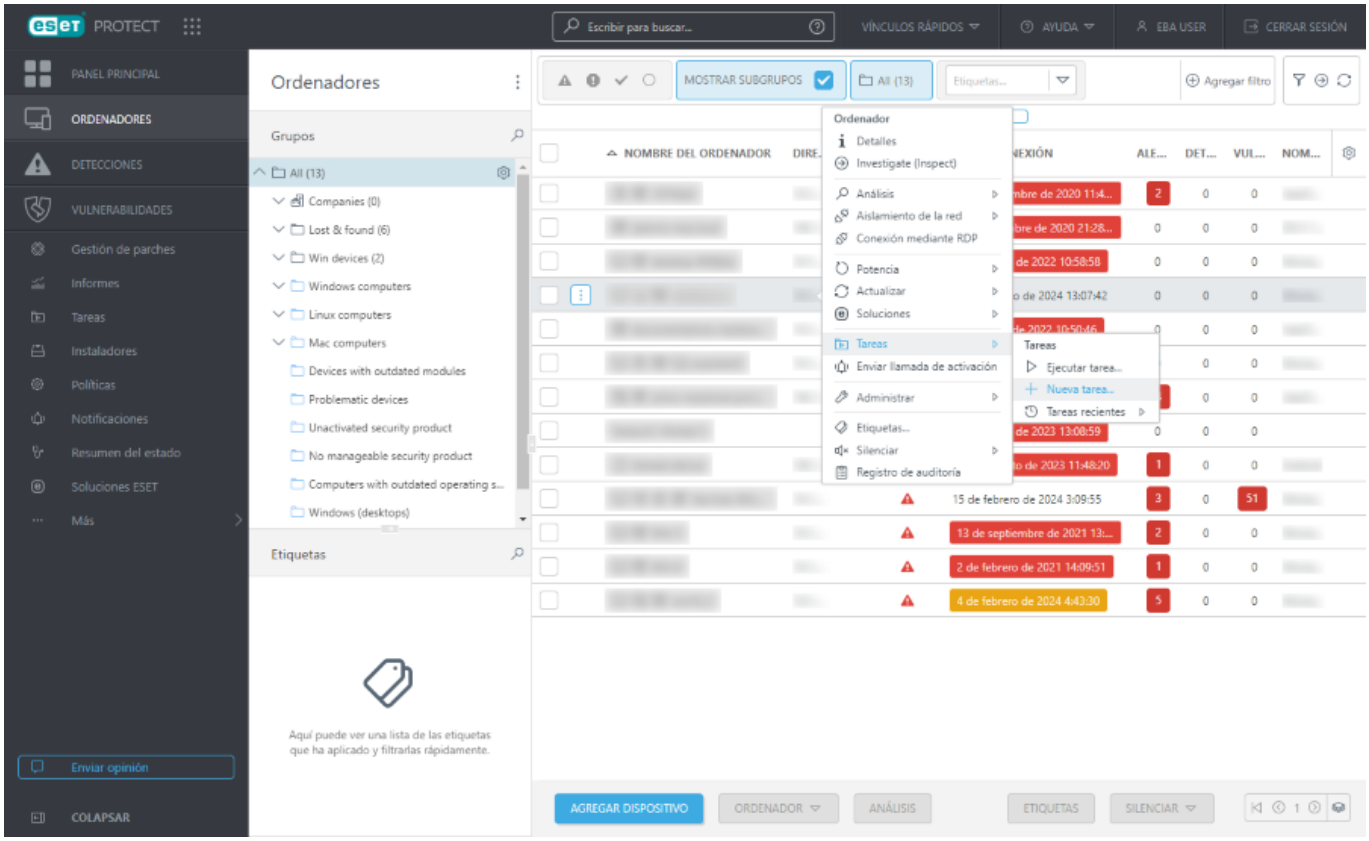
Lea cómo asignar una tarea del cliente a un grupo aquí.

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) 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**.

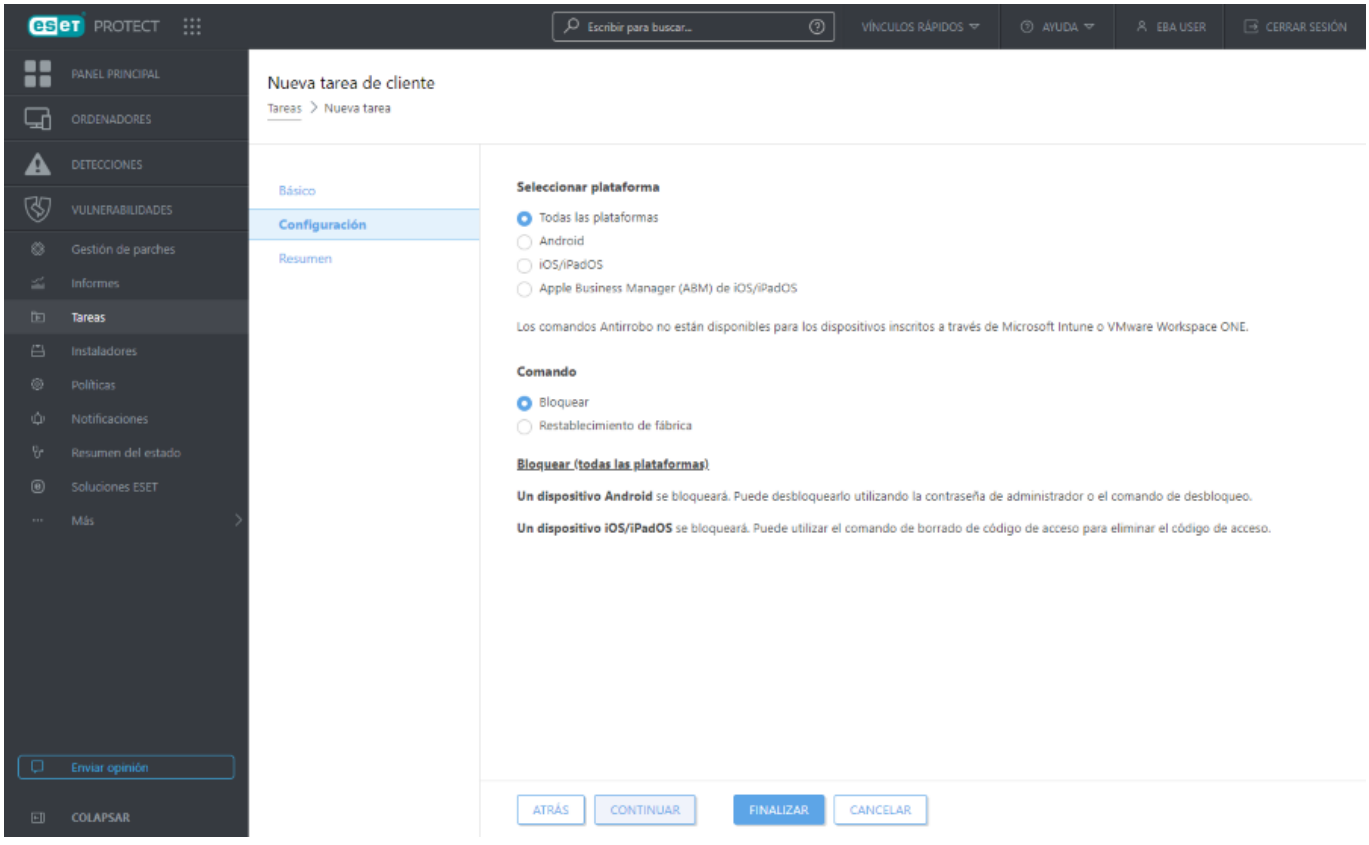
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

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.
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. 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.

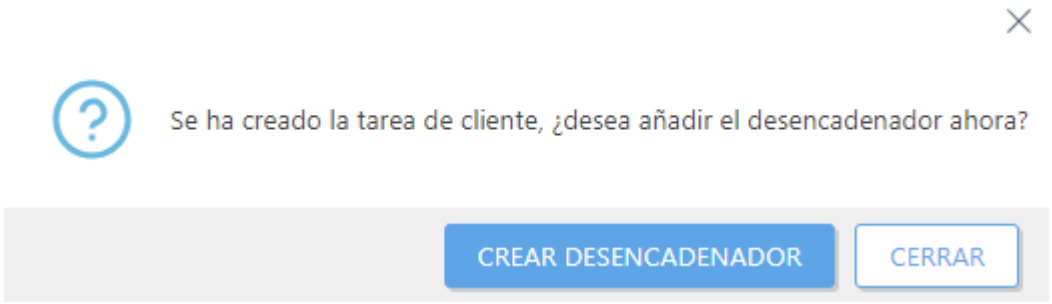


Resumen

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.

> **Desencadenadores de tareas del cliente en dispositivo móvil**
> Solo puede usar estos desencadenadores para las tareas del cliente en dispositivo móvil:
> - Lo antes posible
> - Desencadenador de grupo dinámico unido
>
> Se producirá un error en las tareas del cliente con desencadenadores distintos de los anteriores, y se mostrará el mensaje **Tipo de desencadenador no admitido**.

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
> - ESET Server Security para Microsoft Windows Server versión 11.0 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 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.

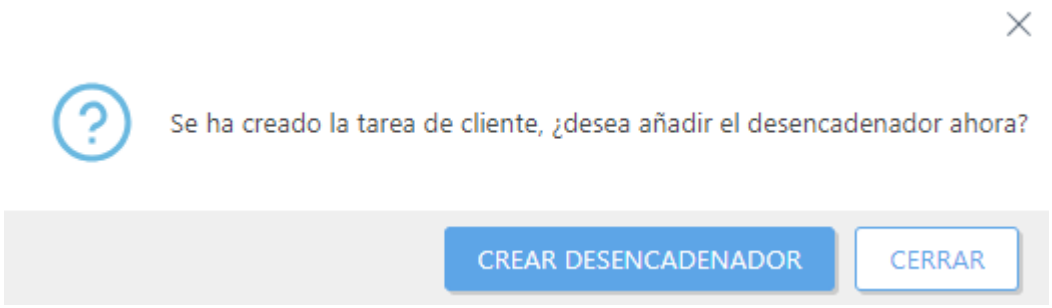
Configuración

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.

  - **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 15 MB. Puede acceder a los registros desde Web Console en **Detalles** > sección **Registros**. Si los registros que ha recopilado la tarea superan los 15 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.

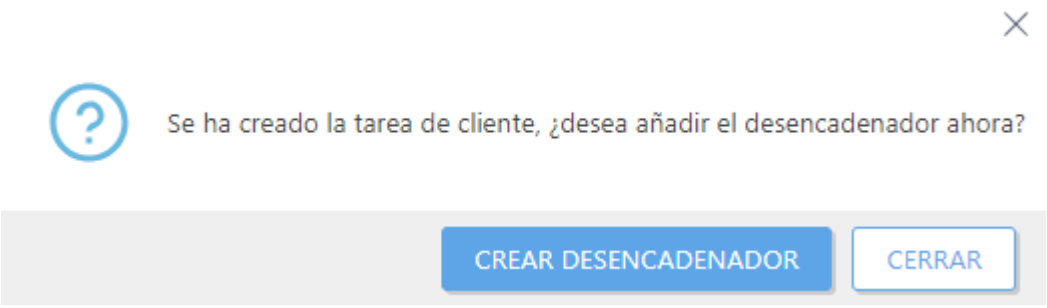
ESET Management Agent solo envía registros recopilados por un producto de ESET instalado en un ordenador cliente. La categoría y el nivel de detalle del registro dependen del tipo y de la configuración del producto. Configure cada producto (mediante Políticas) para recopilar registros específicos.

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.

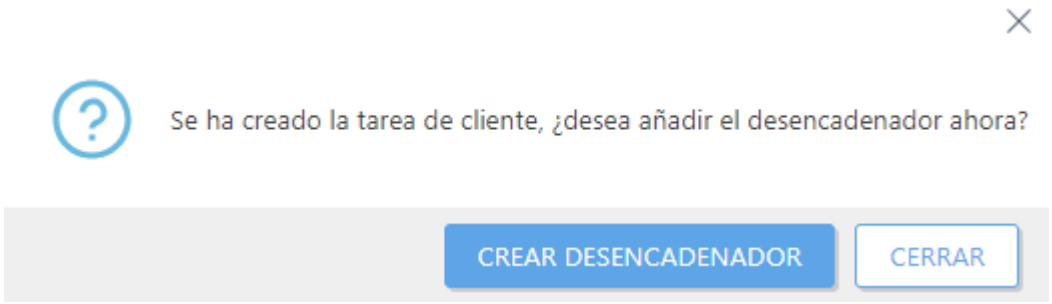
Configuración

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

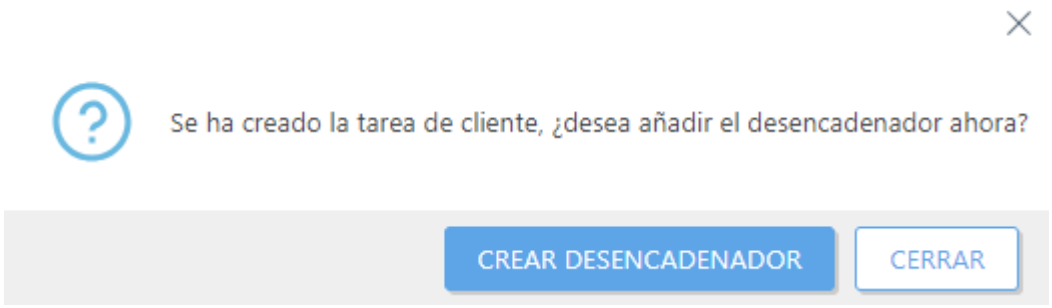
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo 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.

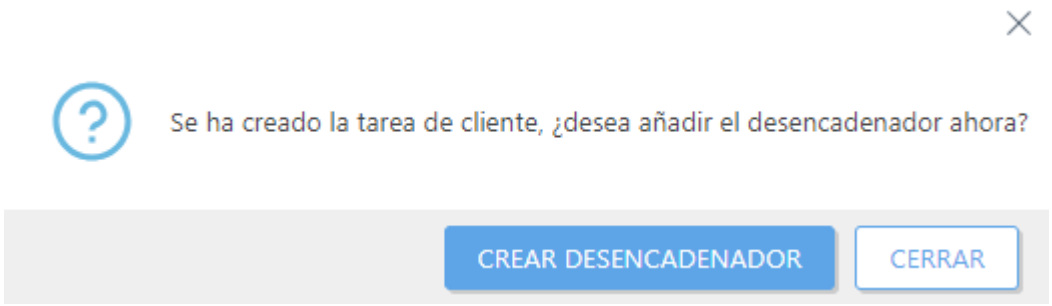
- **Producto**: seleccione un componente de ESET PROTECT o un producto de seguridad de ESET cliente para los que desee exportar la configuración.

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.

Sistemas operativos compatibles
El aislamiento de la red está disponible para dispositivos Windows y macOS.

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

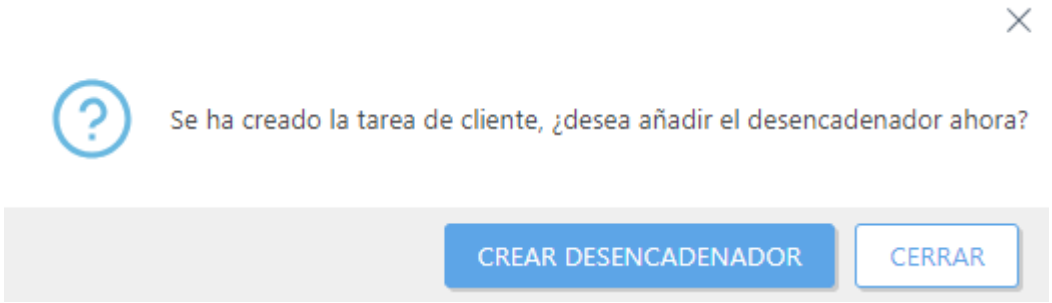
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo 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

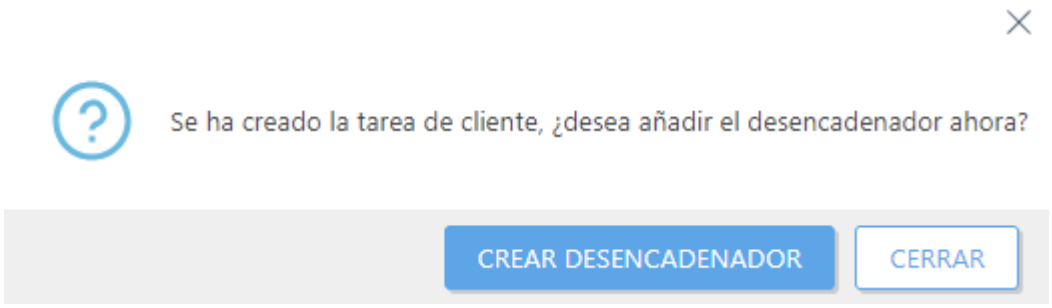
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo 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

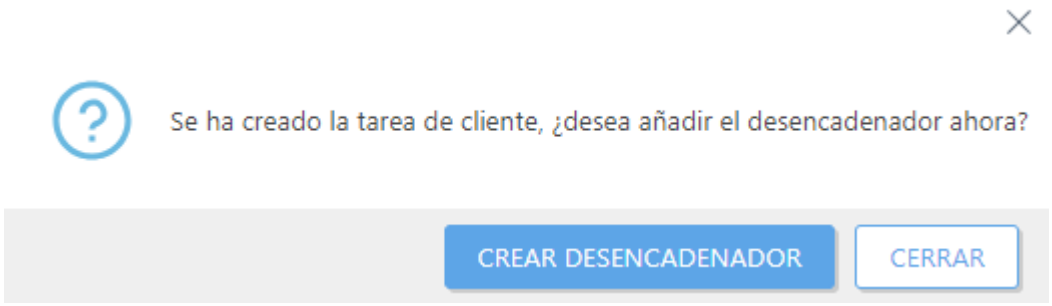
- **Borrar caché de actualización**: esta opción elimina los archivos de actualización temporales de la memoria caché del cliente y, con frecuencia, se puede utilizar para reparar los errores de actualizaciones de módulos.

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

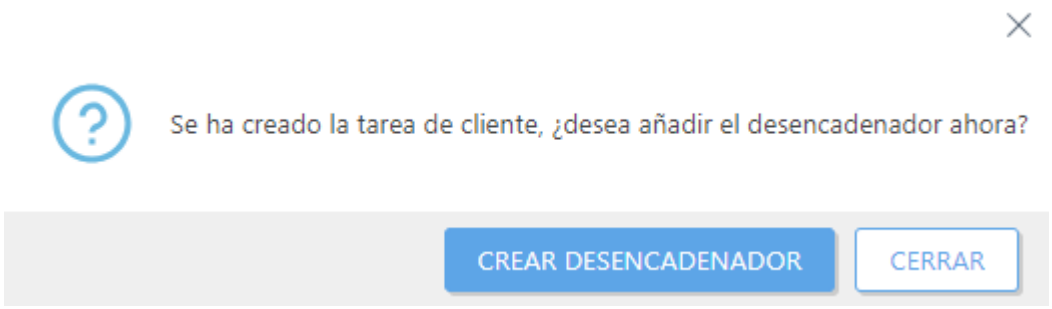
- **Activar actualizaciones:** las actualizaciones están activadas y el cliente recibirá la próxima actualización del módulo.
- **Revertir y desactivar actualizaciones hasta el siguiente**: las actualizaciones están desactivadas durante el periodo de tiempo específico del menú desplegable **Desactivar 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).

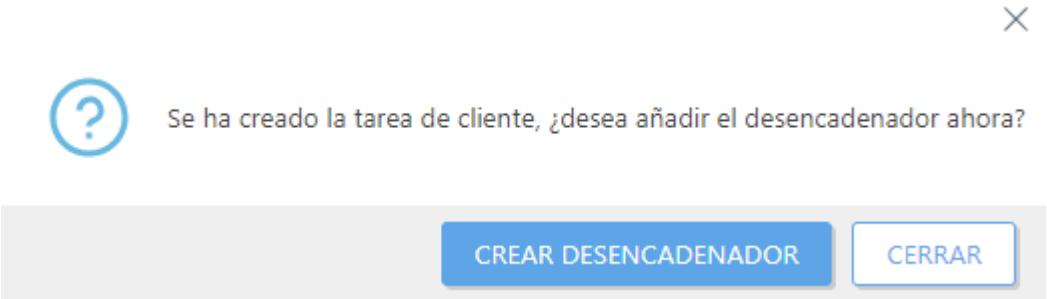
A continuación se exponen algunos ejemplos de uso de los parámetros de objeto del **Análisis a petición**:
■Archivo: *C:\Users\Data.dat*
■Carpeta: *C:\MyFolder*
■Ruta o archivo Unix */usr/data*
■Ubicación UNC de Windows *\\server1\scan_folder*
■Cadena predefinida `${Memory}`

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:

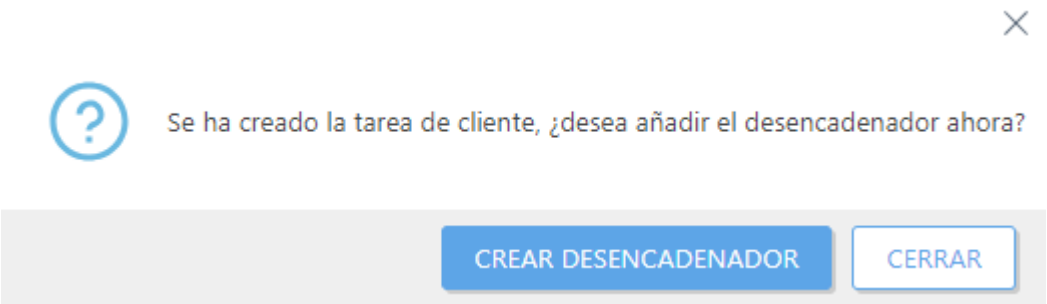
- Windows informará al usuario del ordenador sobre el reinicio forzado planificado 4 horas antes del reinicio y 10 minutos antes del mismo.
- macOS se reiniciará inmediatamente después de la actualización.

- 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: 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.

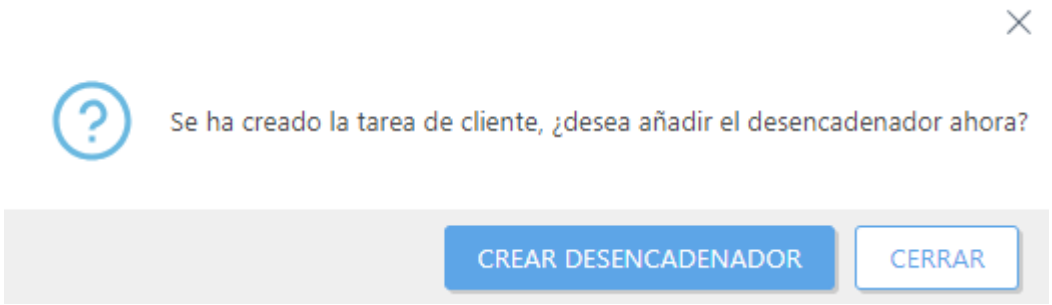
Configuración del filtro:

- **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.

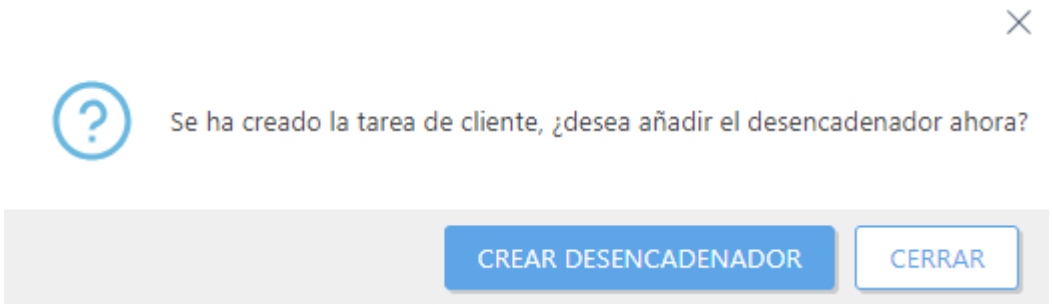
Configuración

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**).

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.

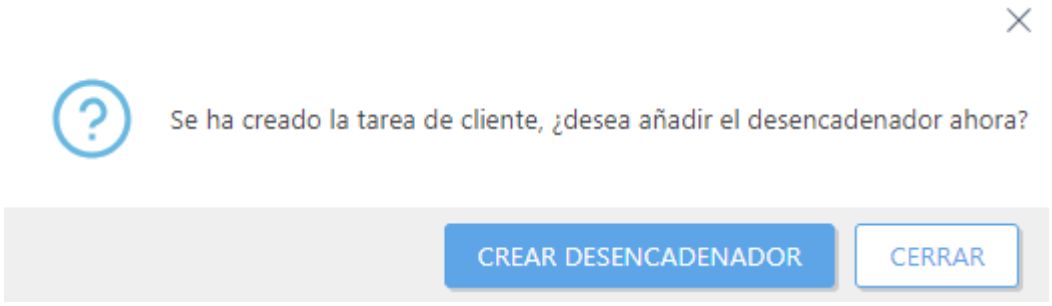
no hay **configuración** disponible para esta tarea.

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.

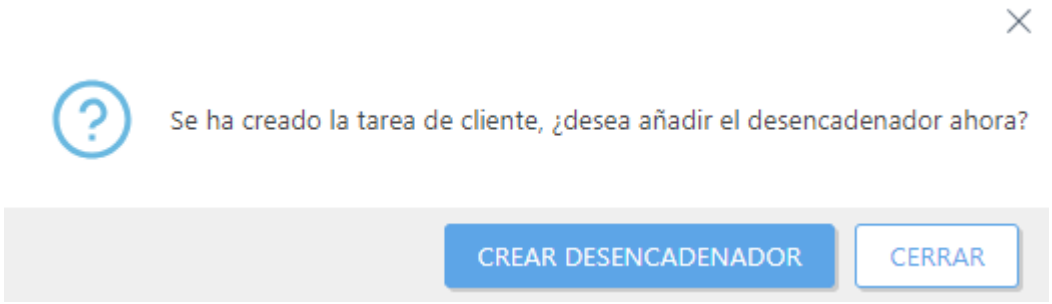
no hay **configuración** disponible para esta tarea.

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.

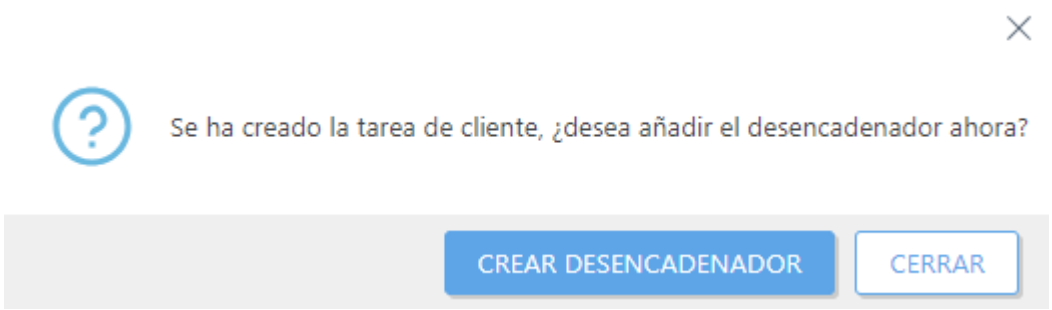
- Para ejecutar un comando de varias líneas para reiniciar un servicio de Windows de forma remota (sustituya `service_name` por el nombre de servicio, por ejemplo, `wuauserv` para el servicio Windows Update):

```
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

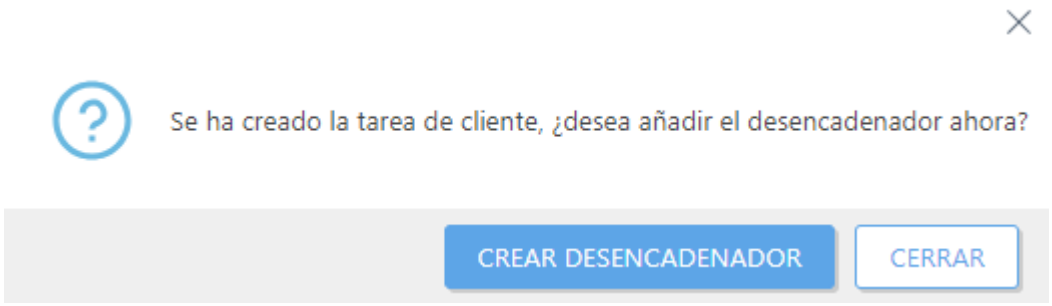
- **Script de SysInspector**: haga clic en **Examinar** para desplazarse hasta el script del servicio. El script del servicio debe crearse antes de ejecutar esta tarea.
- **Acción**: puede **Cargar** o **Descargar** un script de ESET PROTECT Web Console.

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.

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 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 utilice el destino de análisis adecuado. Cuando ESET PROTECT 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.

Producto	Análisis	Descripción
ESET Mail Security para IBM Domino	**Análisis de la base de datos a petición , análisis Hyper-V**	Esta funcionalidad permite que ESET PROTECT 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 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 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.

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

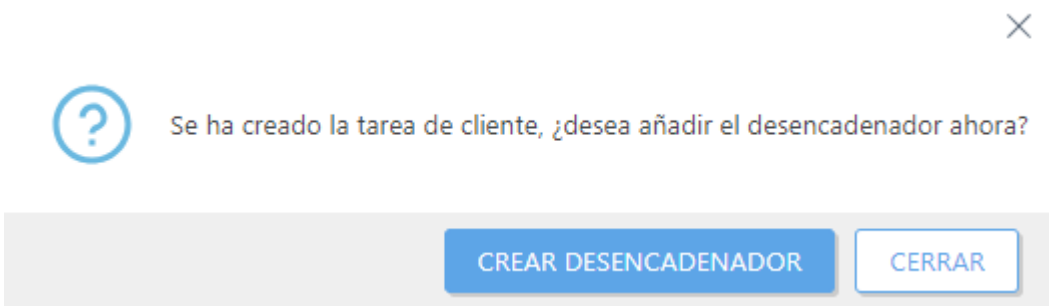
- **Reiniciar ordenadores**: marque esta casilla si desea reiniciar el ordenador cliente después de finalizar la tarea. Anule la selección de esta opción si desea apagar los ordenadores.

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** > **Activar producto de seguridad** para activar 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 Instalación del software para actualizar instancias de ESET Management Agent. En su lugar, utilice la tarea Actualizar 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.

Configuración

Paquete que instalar: hay dos opciones:

- **Instalar paquete desde el repositorio**

  o**Elija un sistema operativo**: seleccione el sistema operativo para la instalación del producto.

  o**Seleccionar 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**).

- 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:

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.

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*):

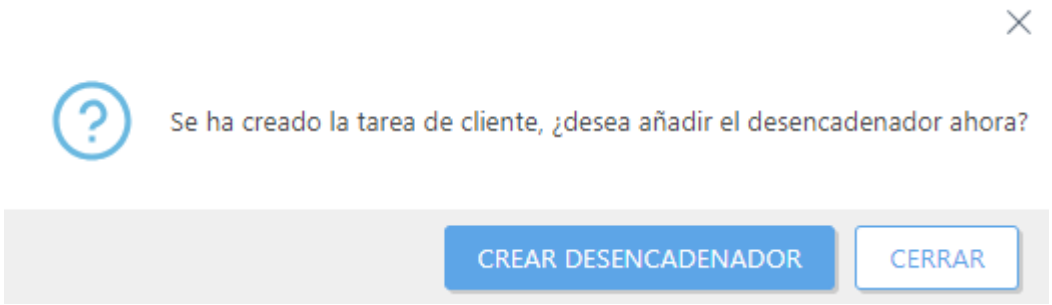
```
./install_script.sh -a parameter_1 -b parameter_2
```

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

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 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.

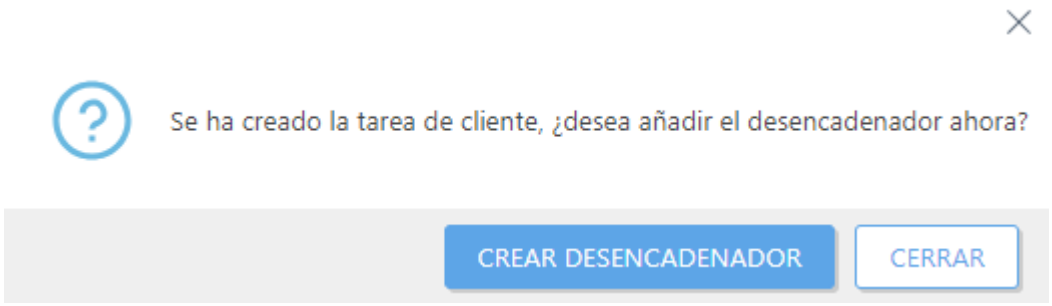
Siga las instrucciones detalladas del artículo Quitar software antivirus de terceros de ordenadores cliente con ESET PROTECT para enviar una tarea de eliminación de software antivirus de terceros de ordenadores cliente.

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 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

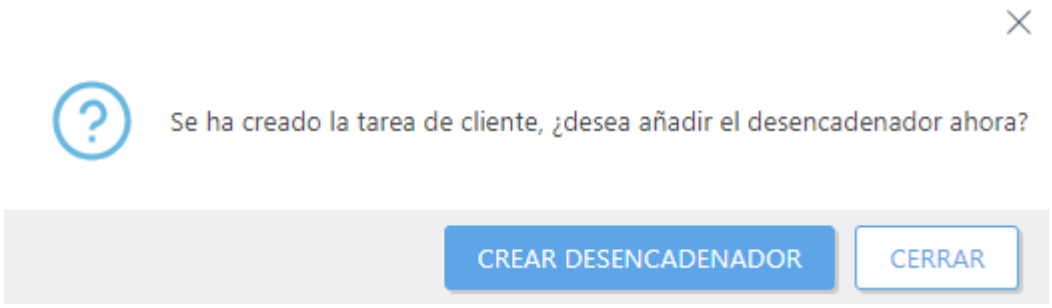
En la sección **Básico**, introduzca información básica sobre la tarea, como el **nombre y la descripción (opcional)**. Haga clic en **Seleccione las etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si ha especificado un tipo 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*.

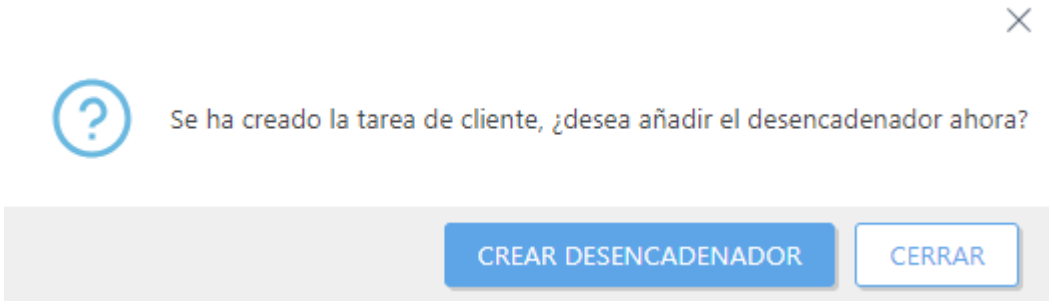
Resumen

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.

Actualizar agente

Puede usar la tarea **Actualizar agente** para actualizar ESET Management Agent a la versión más reciente.

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

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**.

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)

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

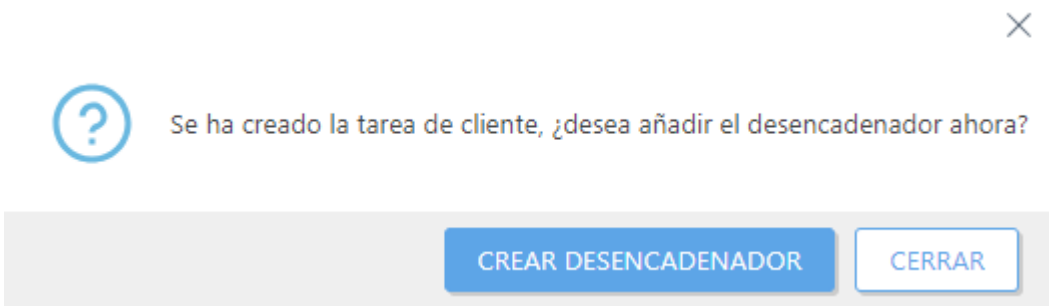
Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

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.

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

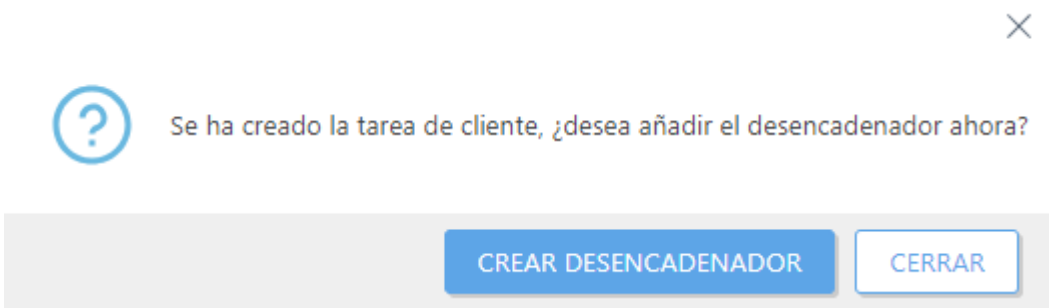
- **Objeto en cuarentena**: seleccione un objeto específico en la cuarentena.
- **Contraseña del objeto**: escriba una contraseña para cifrar el objeto por motivos de seguridad. Tenga en cuenta que la contraseña se mostrará en el informe correspondiente.
- **Cargar ruta**: escriba una ruta a la ubicación 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

- Eliminar ordenadores que no se conecten
- Generar informe
- Cambiar nombre de los ordenadores

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.

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.

- **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 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.

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. Puede utilizar la tarea del servidor existente que se ofrece de forma predeterminada con la instalación de ESET PROTECT. 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.

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.

> **Desencadenadores de tareas del cliente en dispositivo móvil**
> Solo puede usar estos desencadenadores para las tareas del cliente en dispositivo móvil:
> • Lo antes posible
> • Desencadenador de grupo dinámico unido
> Se producirá un error en las tareas del cliente con desencadenadores distintos de los anteriores, y se mostrará el mensaje **Tipo de desencadenador no admitido**.

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. Puede establecer la fecha de caducidad hasta en 6 meses a partir de la fecha actual.

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

- **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`
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:

```
┌──────────── Segundos (0-59)
│ ┌────────── Minutos (0-59)
│ │ ┌──────── Horas (0-23)
│ │ │ ┌────── Día del mes (1 - 31)
│ │ │ │ ┌──── Mes (1-12 o JAN-DEC)
│ │ │ │ │ ┌── Día de la semana (0 - 6 o SUNSAT)(por ejemplo, 0 es lo
mismo que SUN)
│ │ │ │ │ │ ┌ Año
│ │ │ │ │ │ │
* * * * * ? *
```

- 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.

> **i** 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 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).

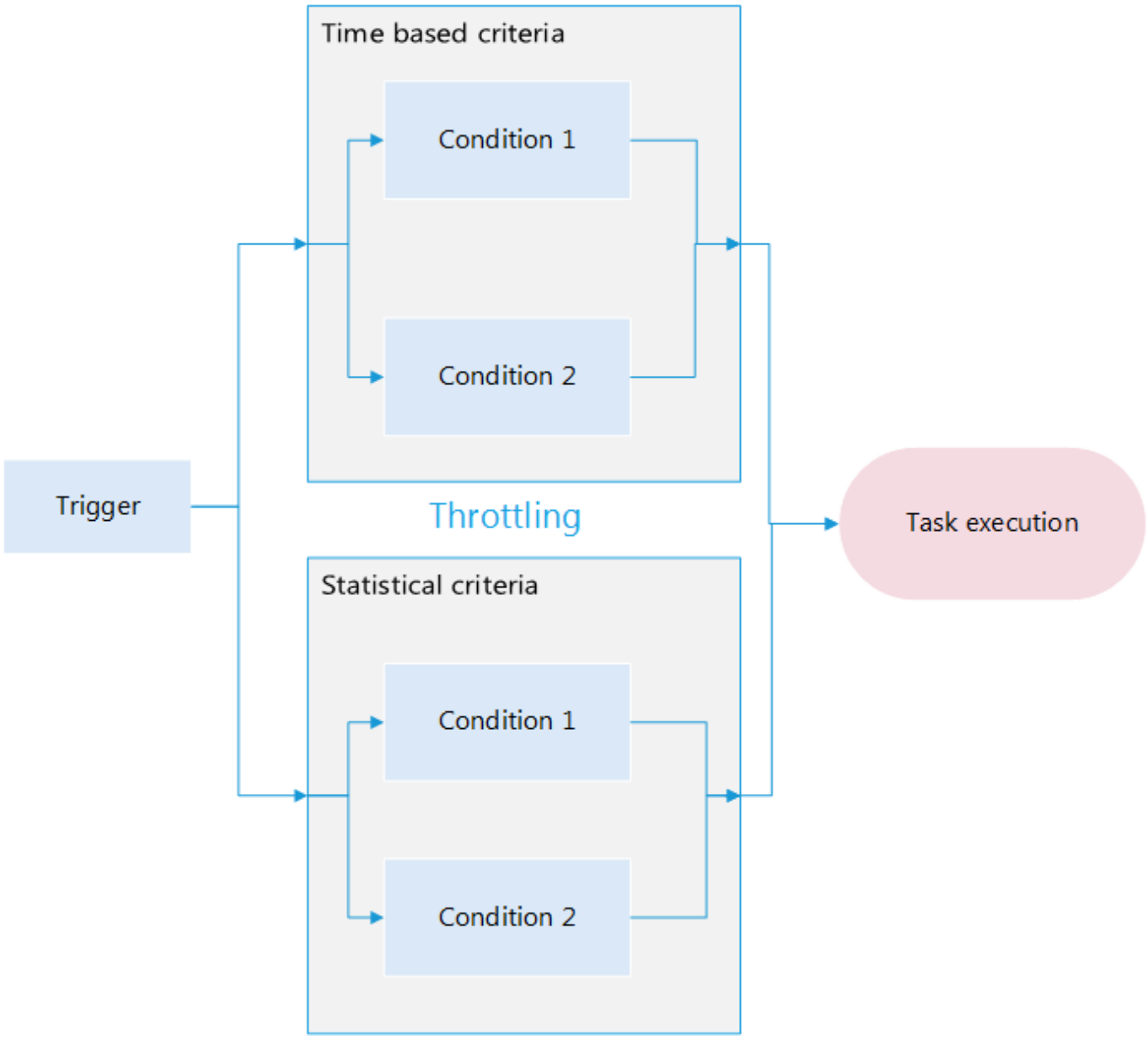
Se recomienda utilizar los momentos de tiempo aleatorios para evitar que todos los ESET Management Agent se conecten a la vez a su ESET PROTECT Server.

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 15 minutos y las notificaciones 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**.

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 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 descargarlos de nuevo cuando sea necesario.

Haga clic en **Instaladores** > **Crear instalador** y seleccione el sistema operativo.

Seleccione la configuración del instalador, acepte el EULA y seleccione una de las opciones de distribución del instalador (la configuración del instalador y las opciones de distribución pueden variar en función del sistema

operativo):

- Haga clic en **Descargar** para descargar el paquete del instalador.
- Haga clic en el icono **Copiar** para copiar el vínculo del instalador en el portapapeles.
- Haga clic en el icono **Correo electrónico** para enviar un mensaje de correo electrónico con un vínculo al paquete del instalador.

También puede hacer clic en **Personalizar instalador** para acceder a más opciones antes de descargar el paquete del instalador:

Windows

- Descargar o enviar 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 y la posibilidad de seleccionar un grupo principal. Puede implementar el instalador de forma local o remota (con ESET Remote Deployment Tool).
- 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.
- 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).

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).

Android o iOS/iPadOS

Inscriba los dispositivos móviles en la nube de Web Console.

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**.

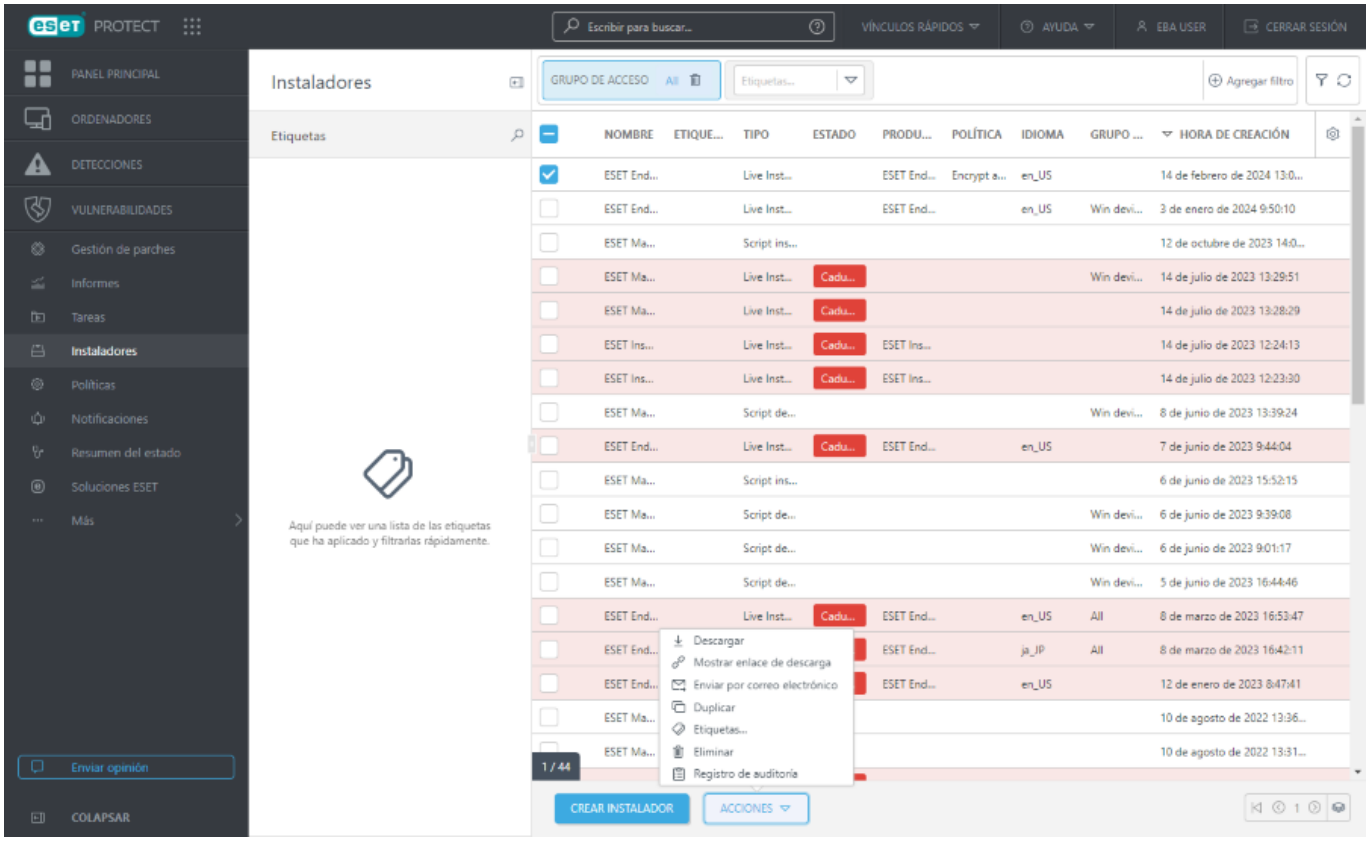
Para descargar instaladores ya creados, el usuario necesita permiso de **Uso** sobre **Grupos y ordenadores** e **Instaladores almacenados**.

- 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.

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.



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 **Acciones** > **Descargar**.

4.Puede encontrar el paquete de instalación en la carpeta donde su navegador web guarda los archivos descargados.

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 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.

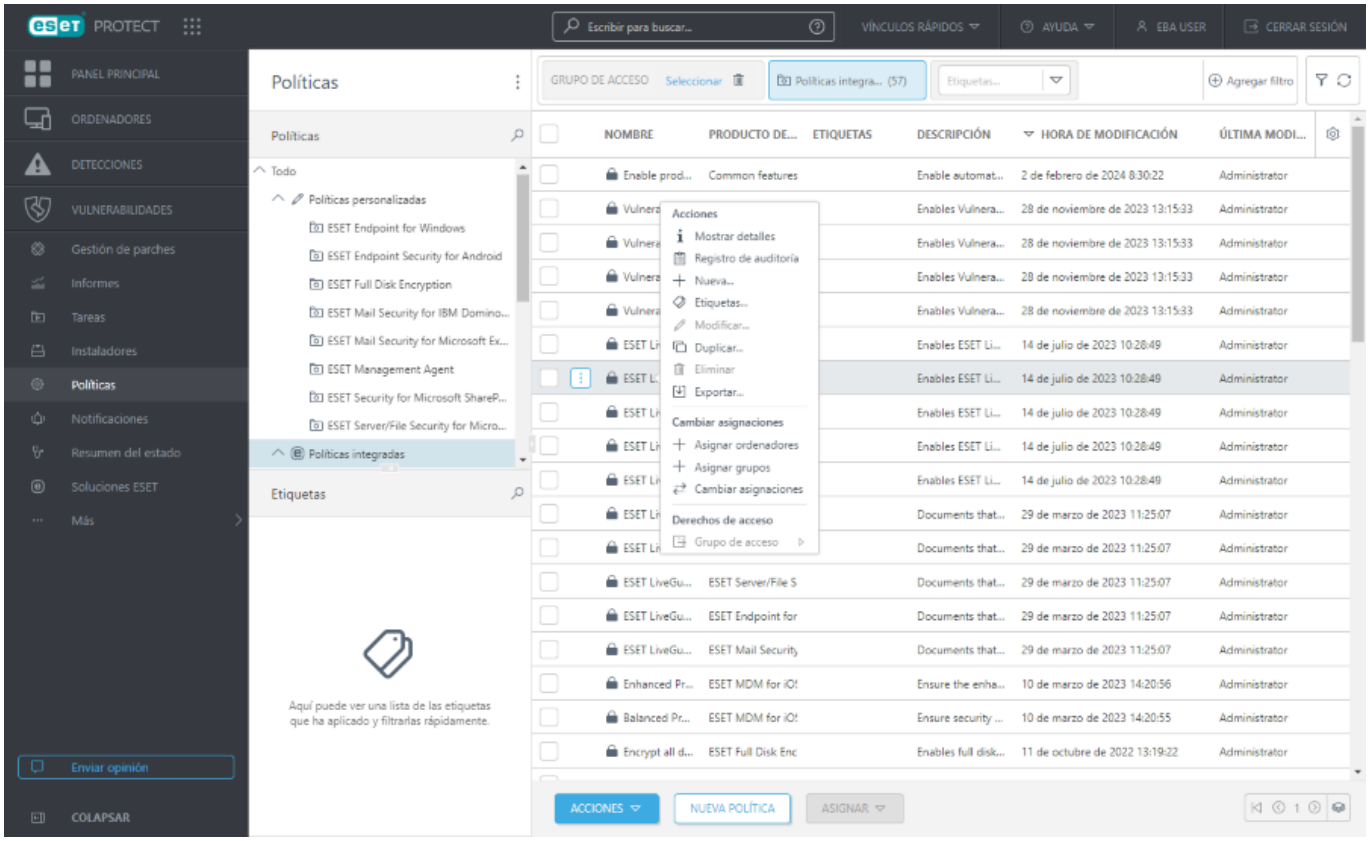
> Le recomendamos que asigne políticas más genéricas (por ejemplo, el servidor de actualización) a grupos que están más arriba en el árbol de grupos. Políticas más específicas (por ejemplo, configuración del control de dispositivos) más abajo en el árbol de grupos. Las políticas más bajas suelen reemplazar 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 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 permisos**, 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**).

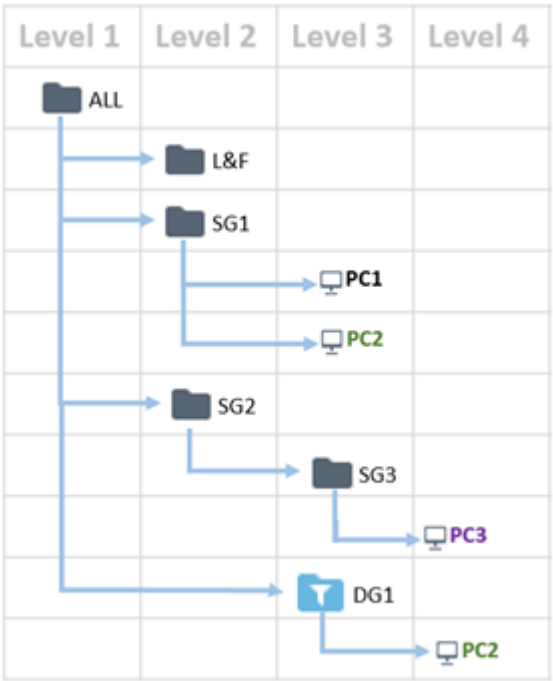
Regla 2: En cada nivel, los grupos estáticos de dicho nivel se recorren en primer lugar siguiendo el orden en el que aparecen en el árbol (esto también se denomina búsqueda "en anchura").

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: 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:

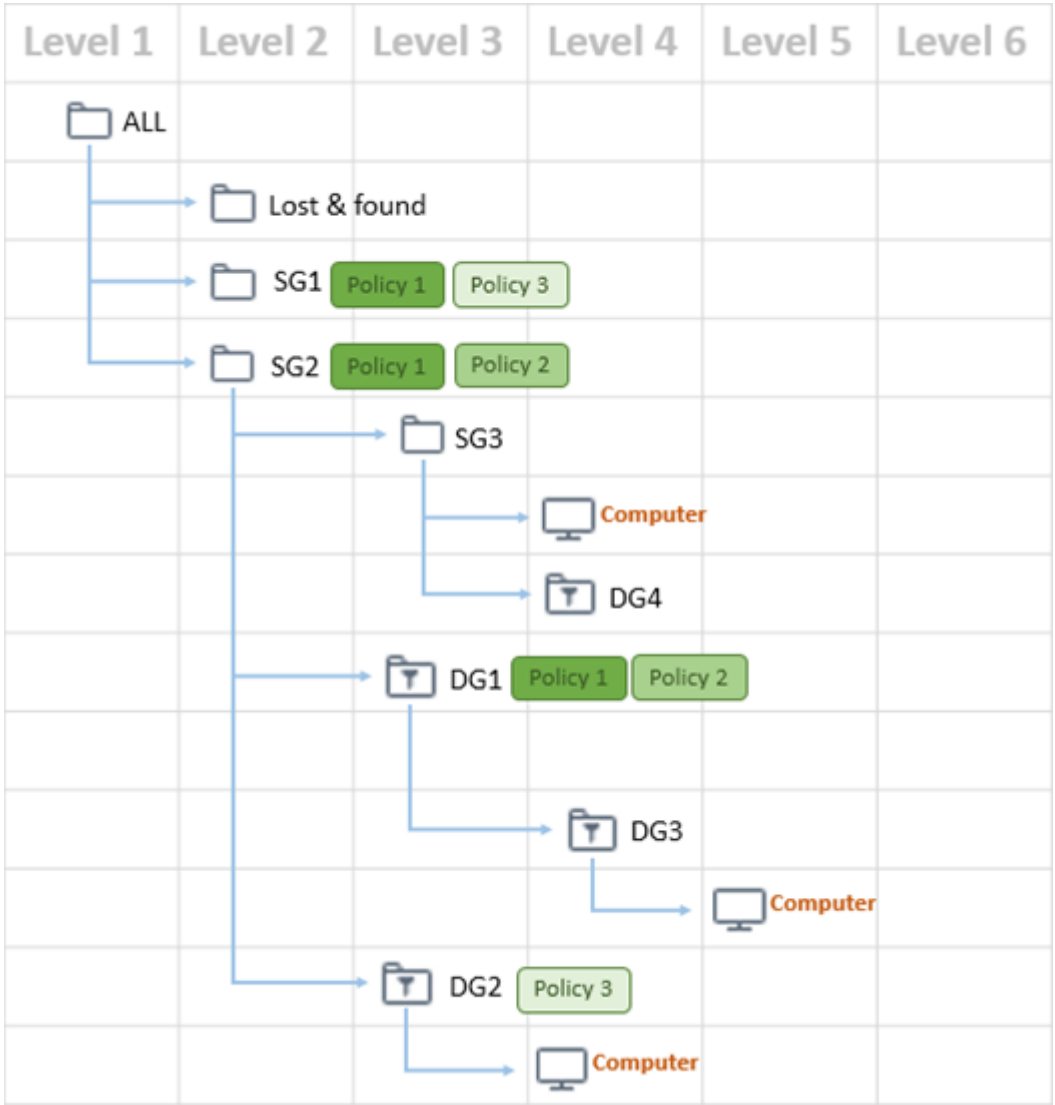
PC1:	PC2:	PC3:
1.ALL 2.SG1 3.PC1	1.ALL 2.SG1 3.DG1 4.PC2	1.ALL 2.SG2 3.SG3 4.PC3

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. 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.

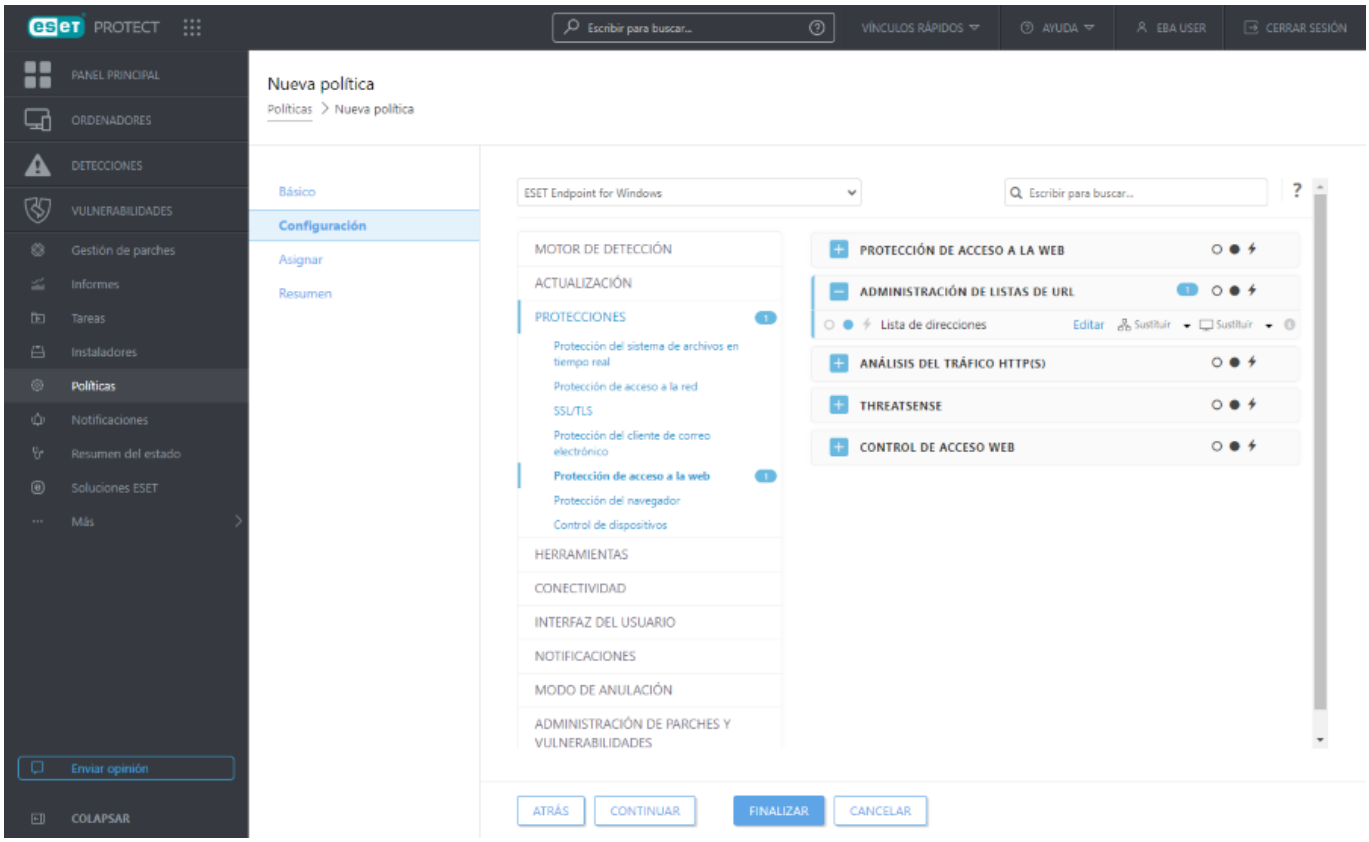
• **Anteponer**: al aplicar la misma configuración en más de una política, puede anteponer la configuración con esta regla. El ajuste se incluirá al principio de la lista creada fusionando políticas.

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:

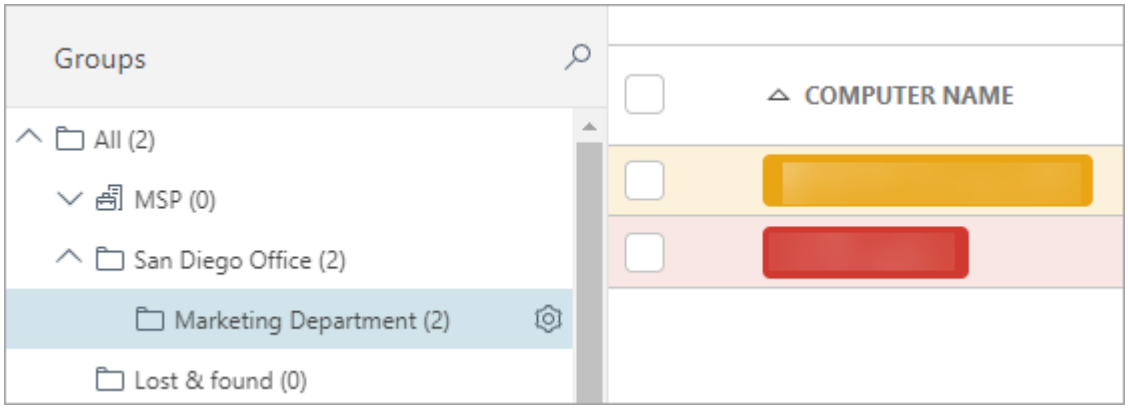
• Instrucciones sobre cómo aplicar ajustes de políticas a productos de seguridad ESET Endpoint

• 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**

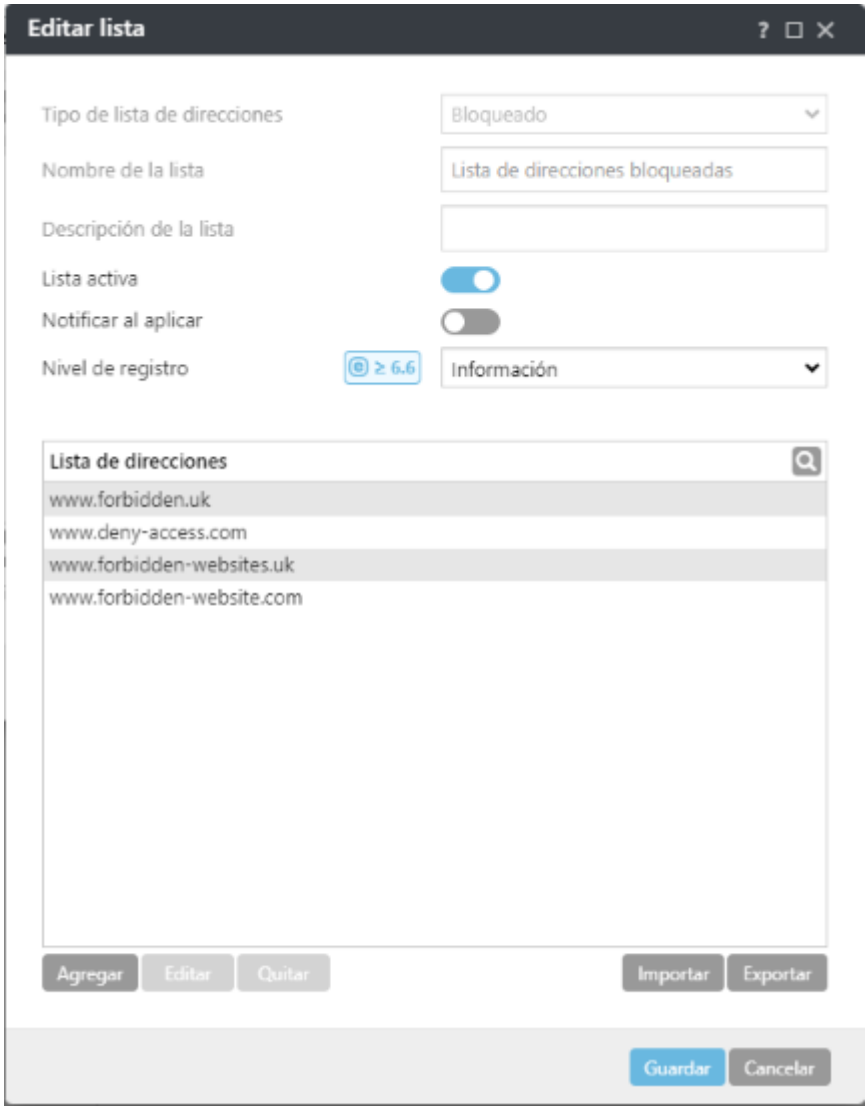
   v)Hacer clic en **Lista de direcciones bloqueadas** y seleccionar **Modificar**.

   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.

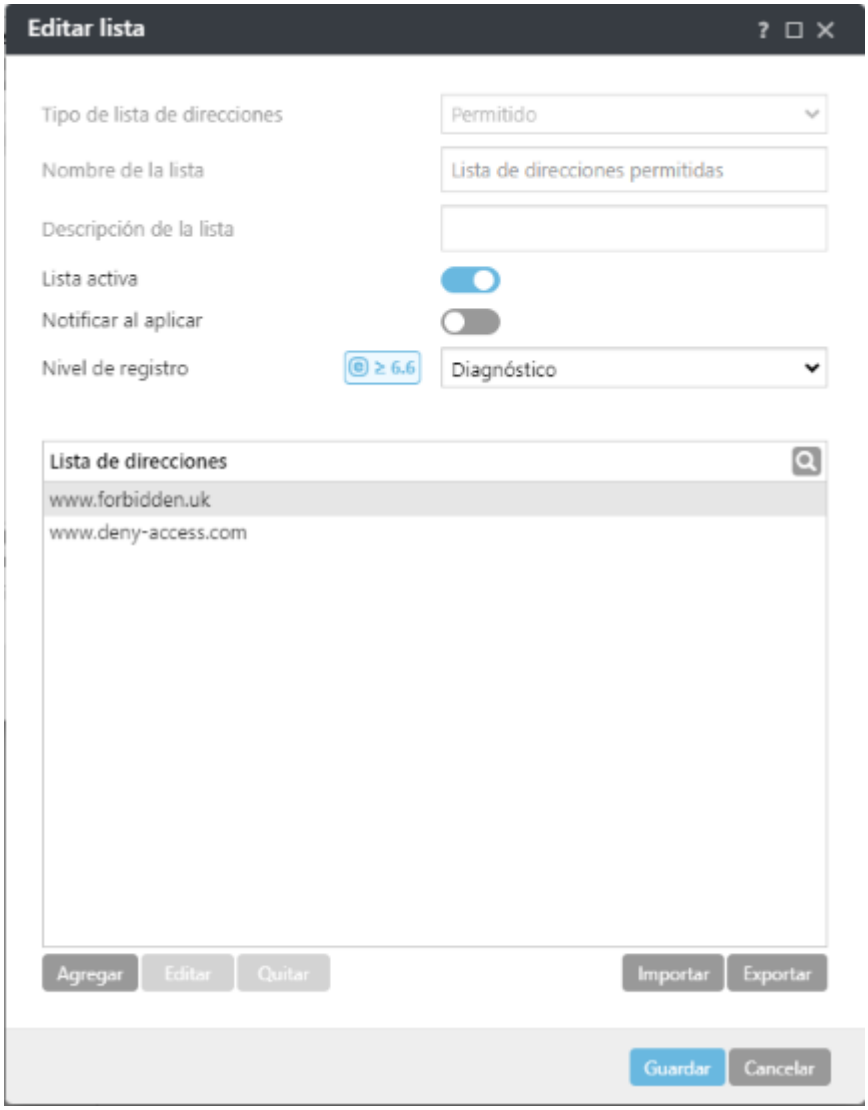


3. Desplazarse hasta **Políticas** y crear una nueva política:

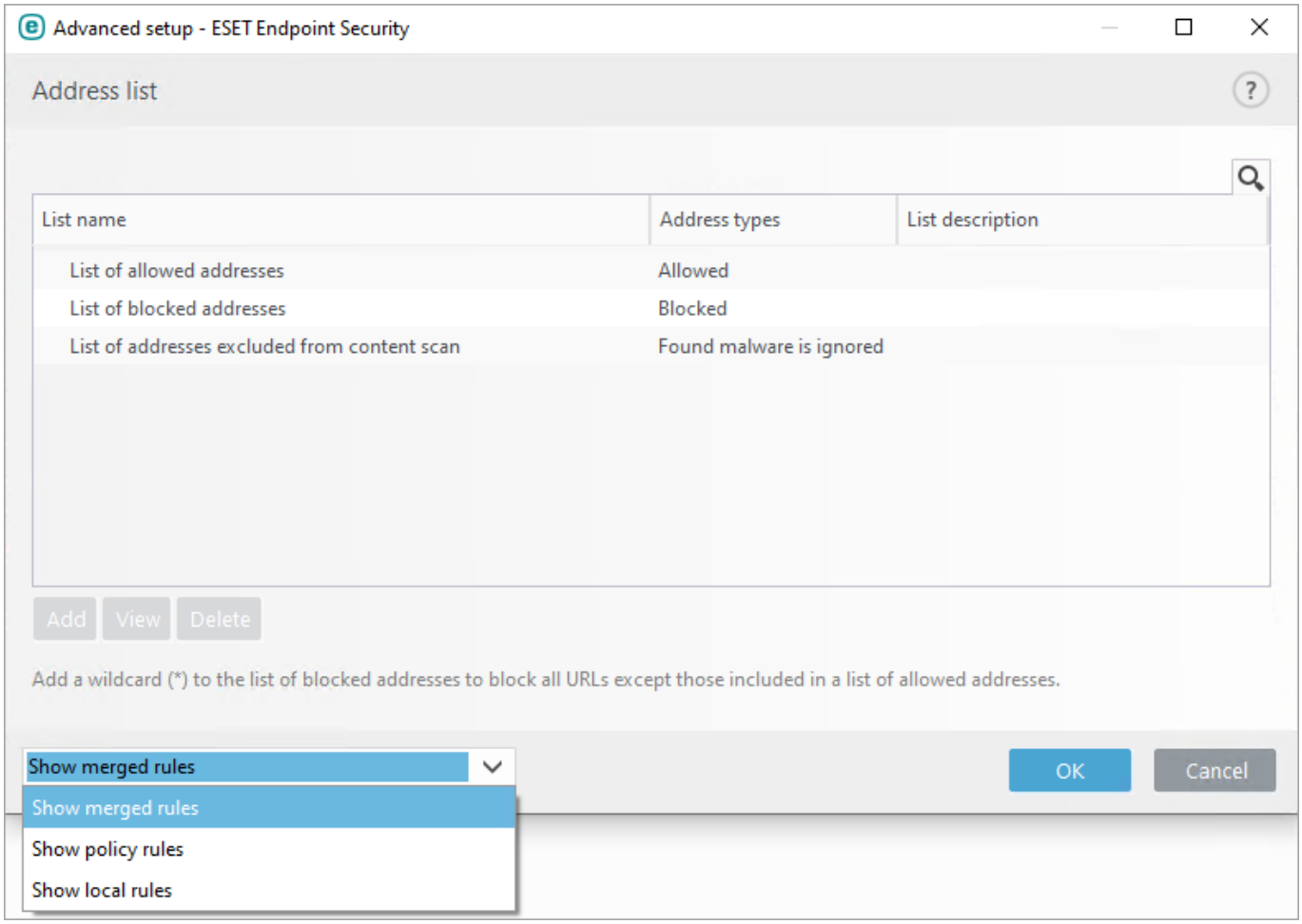
   i)Llamarla *Departamento de marketing*.
   ii)Desplegar **Configuración** y seleccionar **ESET Endpoint para Windows**
   iii)Ir a **Protecciones** > **Protección de acceso a la web** > **Administración de listas de URL**
   iv)Hacer clic en el botón para **Aplicar** la política, seleccionar la regla 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

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 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.

Ejemplos de uso de políticas para configurar productos de ESET:

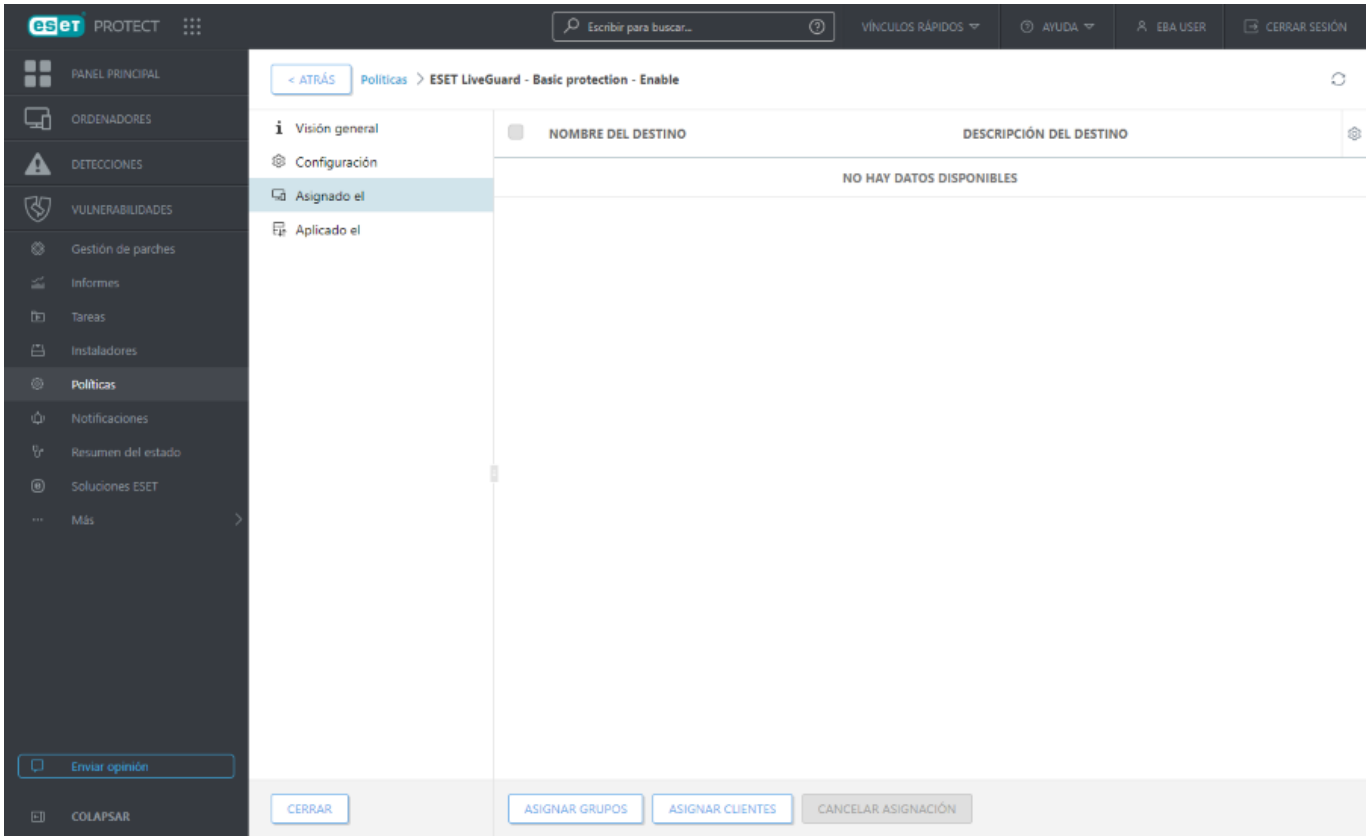
- Configuración de política de ESET Management Agent
- Configuración de políticas de ESET Rogue Detection Sensor

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:

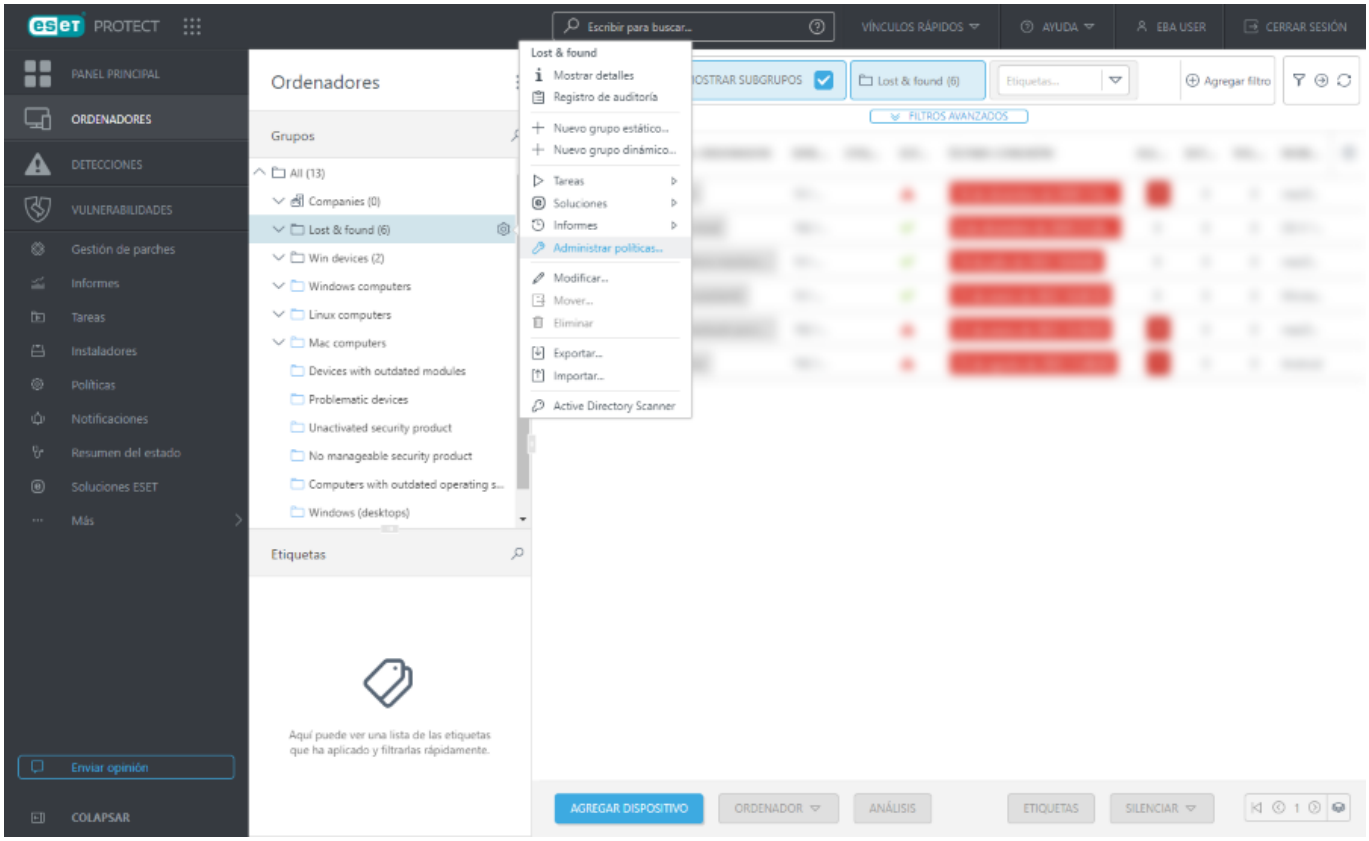
Método I.

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.

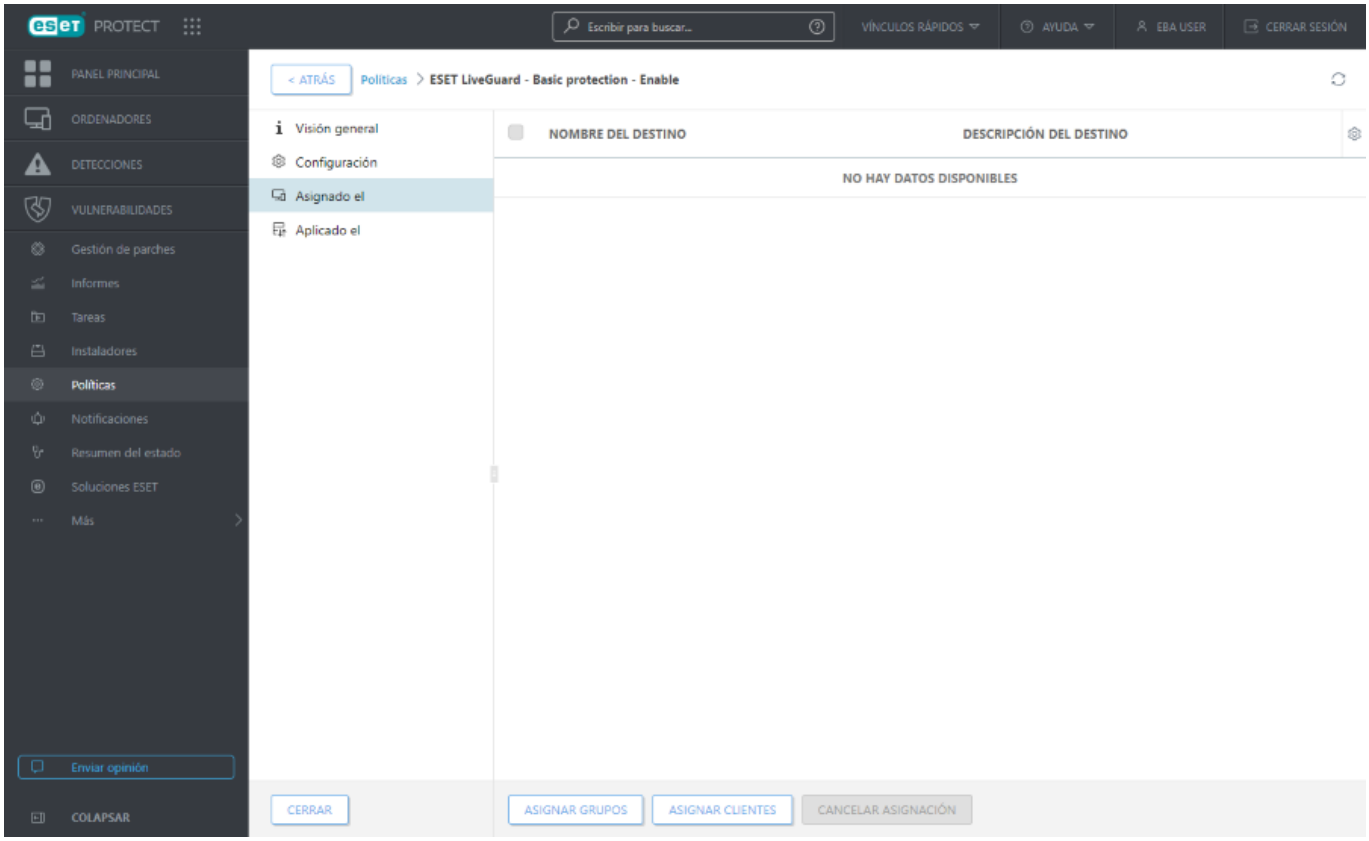
Para ver qué grupos están asignados a una política concreta, seleccione la política y haga clic en **Mostrar detalles** > **Aplicada a**.

para obtener más información acerca de las políticas, consulte el capítulo Políticas.

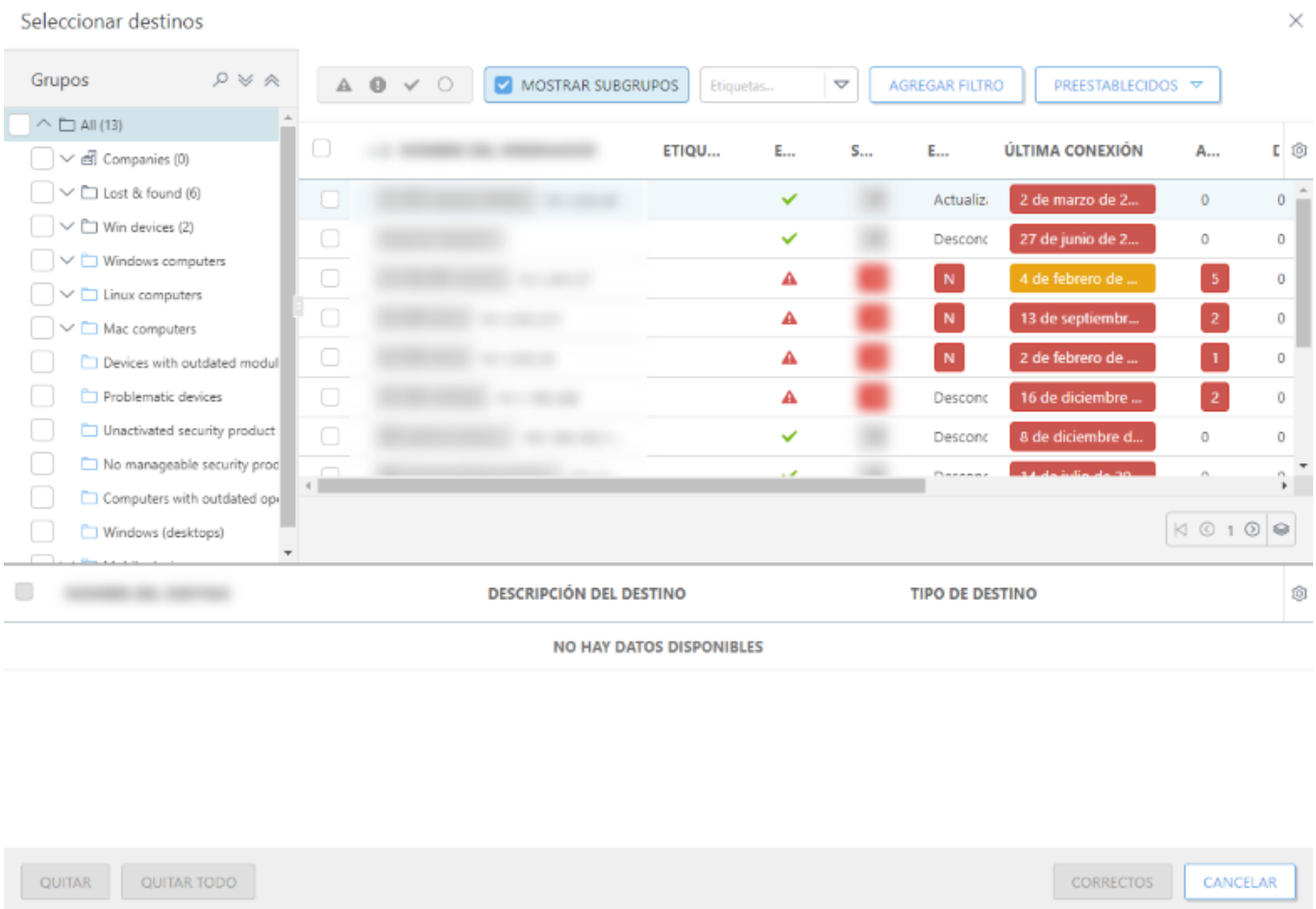
Asignar una política a un cliente

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

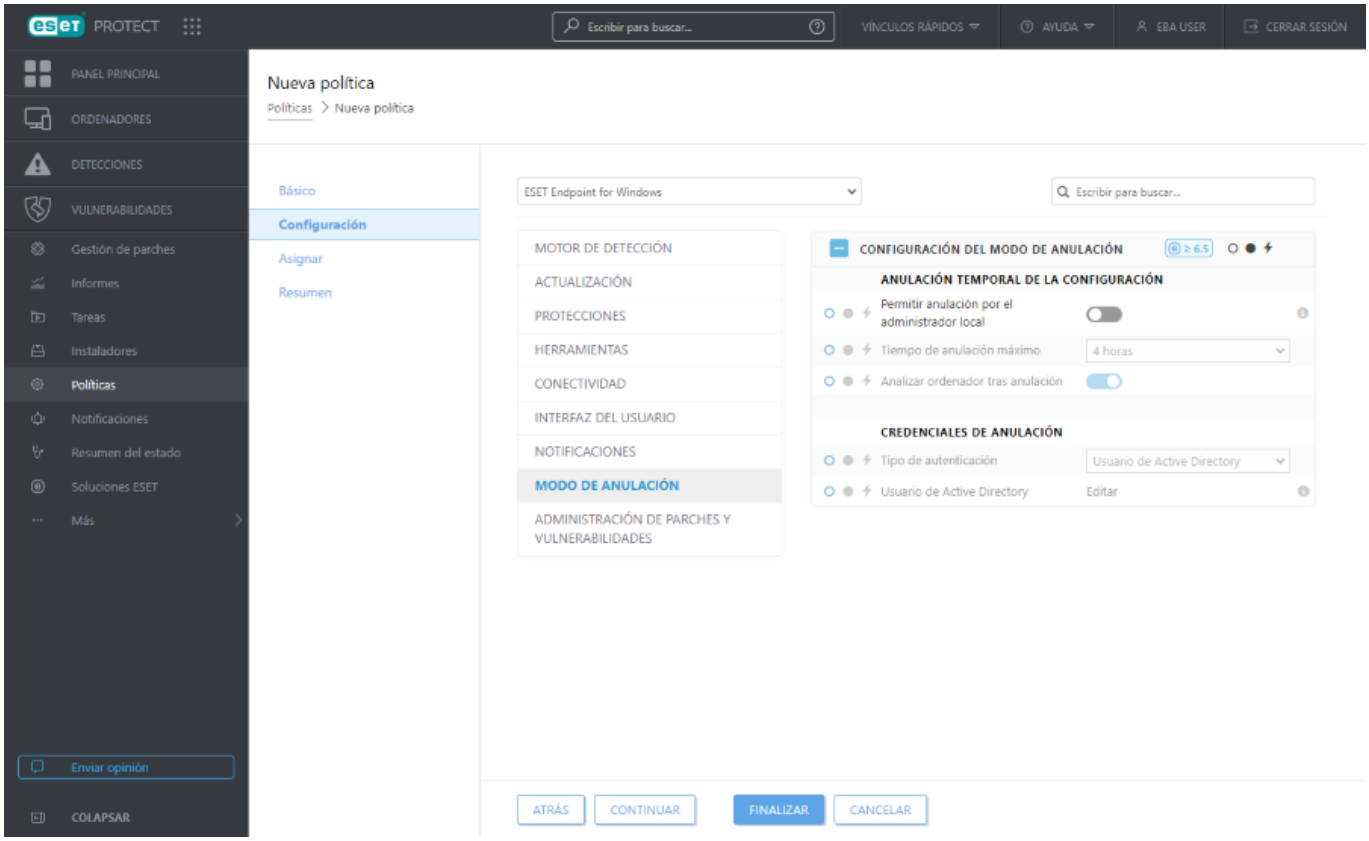
Los usuarios con productos ESET Endpoint para Windows instalados en sus máquinas podrán utilizar la función de anulación. Puede activar el modo de anulación solo de forma remota desde ESET PROTECT Web Console. El modo de anulación permite a los usuarios de nivel de ordenador cliente cambiar la configuración 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 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.

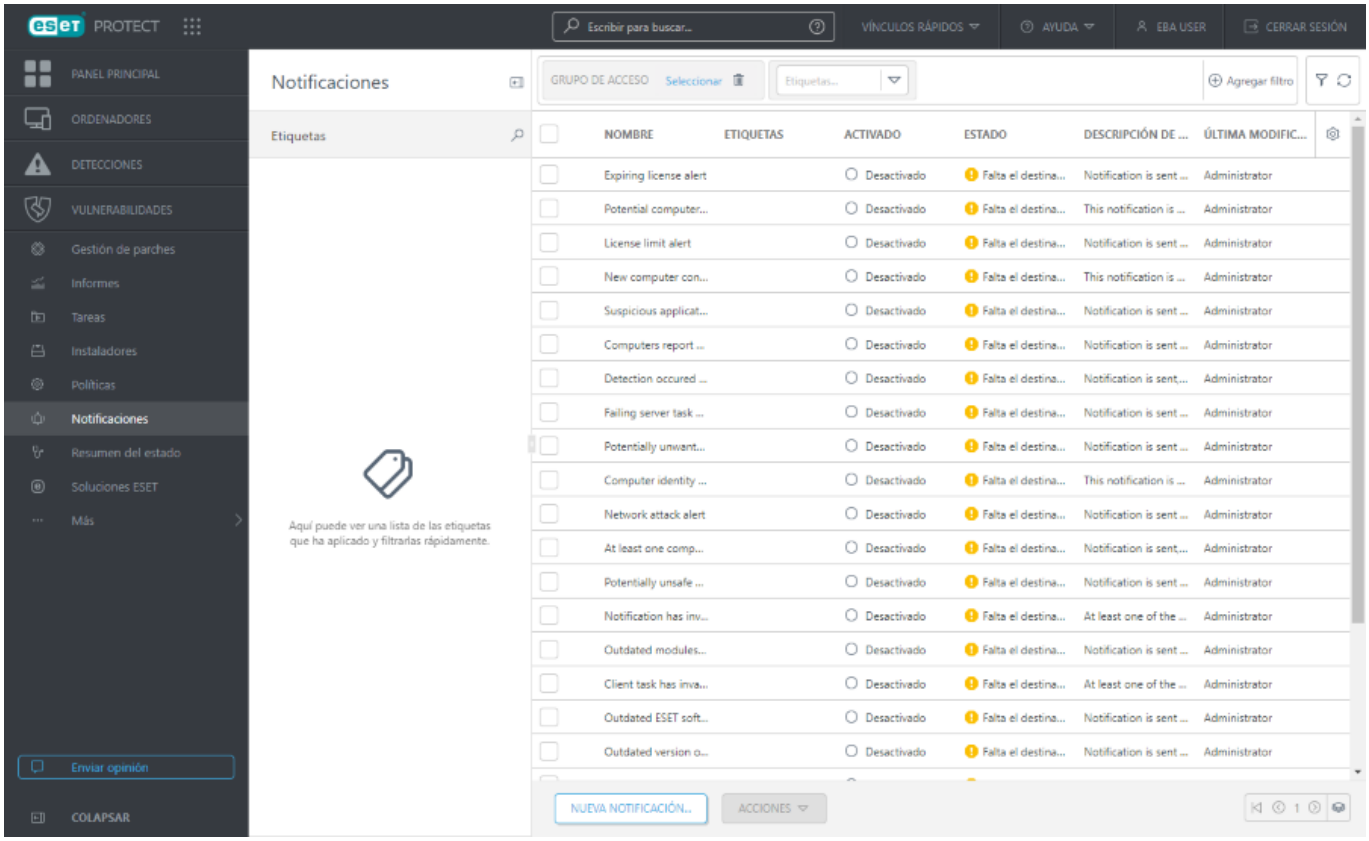
12. En la sección **Asignar**, puede asignar esta política al *Ordenador de John* (o a otros).

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 suceso (y según la configuración de notificaciones), se le informará de él mediante un mensaje de correo electrónico a la dirección de correo electrónico especificada para que pueda responder debidamente. El servidor SMTP necesario para enviar las notificaciones se configura automáticamente, por lo que no son necesarias modificaciones adicionales. 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.

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**
- **ESET Inspect incidentes**

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
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.
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 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 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.

Puede seleccionar ambos medios de distribución: **Enviar correo electrónico** y **Enviar webhook** y, a continuación:
1.Rellene la **Configuración de la distribución por correo electrónico**.
2.Rellene la **Configuración de distribución de webhook**.

Enviar correo electrónico

Si selecciona **Enviar correo electrónico**, inserte al menos un destinatario de correo electrónico.De forma predeterminada, el correo electrónico de notificaciones se envía en formato HTML e incluye un logotipo de ESET PROTECT en el encabezado.

Configuración de la distribución por 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.

Incluir un vínculo en el correo electrónico: marque la casilla para incluir un vínculo a Web Console con detalles sobre el evento de la notificación.

Enviar correo electrónico de prueba: haga clic en el botón **Enviar** para enviar un correo electrónico de prueba a la dirección anterior.

Enviar webhook

Puede utilizar ESET PROTECT para enviar notificaciones como webhooks. Puede recibir notificaciones de ESET PROTECT como mensajes en su canal de comunicación principal.

- **URL de webhook**: escriba la URL del webhook del canal de comunicación.

Vea un ejemplo de la URL de webhook de Teams a continuación:
https://xxxxx.webhook.office.com
Después de escribir la URL del webhook de Teams, no se muestra la **Carga útil de JSON**.

- **Incluir un vínculo en el contenido del webhook**: marque la casilla para incluir un vínculo en Web Console con detalles sobre el evento de la notificación; esta función es válida para los webhooks de Teams.
- Cuando escribe la URL de su webhook personalizado (no de Teams ni de Slack), puede seleccionar Autenticación

- **Carga útil JSON**: escriba el archivo JSON válido. Puede usar variables. Para ello, haga clic en **Agregar variable**

y seleccione la variable: **Asunto**, **Contenido**, **Vínculo**.

- Cuando rellene el **Asunto** y el **Contenido** en la **Vista previa del mensaje**, los valores de las variables se utilizarán en la **Carga útil de JSON**.

- Para crear una carga útil de JSON personalizada para un canal de comunicación de terceros, consulte su ayuda oficial, por ejemplo, Discord.

- **Autenticación**: se muestra cuando escribe un vínculo de webhook personalizado. Proteja sus datos y mejore la seguridad con la autenticación de webhook. Seleccionar:

  - **Sin autenticación**: seleccione esta opción cuando el receptor del webhook no tenga esquema de autenticación. Recomendamos agregar autenticación para proteger los datos y mejorar la seguridad.

  - **Token del portador**: escriba el token del portador en el campo **Token del portador**.

  - **Autenticación básica**: escriba los valores de los campos **Nombre de usuario** y **Contraseña**.

- **Enviar webhook de prueba**: haga clic en el botón **Enviar** para enviar un webhook de prueba al vínculo de webhook proporcionado.

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**

  - **Configuración regional**: idioma del mensaje predeterminado. El contenido del mensaje no está traducido.

  - **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.

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. También puede resultar útil en la configuración inicial de ESET PROTECT. Haga clic en **Resumen del estado** para ver información de estado detallada sobre ESET PROTECT.

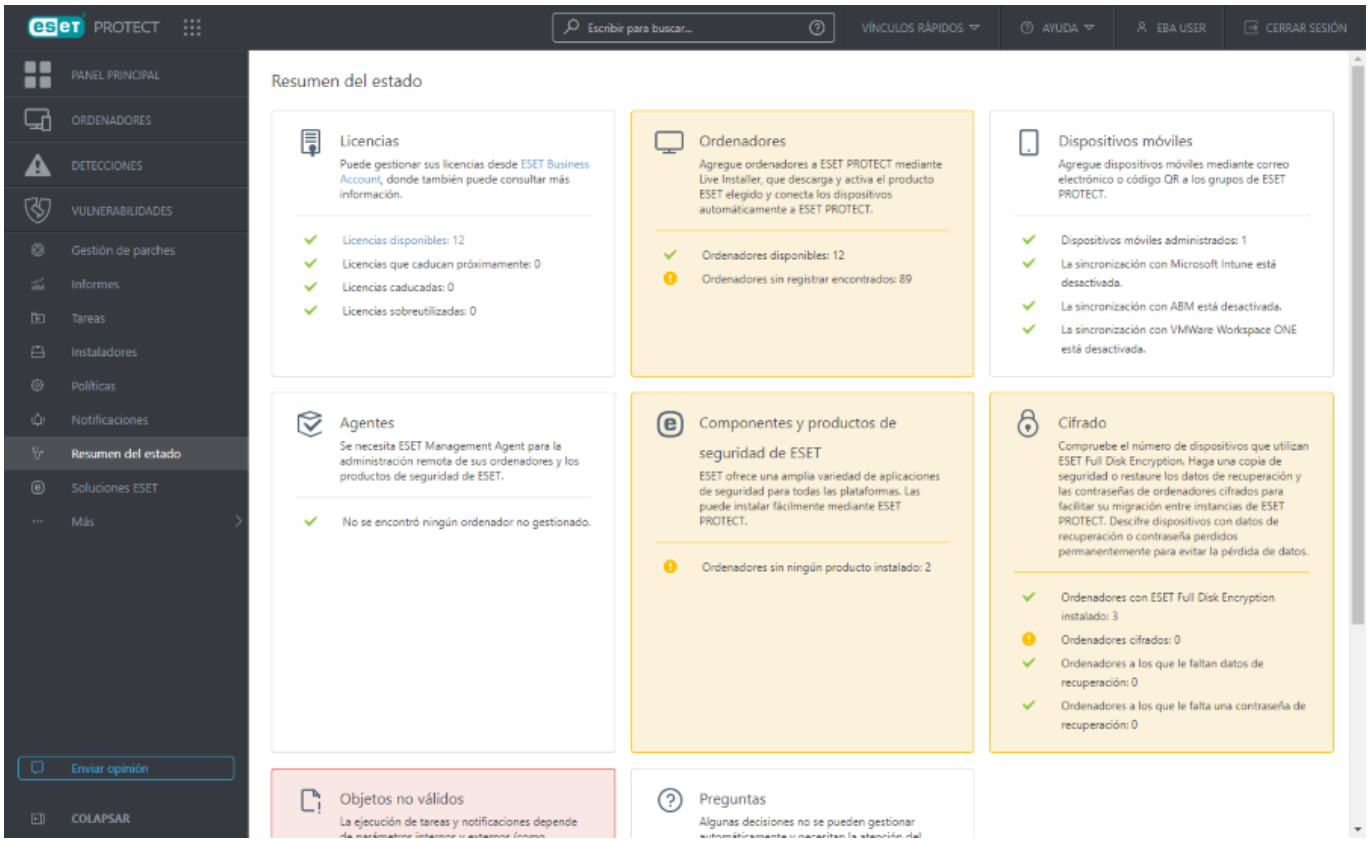
Haga clic en la ventana dinámica de una sección para mostrar una barra de tareas a la derecha con acciones. Cada ventana dinámica de sección puede tener un color de los varios existentes, según el estado de gravedad más alta de los elementos incluidos:

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:

Licencias	ESET PROTECT utiliza el sistema de licencias de ESET. Si desea administrar sus licencias, vaya a ESET Business Account.
Ordenadores	• **Agregar equipo**: agregue equipos en su red a la estructura de ESET PROTECT.
Dispositivos móviles	**Agregar dispositivos móviles**: inscriba dispositivos móviles. • **Configuración de inscripción con Microsoft Entra ID**: configure la inscripción con Microsoft Entra ID. • **Sincronización de Microsoft Intune**: configurar la sincronización con Microsoft Intune. • **Sincronización con ABM**: configure la sincronización con Apple Business Manager (ABM). • **Sincronización con VMware Workspace ONE**: configure la sincronización con VMware Workspace ONE.
Agentes	• **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. • **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). • **Configurar protección:** revise y ajuste la configuración de seguridad aplicada a todos los dispositivos conectados a ESET PROTECT.
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.

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.
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	Hay estados de MSP disponibles en instancias con una cuenta MSP.



Soluciones ESET

En esta sección se activa la implementación simplificada de los siguientes productos:

- **ESET LiveGuard Advanced**
- **ESET Full Disk Encryption**

Para cada uno de los productos, puede seleccionar una de las siguientes opciones:

- **Probar**: solicite una licencia de prueba para un producto seleccionado si tiene usuarios sin licencia.
- **Comprar**: compre una licencia del producto seleccionado.
- **Activar**: active el producto seleccionado en todos los dispositivos aptos. Para obtener más información, consulte las subsecciones de cada uno de los productos.

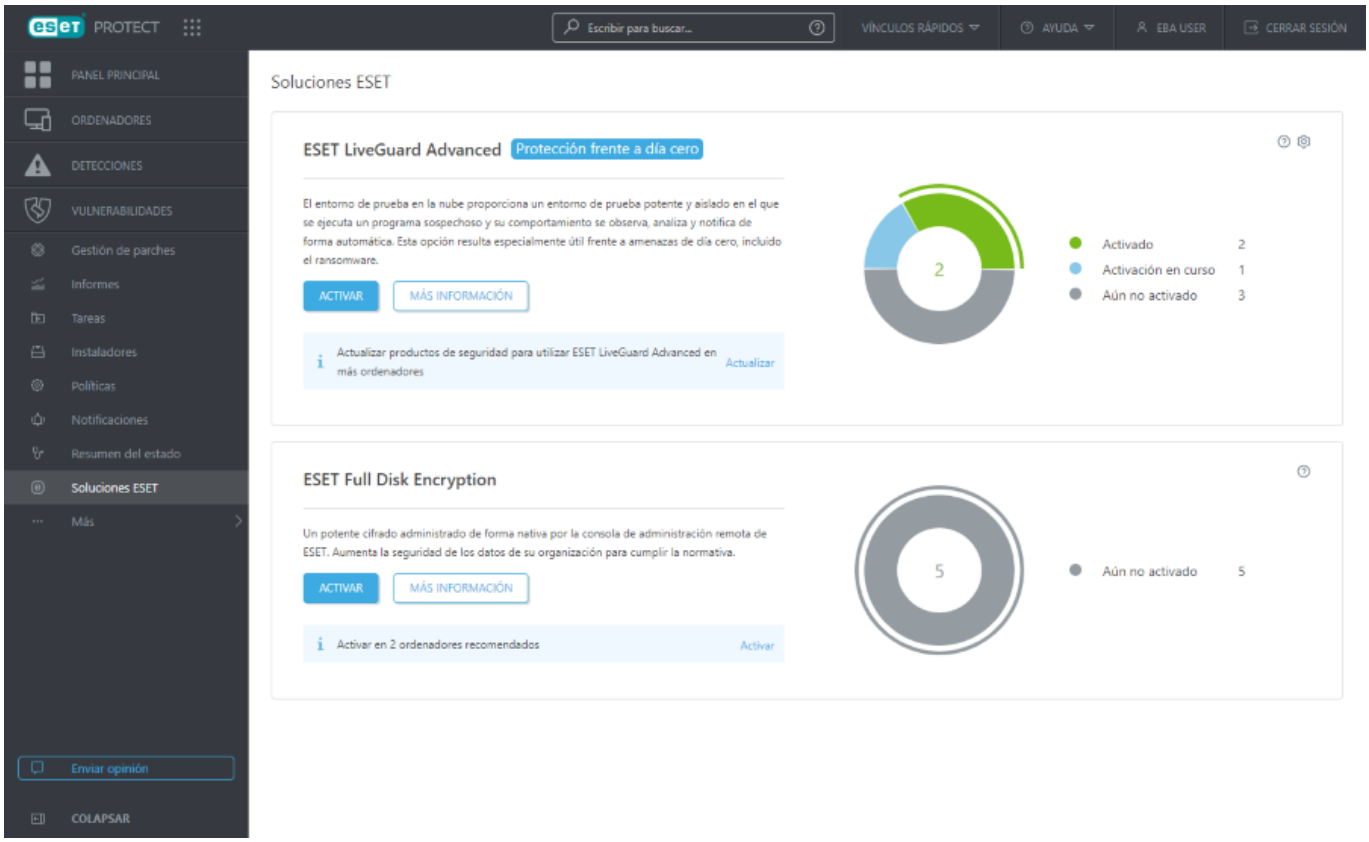
- Haga clic en el **icono del engranaje** > **Quitar** para quitar ESET LiveGuard Advanced o ESET Full Disk Encryption de todos los dispositivos.

- **Más información**: abre una página con información sobre el producto seleccionado.

También puede acceder a los **detalles** de cada una de las categorías representadas en el gráfico, donde se muestran los primeros 100 dispositivos.

Limitaciones de implementación

- La cuenta de usuario necesita permiso de **Escritura** para activar esta funcionalidad.
- Cada empresa MSP cuenta únicamente con una opción de un solo uso para probar esta funcionalidad.



Activar ESET LiveGuard Advanced

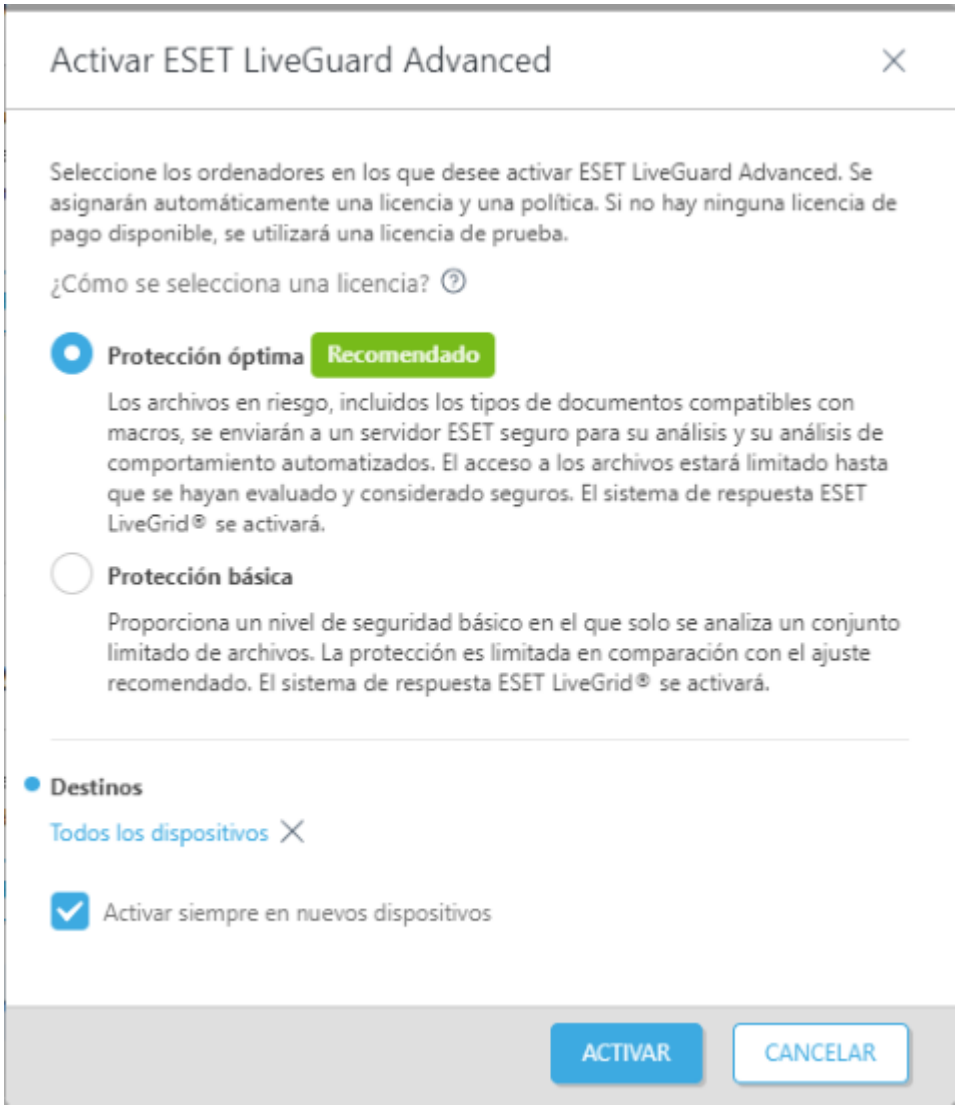
Seleccione la sección **Soluciones de ESET**. En **ESET LiveGuard Advanced**, haga clic en **Comprar** para ir al procedimiento de actualización del nivel de protección de ESET PROTECT. Cuando termine la actualización, podrá implementar y activar la funcionalidad de ESET LiveGuard Advanced en la red administrada.

Licencia de prueba

Si ya tiene una licencia de prueba activa y compra una licencia completa del producto, aparecerá una nueva opción para migrar los dispositivos a la licencia completa.

Si selecciona **Implementar**, se mostrará una nueva ventana. En ella puede seleccionar **Protección óptima** (opción recomendada) o **Protección básica**. Seleccione los valores de **Destinos** para la implementación. Puede dejarla en la selección predeterminada de **Todos los dispositivos**, o puede seleccionar manualmente los dispositivos de destino y los grupos estáticos o dinámicos. Si mantiene la selección predeterminada de **Todos los dispositivos**, puede marcar la casilla de verificación **Activar siempre en nuevos dispositivos** para activar la implementación

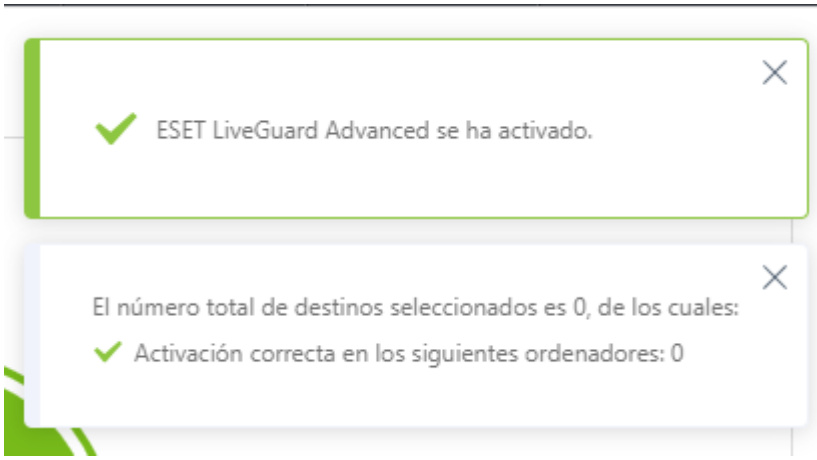
automática de ESET LiveGuard Advanced en todos los nuevos dispositivos que administrará ESET PROTECT en el futuro. Seleccione **Activar** para confirmar su decisión.



> **Protección básica**: La implementación se ejecuta con una política integrada **ESET LiveGuard: Activar**.
> **Protección óptima** La implementación se ejecuta con una política integrada **ESET LiveGuard - Protección óptima: Activar**.

ESET PROTECT ejecutará la Tarea de activación para ESET LiveGuard Advanced en todos los dispositivos administrados seleccionados.

A la derecha aparecerá una pequeña notificación que mostrará los detalles de la implementación.

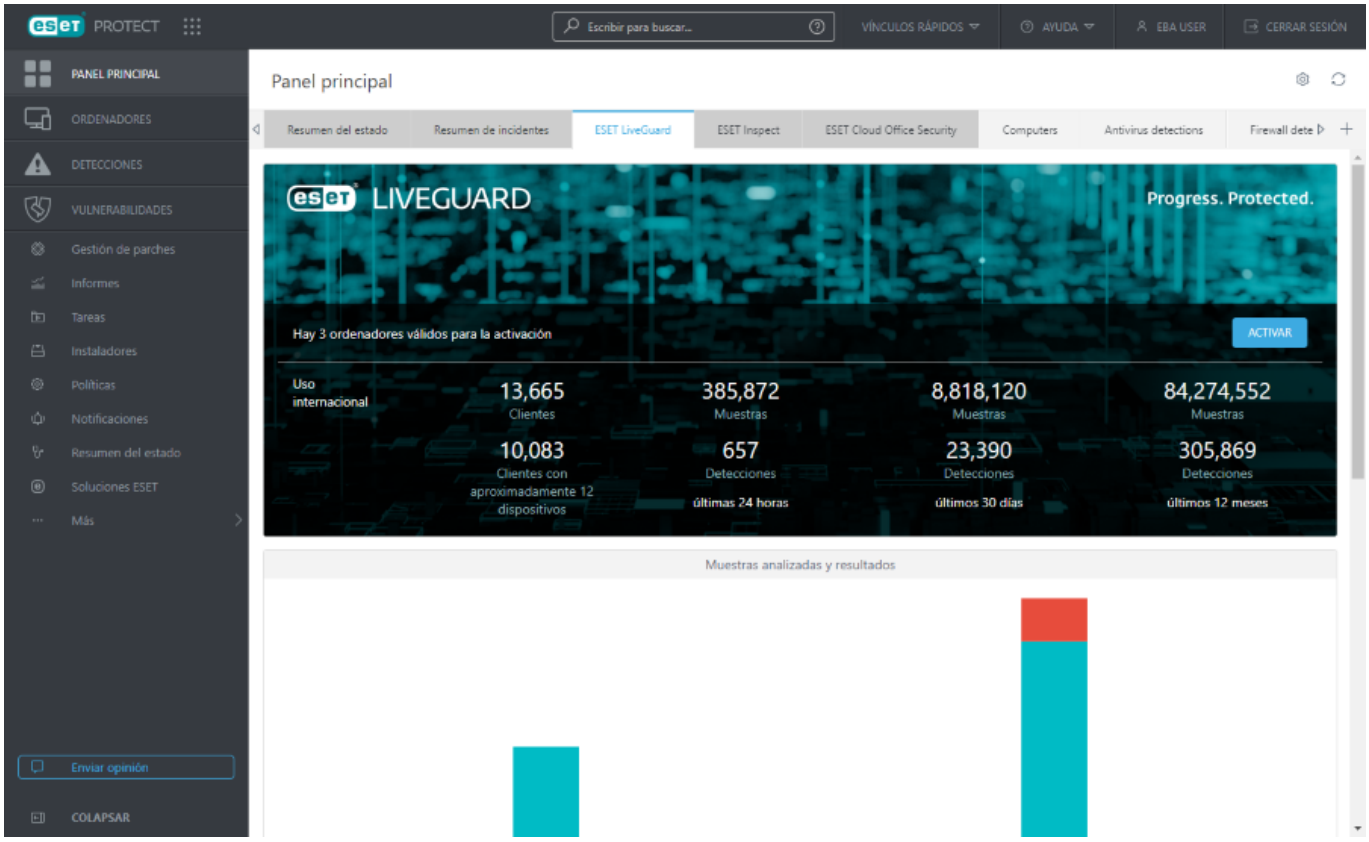


Puede revisar el progreso en **Soluciones de ESET**.

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.



Eliminar ESET LiveGuard Advanced

Haga clic en el icono del engranaje situado en la parte superior derecha de la ventana **ESET LiveGuard Advanced** y seleccione **Eliminar ESET LiveGuard Advanced** para eliminar ESET LiveGuard Advanced de los dispositivos administrados. ESET PROTECT desactivará ESET LiveGuard Advanced y eliminará la opción de política correspondiente de todos los dispositivos seleccionados.

Desactivar implementación automática

Haga clic en el icono del engranaje situado en la parte superior derecha de la ventana **ESET LiveGuard Advanced** y seleccione **Desactivar implementación automática** para desactivar la implementación automática en los nuevos dispositivos.

Activar ESET Full Disk Encryption

Seleccione la sección **Soluciones de ESET**. En **ESET Full Disk Encryption**, haga clic en **Comprar** para ir al procedimiento de actualización del nivel de protección de ESET PROTECT. Cuando termine el procedimiento de actualización, podrá implementar y activar el producto ESET Full Disk Encryption en la red administrada.

Seleccione la opción **Activar** y aparecerá una nueva ventana:

1. **Destinos**: mantenga el valor predeterminado (**Todos los dispositivos**) o seleccione los destinos (dispositivos, grupos estáticos o dinámicos).

2. **Idioma**: seleccione el idioma de ESET Full Disk Encryption que se implementará en todos los dispositivos seleccionados.

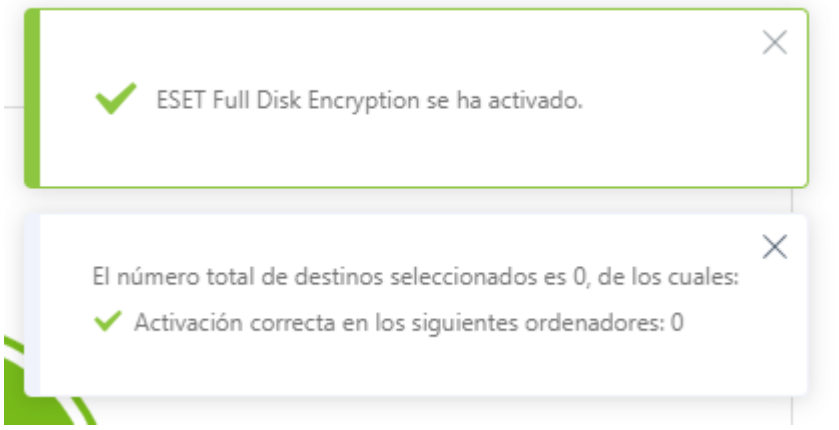
3. Marque la casilla **Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad**. Consulte el Acuerdo de licencia para el usuario final (EULA), los Términos de uso y la Política de privacidad de los productos de ESET.

4. Haga clic en **Activar**. ESET PROTECT ejecutará la Tarea de activación y la Tarea de instalación de software de ESET Full Disk Encryption en todos los dispositivos administrados seleccionados.

> La implementación se ejecuta con la política integrada **Cifrar todos los discos: se usa TPM si está disponible y no se usa OPAL**.

A la derecha aparecerá una pequeña notificación que mostrará los detalles de la implementación.

> El usuario del dispositivo administrado debe seguir pasos adicionales para implementar ESET Full Disk Encryption. Siga los pasos descritos en la documentación de ESET Full Disk Encryption.



Puede revisar el progreso en **Soluciones de ESET**.

Eliminar ESET Full Disk Encryption

Haga clic en el **icono del engranaje** situado en la parte superior derecha de la ventana **ESET Full Disk Encryption** y seleccione **Eliminar ESET Full Disk Encryption** para eliminar ESET Full Disk Encryption de los dispositivos administrados. ESET PROTECT desactivará ESET Full Disk Encryption, descifrará todos los discos cifrados y eliminará la opción de política correspondiente de todos los dispositivos seleccionados.

La eliminación se ejecuta con la política integrada **Descifrar todos los discos**.

Más

La sección **Más** es el componente de configuración avanzada de ESET PROTECT. Esta sección contiene herramientas que el administrador puede utilizar para administrar las soluciones de seguridad del cliente, así como la configuración de ESET PROTECT. 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
Auditoría de actividad oRegistro de auditoría
Admin oConfiguración

Archivos enviados

ESET LiveGuard Advanced es un servicio que ofrece protección avanzada ante detecciones nunca vistas. Un usuario de ESET PROTECT 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.

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:

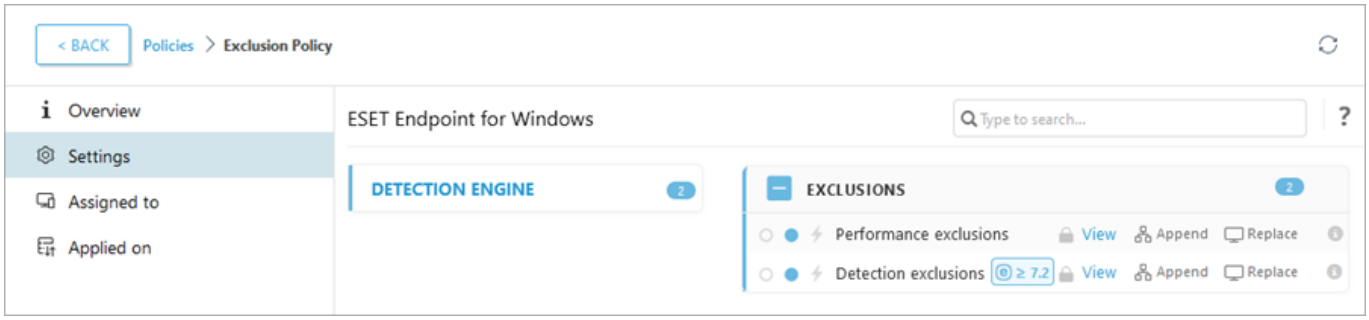
- **Cambiar asignación** : cambie los ordenadores de destino en los que se aplicará la exclusión.
- **Mostrar ordenadores afectados**: vea los ordenadores en los que se aplica la exclusión.
- **Registro de auditoría**: muestre el registro de auditoría de la exclusión seleccionada.
- **Eliminar**: elimine 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.

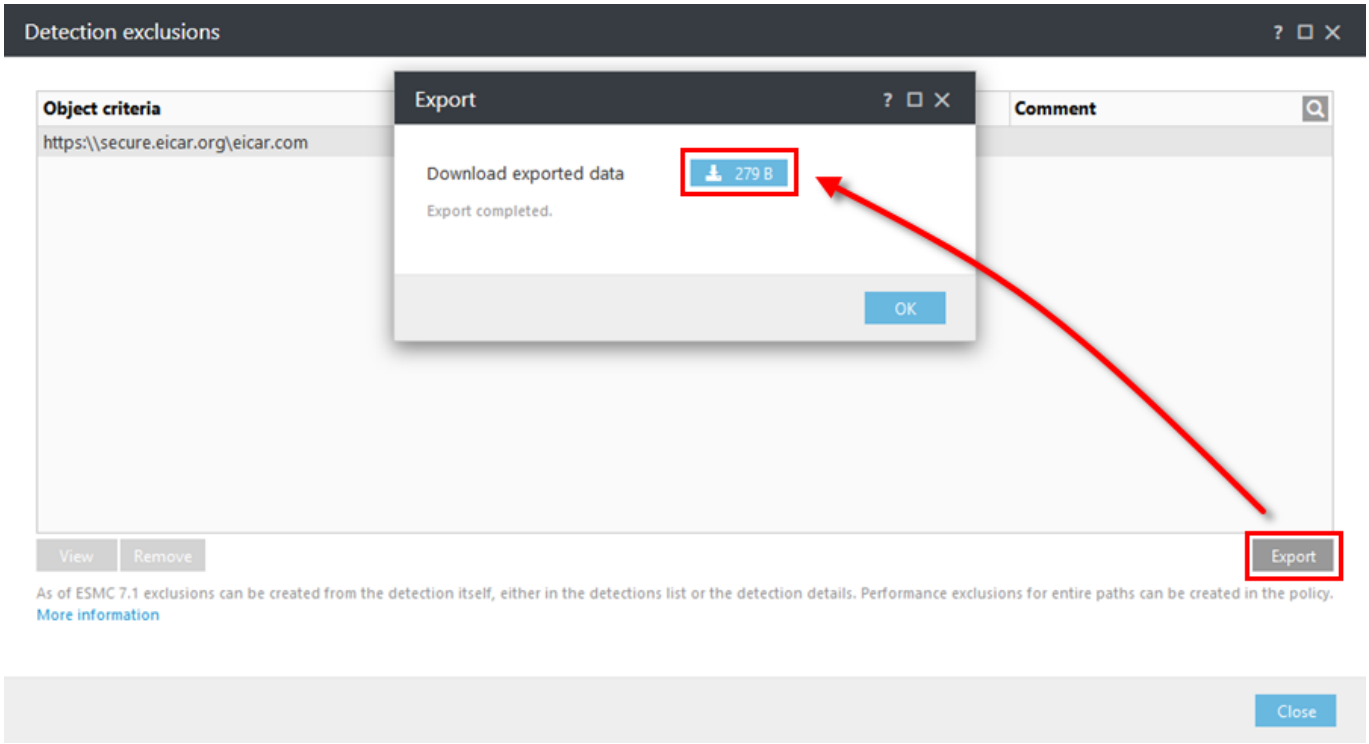
Migrar exclusiones desde una política

En ESET PROTECT 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:

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**.

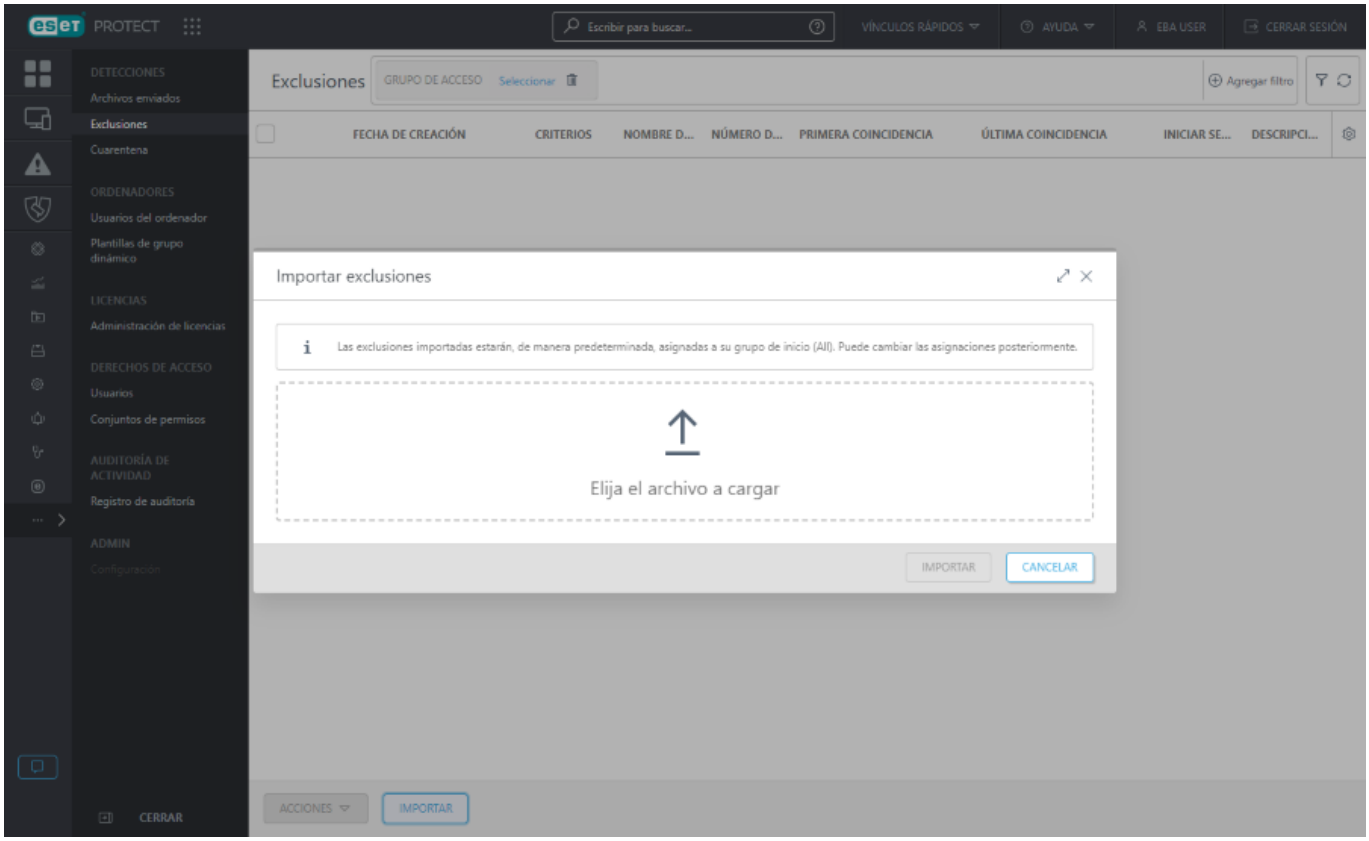


4. Haga clic en el botón **Exportar** y, a continuación, haga clic en el botón situado junto a **Descargar los datos exportados** y guarde el archivo *export.txt*. Haga clic en **Aceptar**.



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:

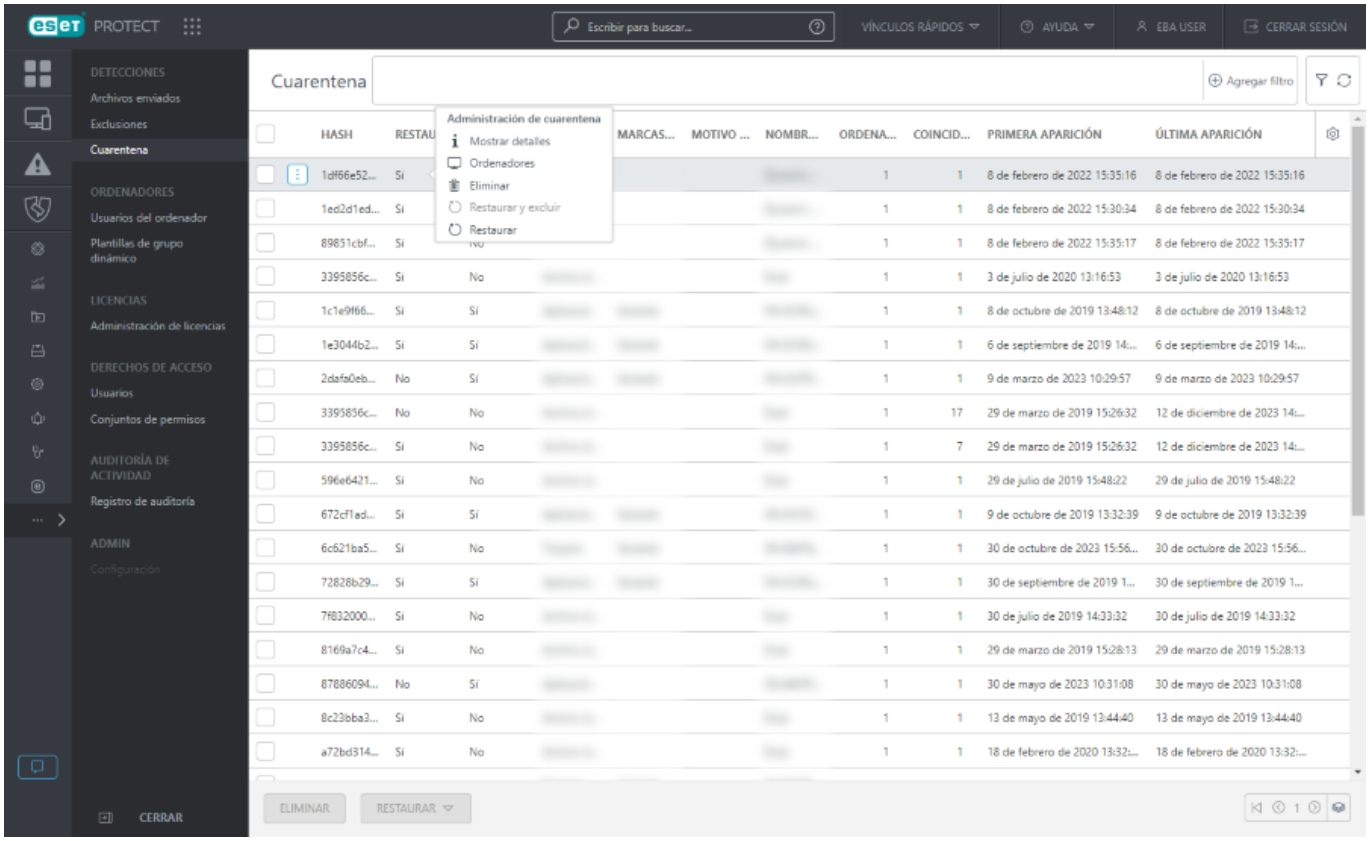
- Administre el panel lateral y la tabla principal.
- Agregar filtros y preajustes de filtros. Puede usar etiquetas para filtrar los elementos mostrados.

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 ESET PROTECT Web Console**. La sección Usuarios del ordenador le permite emparejar un usuario con un dispositivo para sincronizar algunos ajustes específicos del usuario. Para administrar los usuarios y conjuntos de permisos de la Consola web de ESET PROTECT, vaya a ESET Business Account.

- 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.

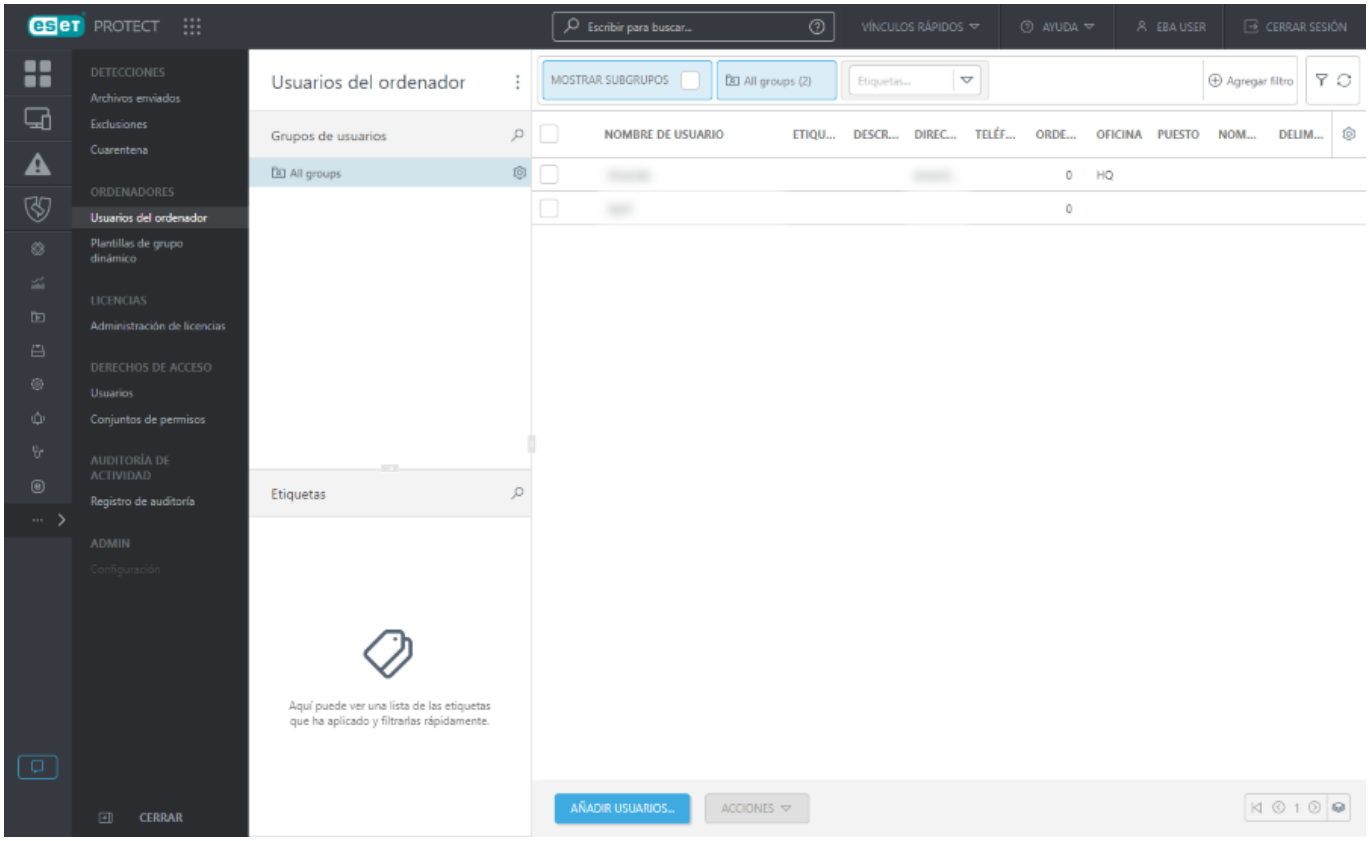
Filtros y personalización del diseño

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.

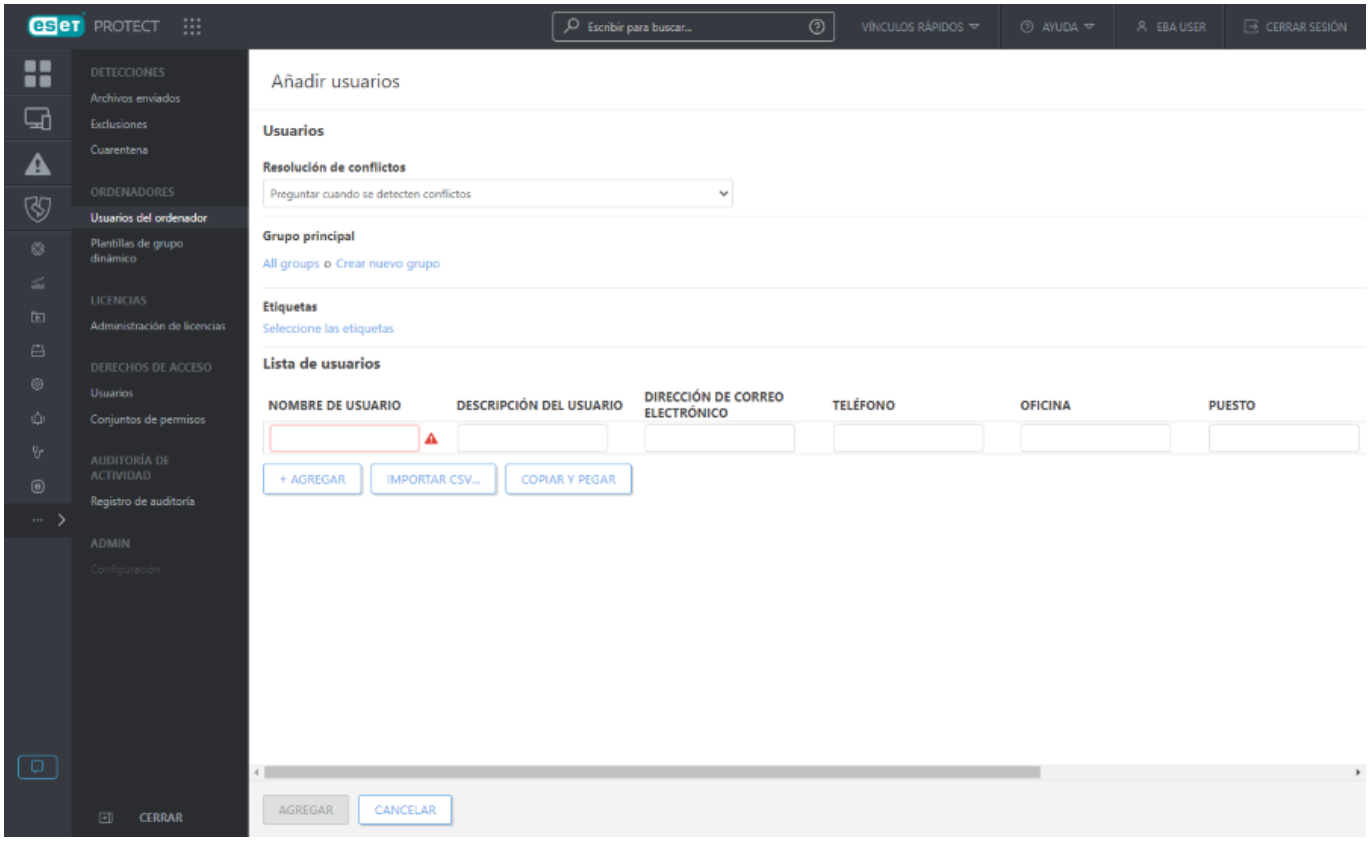
5. Utilice el menú desplegable **Resolución de conflictos** para seleccionar la acción que desee realizar si un usuario que está agregando ya existe en ESET PROTECT:

- **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 se conservarán (no se sobrescribirán con los datos de Active Directory).

- **Sobrescribir usuarios que causan conflictos:**: los usuarios existentes en ESET PROTECT se sobrescribirán por los usuarios de Active Directory. Si hay dos usuarios con el mismo SID, el usuario existente en ESET PROTECT 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.



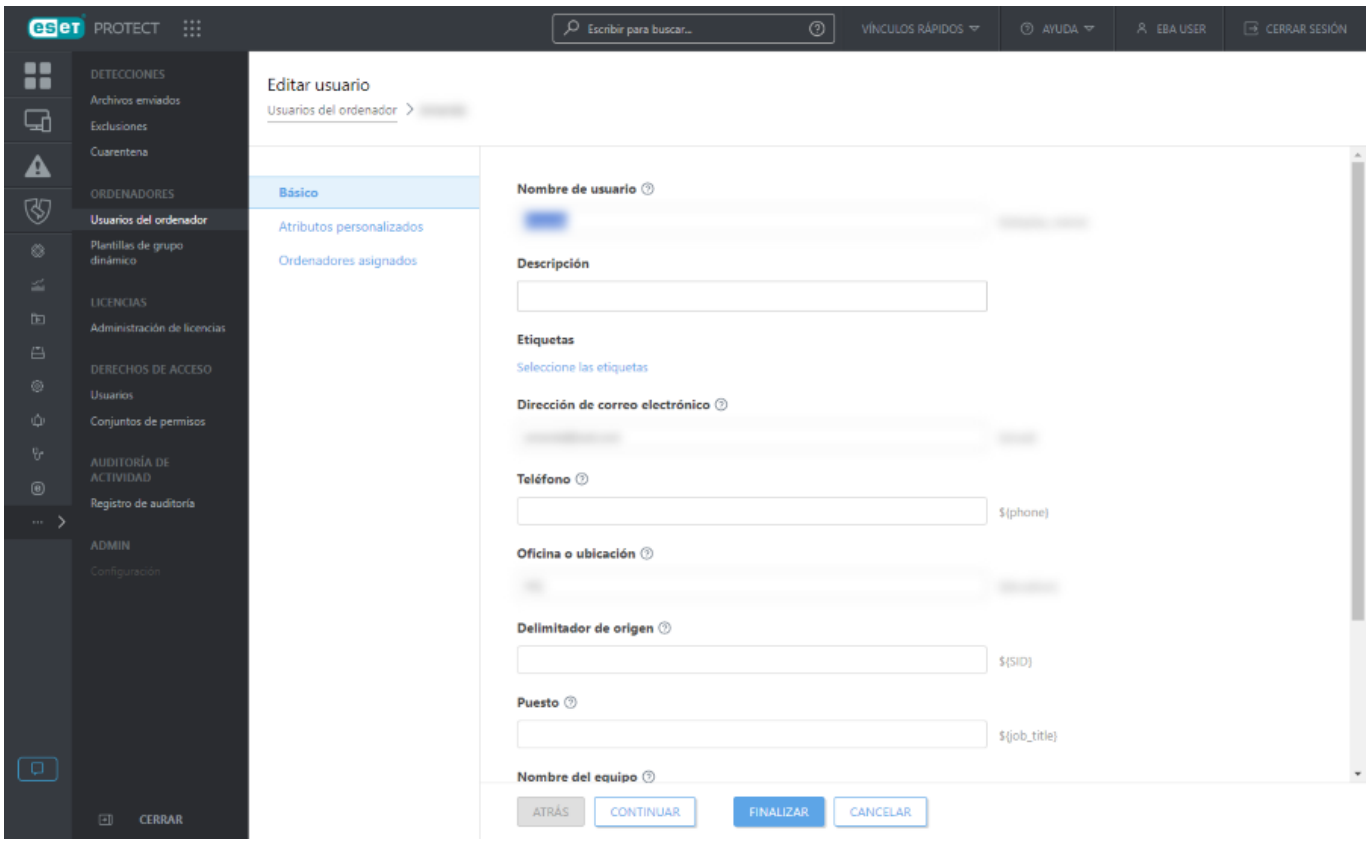
Modificar usuarios

Puede modificar detalles del usuario tales como la información **básica** y los **Ordenadores asignados**.

Básico

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.
- **Delimitador de origen**: se lo puede asociar con varias funciones de ESET PROTECT 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.

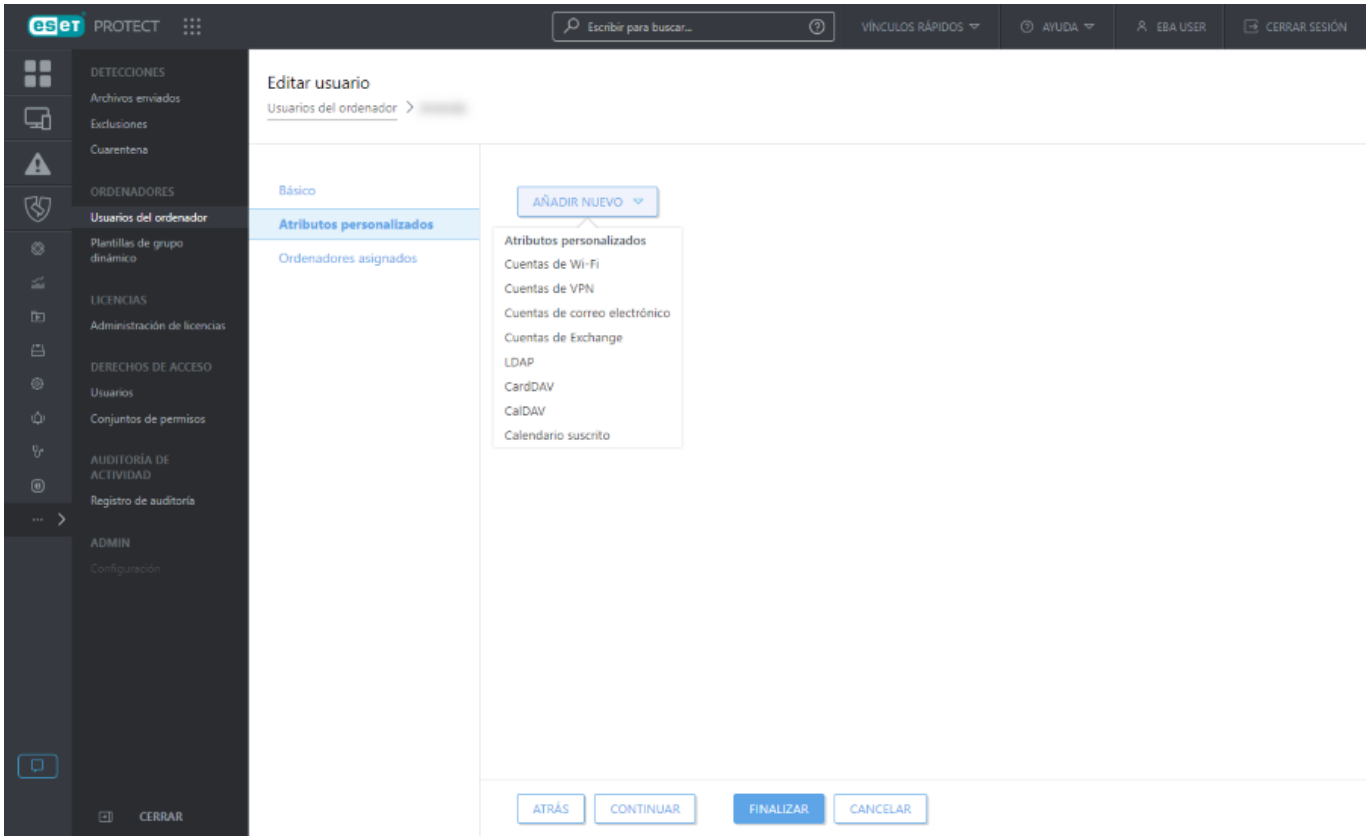
• **LDAP (alias del atributo)**: esta opción resulta especialmente útil si su empresa utiliza LDAP para los contactos. Puede asignar los campos de contacto a los campos de contacto de iOS correspondientes.

• **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}`.

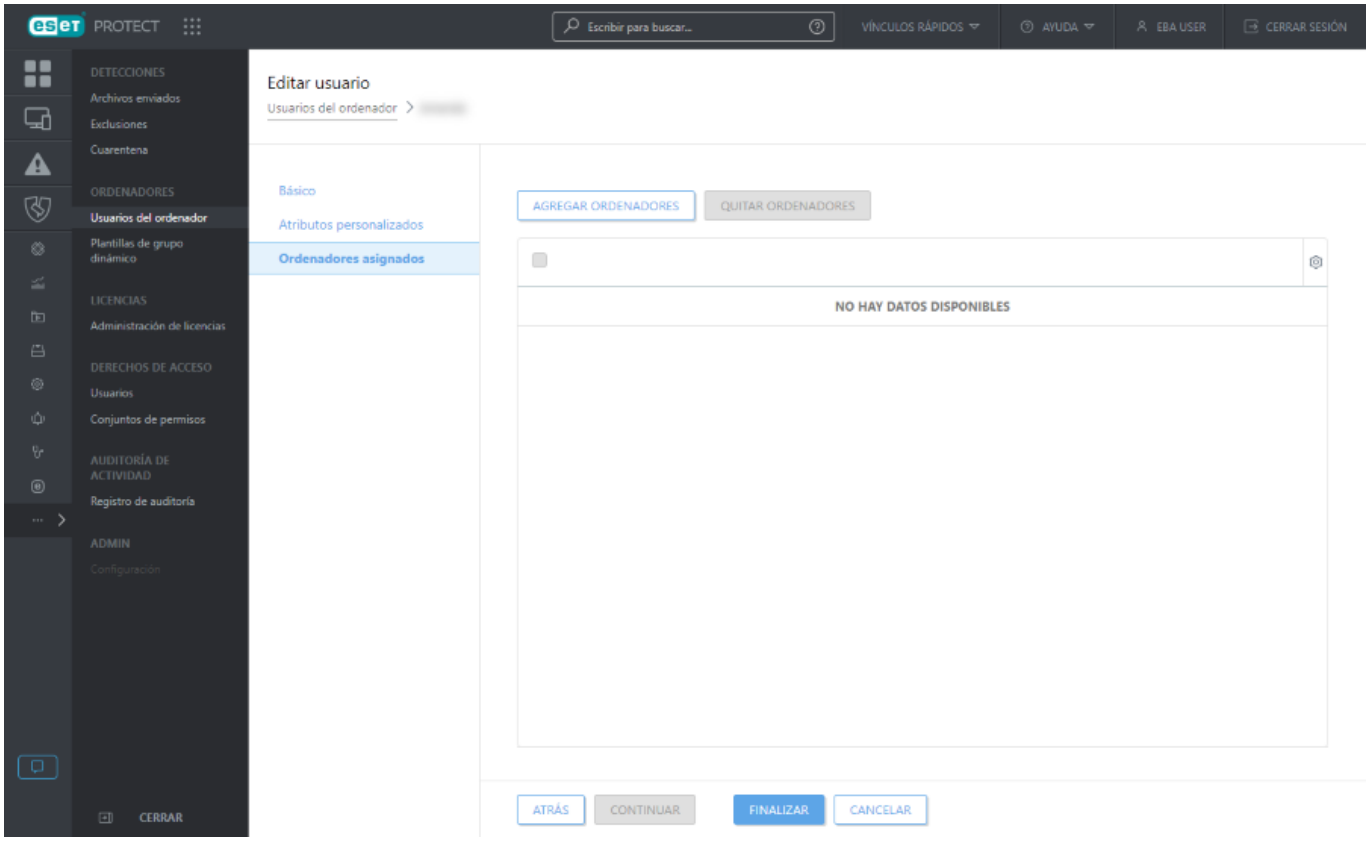


Ordenadores asignados

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.

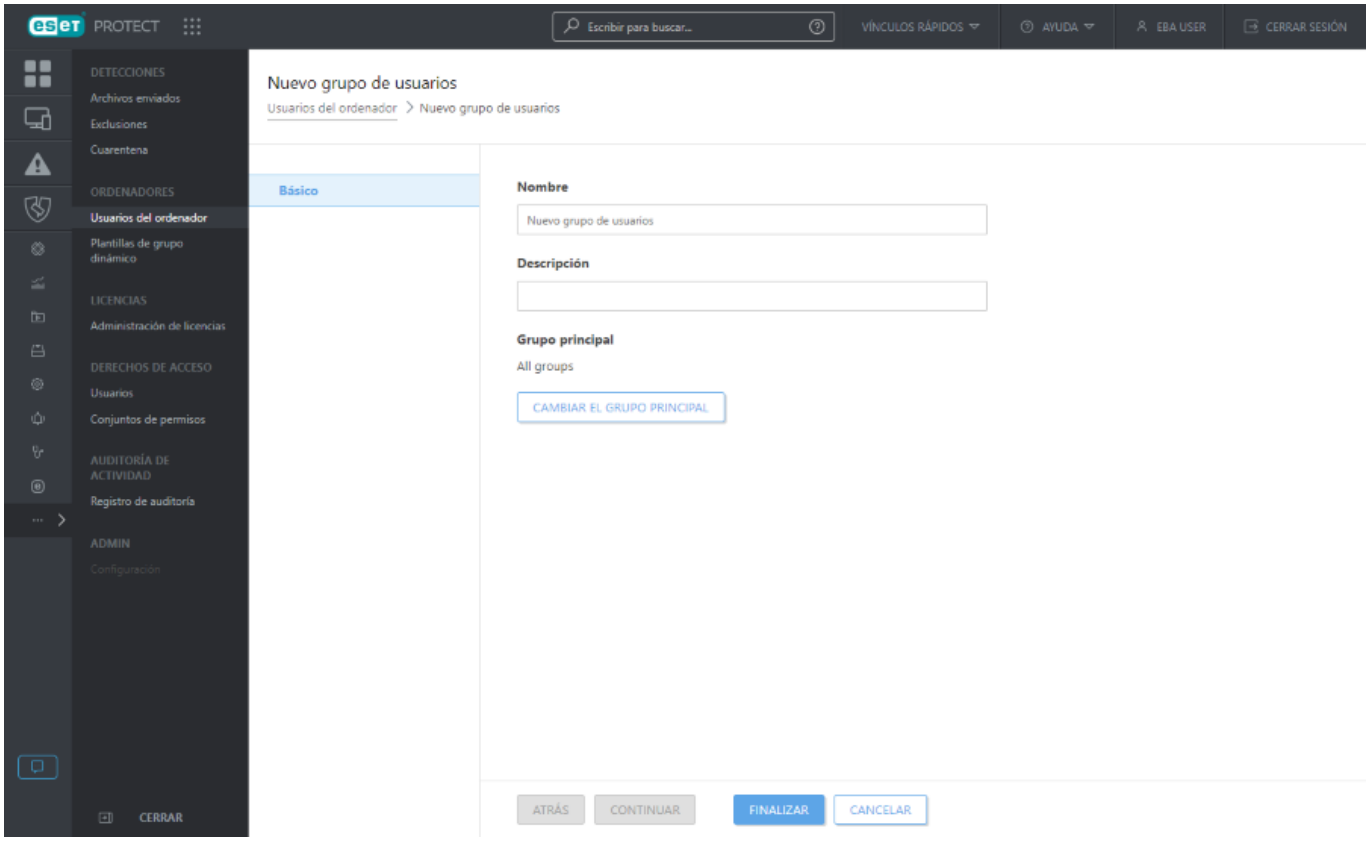


Crear un nuevo grupo de usuarios

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.



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

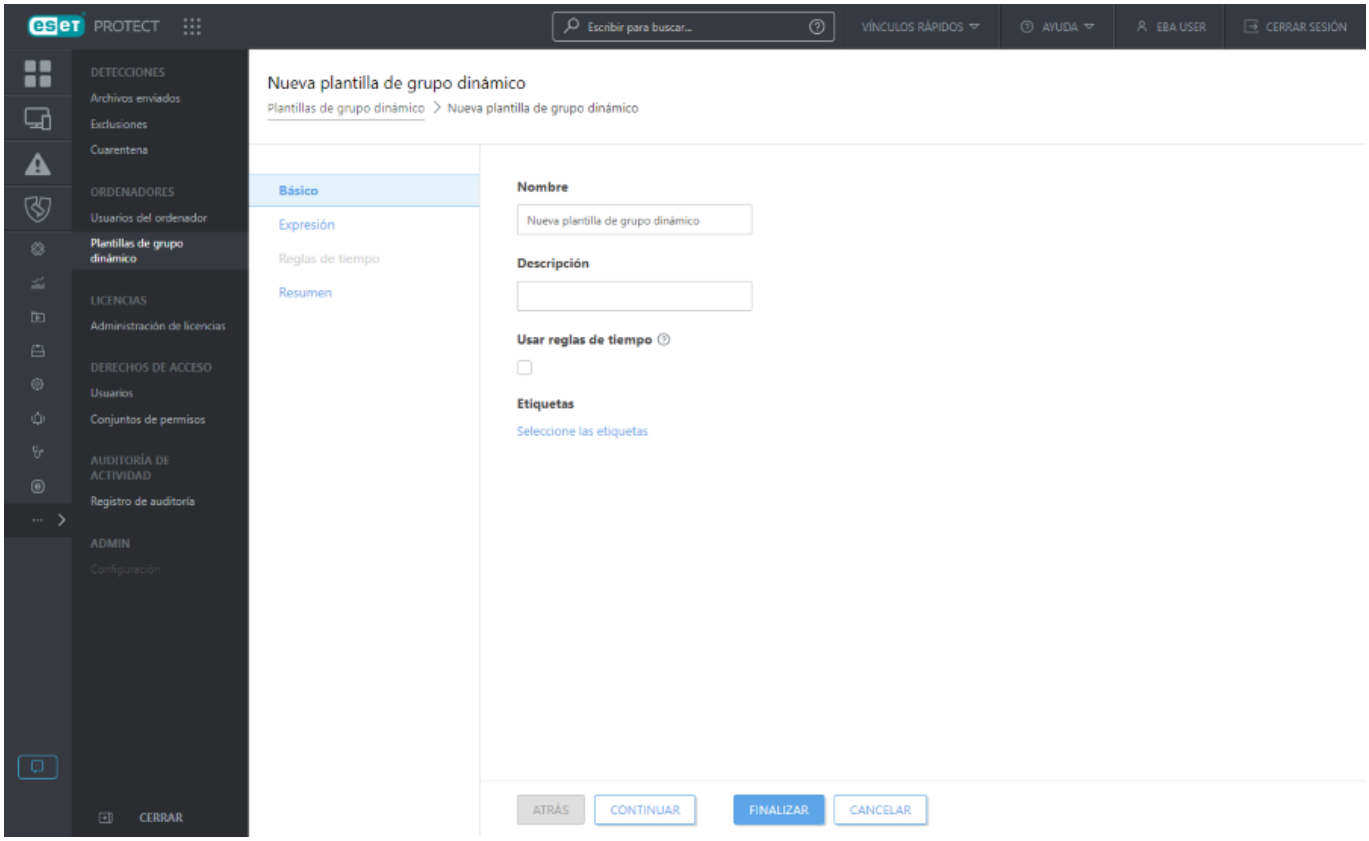
Introduzca un **nombre** y una **descripción** para la nueva plantilla de grupo dinámico.

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

- 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**.

> 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"**

> 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
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
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: 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 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
Cree un certificado nuevo para que las estaciones de trabajo nuevas se unan automáticamente a un grupo dinámico en ESET PROTECT

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

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

Puede administrar fácilmente sus licencias con ESET PROTECT desde el menú principal en **Más** > **Administración de licencias**. Puede ver aquí las licencias sincronizadas desde ESET Business Account que ha utilizado para la implementación de ESET PROTECT.

Para utilizar licencias de otro ESET Business Account, debe mover licencias al ESET Business Account que utilizó para la implementación de ESET PROTECT.

Puede activar el producto empresarial de ESET con ESET PROTECT.

Consulte también Preguntas frecuentes sobre licencias (usuarios empresariales).

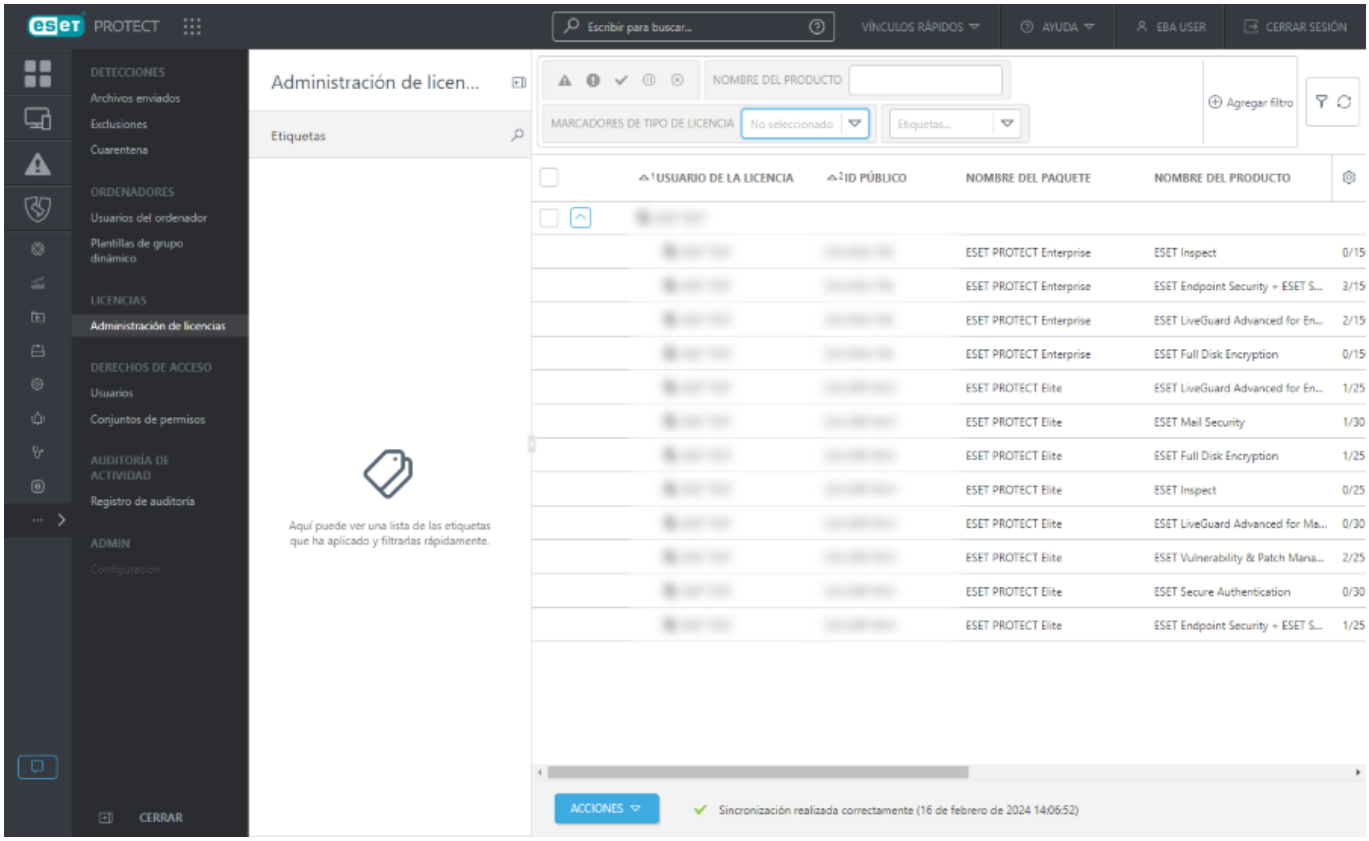
Permisos de administración de licencias

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, 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).
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 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.
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 permite administrar licencias de suscripción. Puede comprobar la validez de su suscripción en **Administración de licencias** en la columna **Validez** o en **Ordenadores** > Detalles.

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

No puede utilizar la licencia de ESET PROTECT para activar los productos de seguridad de ESET en equipos administrados. Para activar productos de seguridad de ESET individuales, utilice las licencias correspondientes a esos productos.

Puede distribuir licencias a los productos de ESET desde ESET PROTECT 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 o la licencia no estuviera administrada por ESET PROTECT.

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.

Licencias válidas para nube

Las licencias válidas para nube son licencias que se pueden usar con ESET PROTECT. Obtenga más información sobre los niveles de protección de ESET.

No se pueden usar los niveles de protección de ESET PROTECT local en ESET PROTECT en la nube.

Consulte en la tabla que aparece a continuación qué licencias pueden usarse para crear la instancia de ESET PROTECT y qué niveles se utilizan solo para activar funciones específicas del producto.

Nombre del nivel	Válida para crear la instancia de ESET PROTECT en ESET Business Account	Válida para crear la instancia de ESET PROTECT en ESET MSP Administrator
ESET PROTECT Essential	✔	
ESET PROTECT Entry (anteriormente: ESET Endpoint Protection Advanced Cloud)	✔	✔
ESET Secure Business Cloud	✔	
ESET PROTECT Advanced (anteriormente: ESET Remote Workforce Offer)	✔	✔
ESET PROTECT Complete	✔	✔
ESET PROTECT Enterprise	✔	✔
ESET PROTECT Mail Plus	✔	✔
ESET PROTECT Elite	✔	✔
ESET PROTECT MDR	✔	
ESET Security for Microsoft SharePoint Server (Per Server)	✔	
ESET LiveGuard Advanced		
ESET LiveGuard Advanced for Endpoint Security + ESET Server Security (ESET File Security)		
ESET LiveGuard Advanced for Mail Security		
ESET Full Disk Encryption para ECA		

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.

Derechos de acceso

Los derechos de acceso le permiten administrar usuarios de ESET PROTECT Web Console y sus permisos.

El modelo de seguridad

Estos ajustes de derechos de acceso solo se aplican a los usuarios cuando se configura un **Permiso personalizado** en la administración de cuentas de ESET Business Account (EBA). Solo pueden agregarse **Permisos personalizados** en ESET PROTECT Web Console mediante una cuenta con permisos de **Superusuario** en el portal ESET Business Account.

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 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.

- Acciones y detalles del usuario
- Usuarios asignados
- Asignar un conjunto de permisos a un usuario

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.
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.
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 **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:

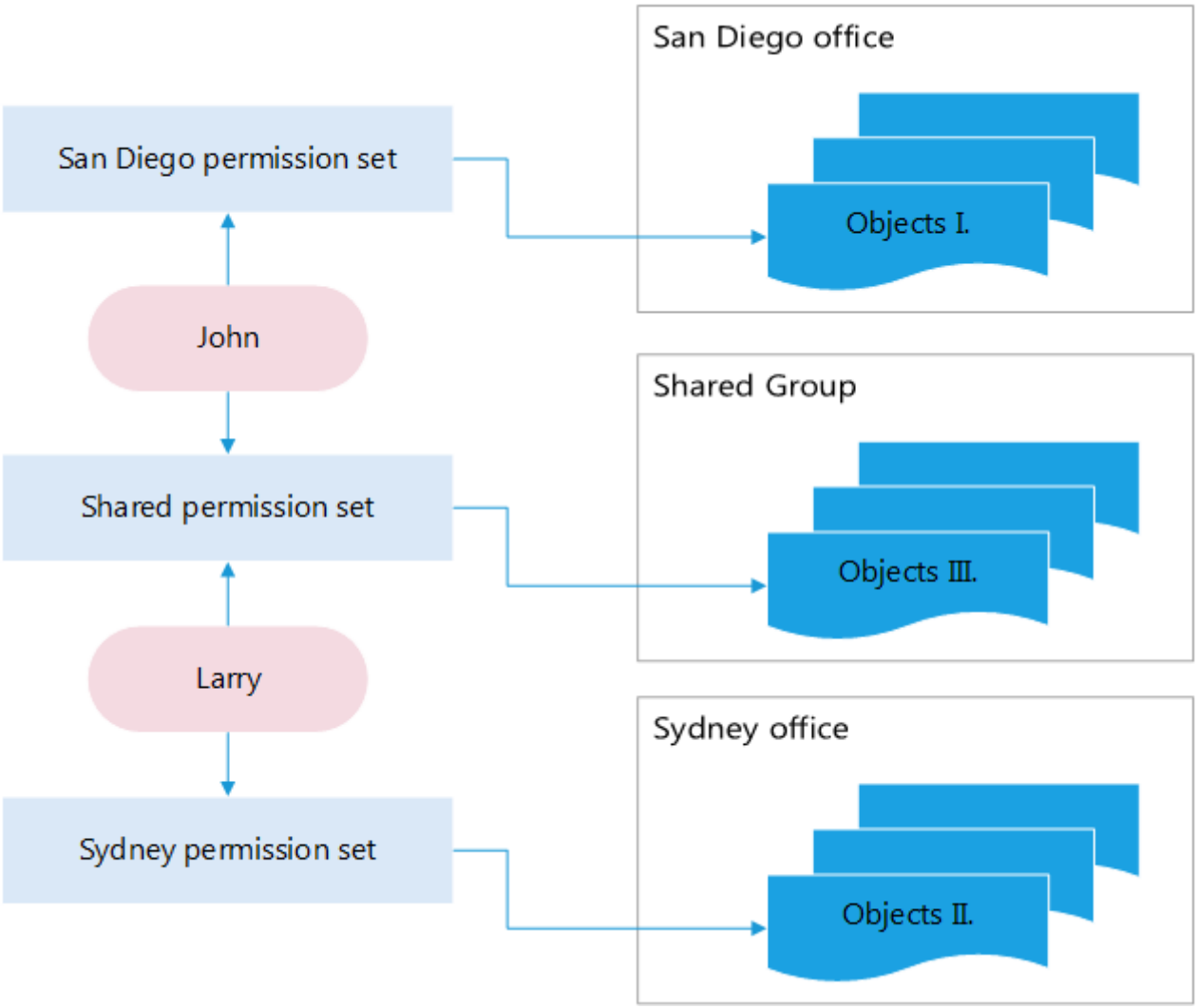
- Mover esos objetos a grupos compartidos

- 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.

Acciones y detalles del usuario

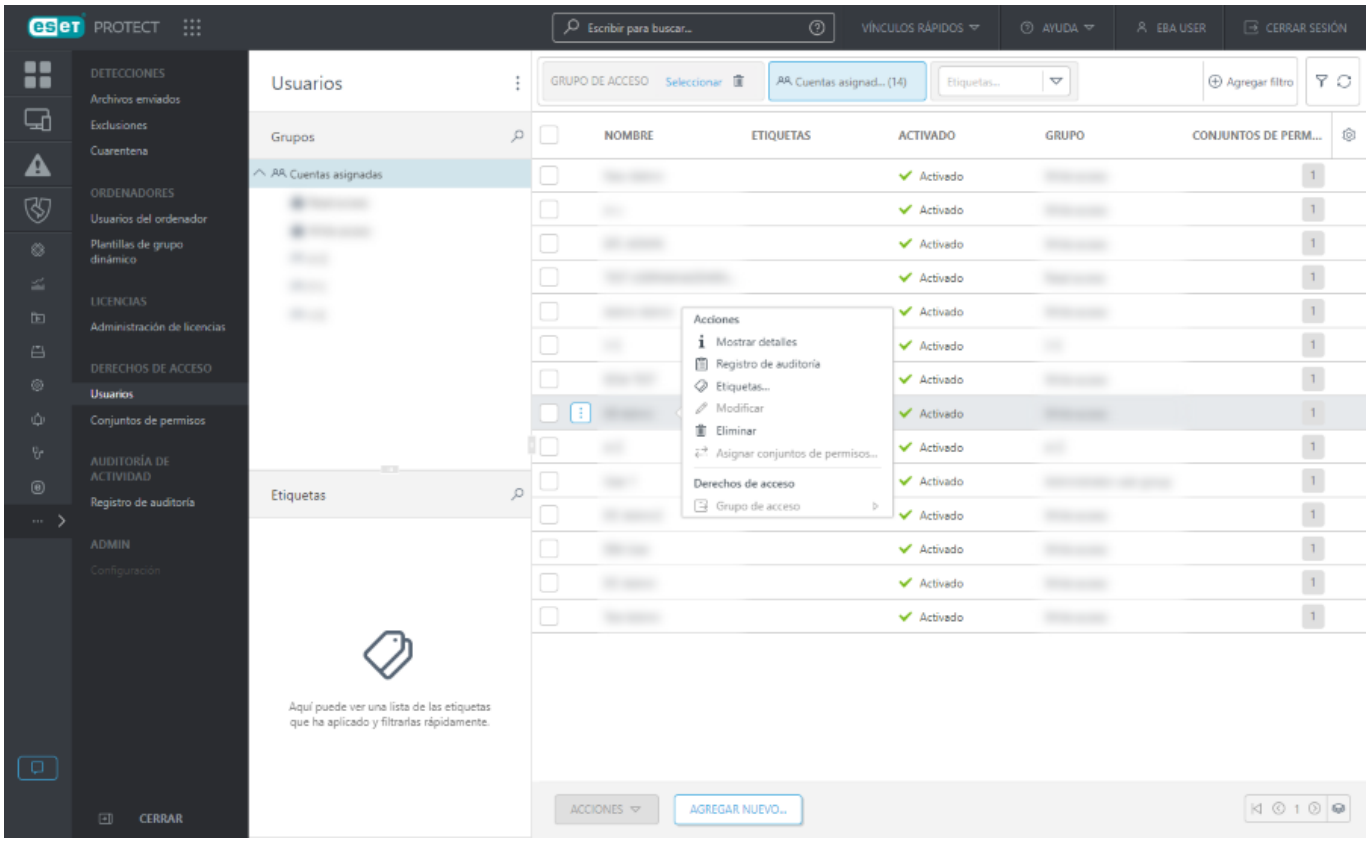
Para administrar un usuario, seleccione el usuario en cuestión y seleccione una de las acciones disponibles:

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.

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:

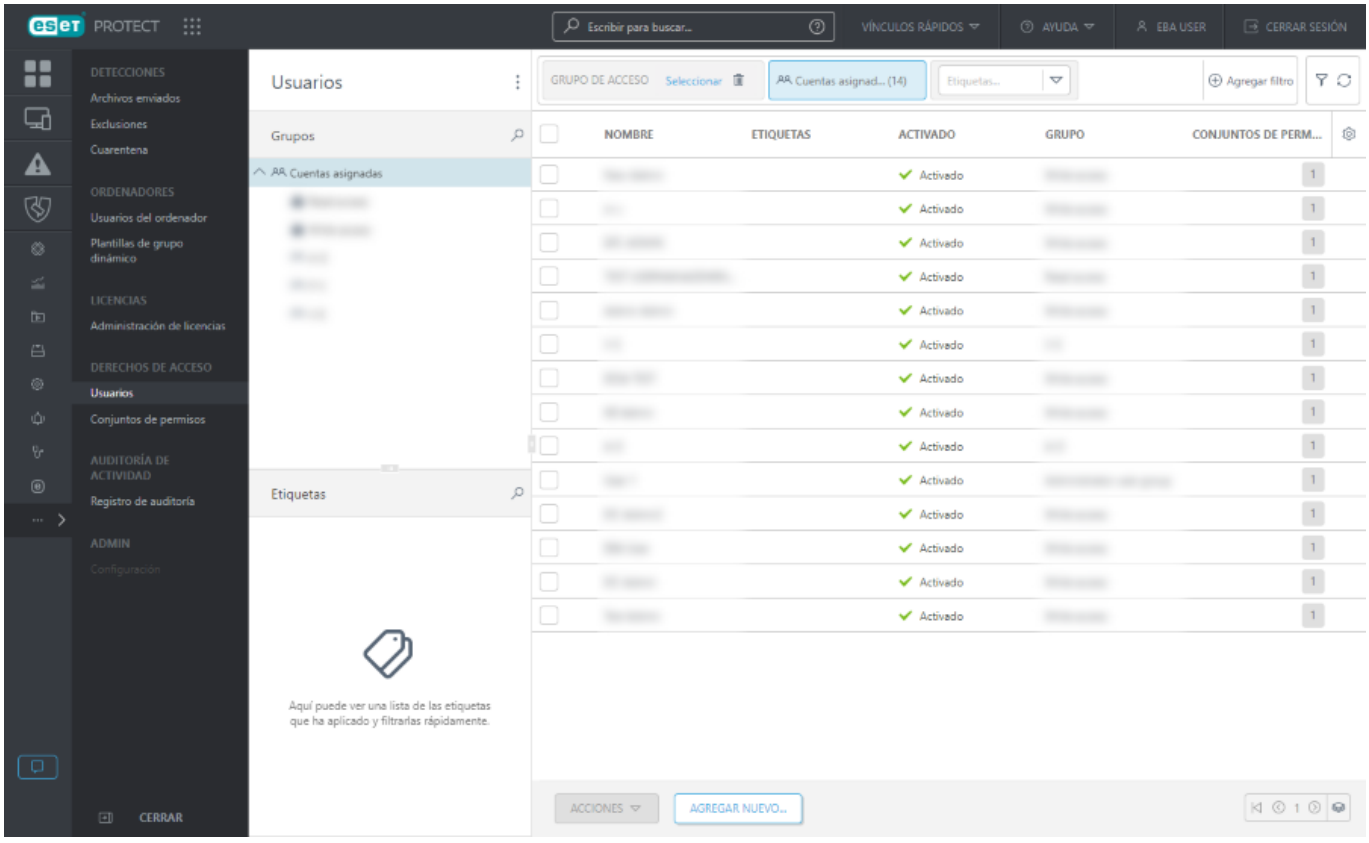
- **Visión general**: información básica sobre el usuario. Puede administrar el usuario con el botón **Acciones** situado en la parte inferior.
- **Conjuntos de permisos**: la lista de conjuntos de permisos asignados al usuario. Haga clic en un conjunto de permisos para administrarlo.

Asignar usuarios de ESET Business Account

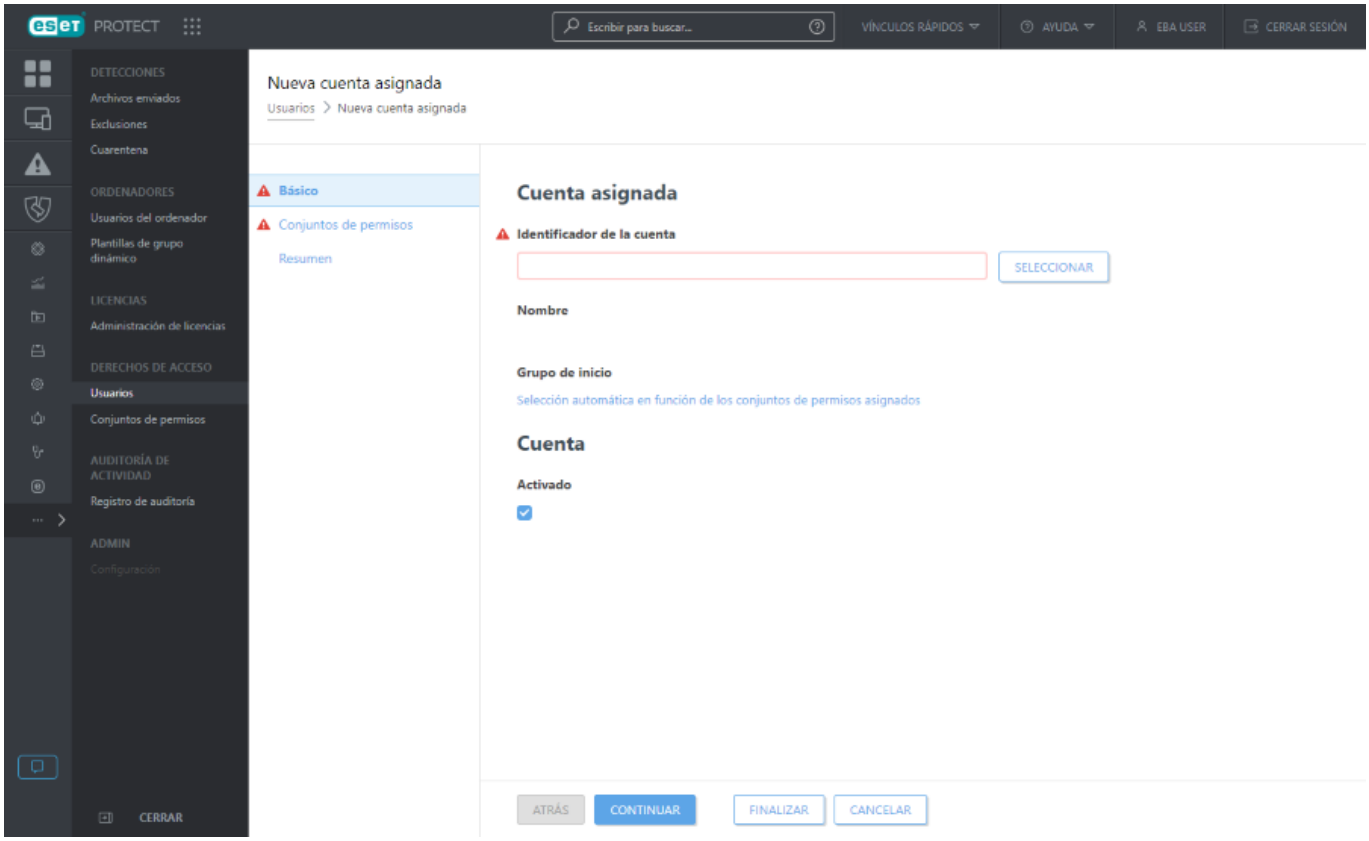
Siga los pasos indicados a continuación para asignar un usuario de ESET Business Account a ESET PROTECT:

1. Inicie sesión en ESET Business Account con la cuenta de usuario que utilizó al crear un usuario nuevo en ESET Business Account; no utilice aún la cuenta de usuario que acaba de crear.

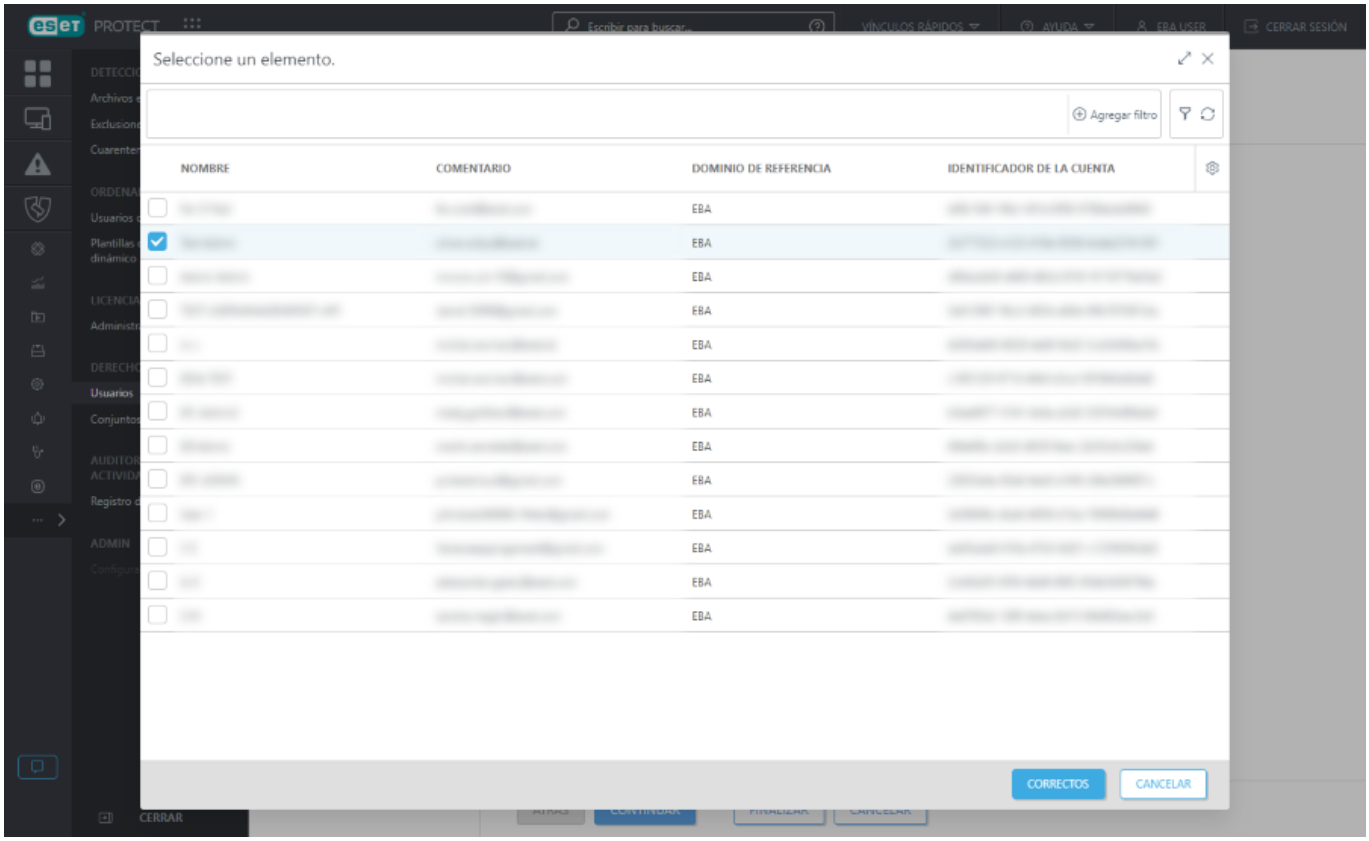
2. Abra ESET PROTECT Web Console. Haga clic en **Más** > **Usuarios** > seleccione **Cuentas asignadas** > haga clic en el botón **Agregar nuevo**.



3. Haga clic en **Seleccionar** en **Identificador de la cuenta**.



4. Seleccione el usuario que creó en ESET Business Account y haga clic en **Aceptar**.



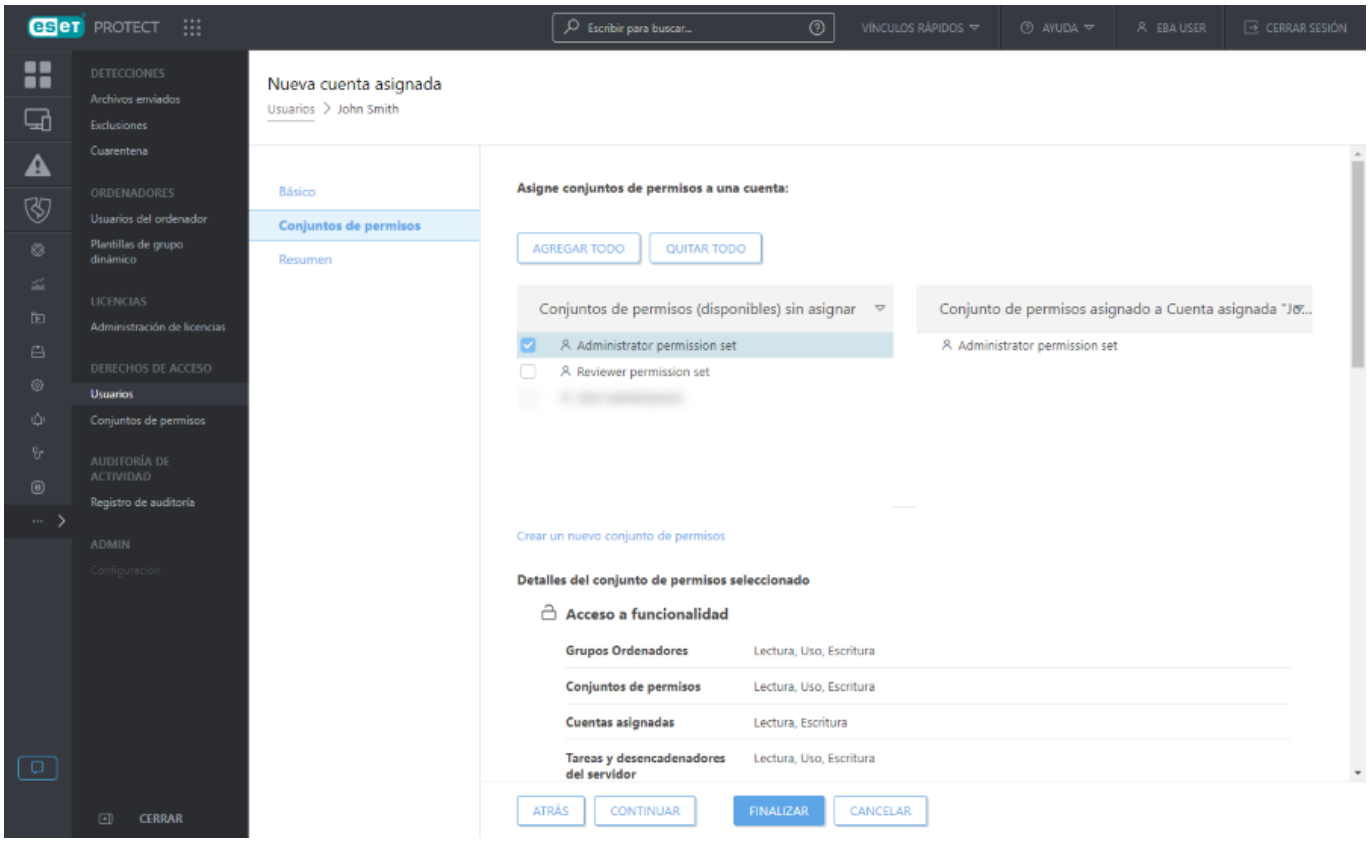
5. **Grupo de inicio** – El grupo de inicio se detecta automáticamente según el conjunto de permisos asignado del usuario activo en ese momento.

Situación de ejemplo:

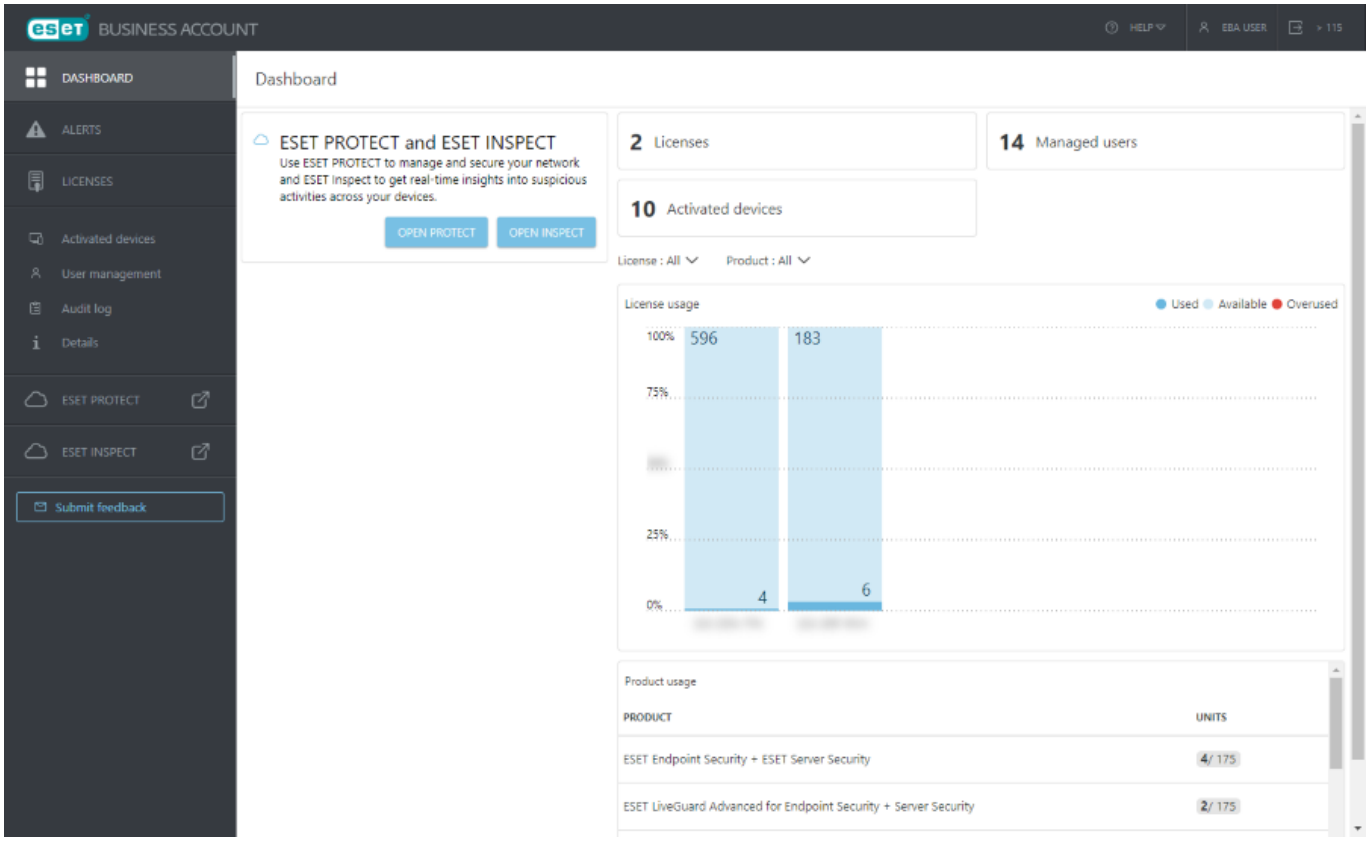
La cuenta de usuario activa actualmente tiene derechos de acceso de **Escritura** para la **tarea del cliente Instalación de software** y el **grupo de inicio** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación de software**, se seleccionará automáticamente "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.

6. En **Conjuntos de permisos** puede ver el nivel de permisos que ha asignado al usuario cuando lo creó en ESET Business Account. Si seleccionó **Acceso a ESET PROTECT personalizado**, debe asignar un conjunto de permisos al usuario (uno existente o puede crear un nuevo conjunto de permisos). Haga clic en **Finalizar**.



7. Los usuarios a los que se les concedió acceso a ESET PROTECT verán la opción de abrir ESET PROTECT en su ESET Business Account.

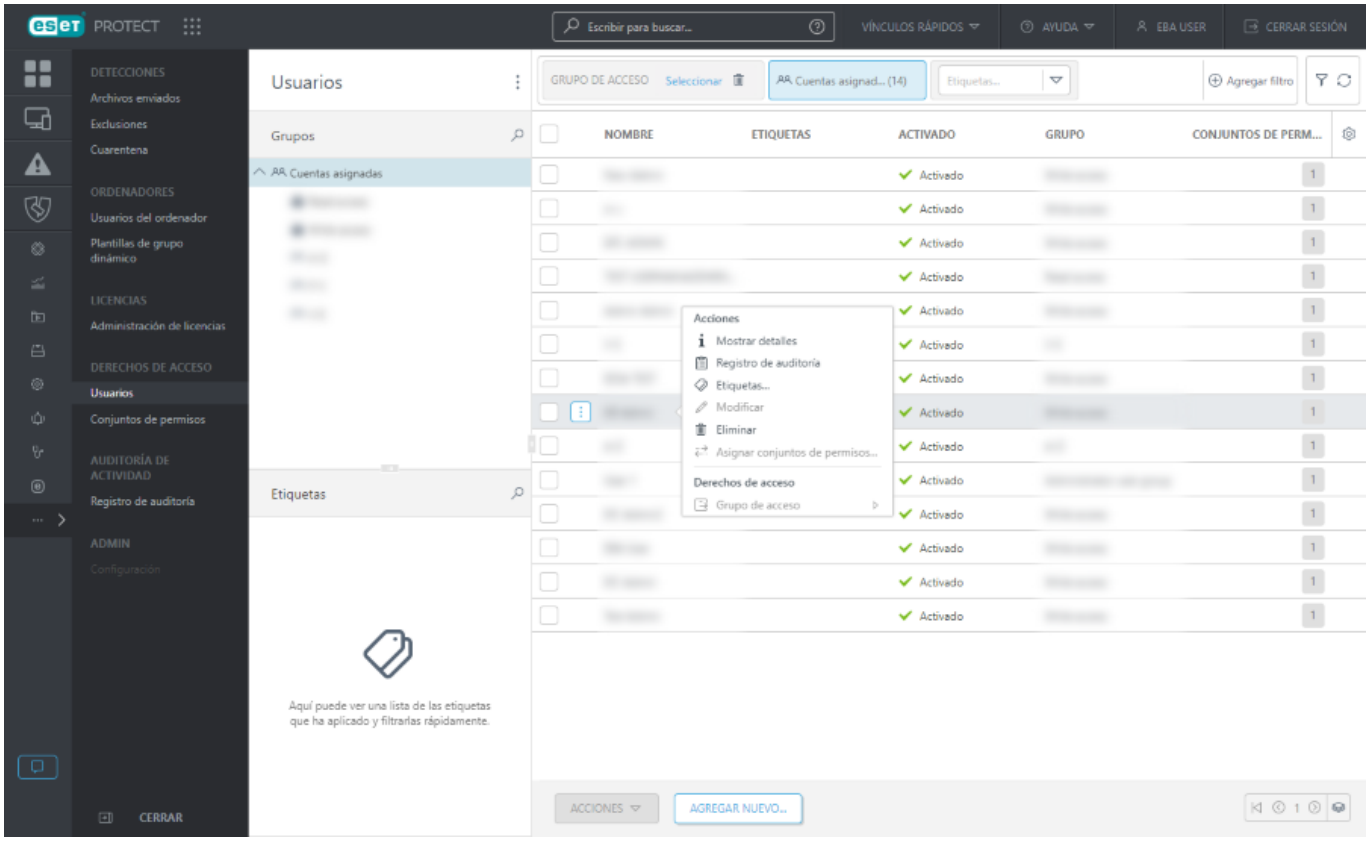


Asignar un conjunto de permisos a un usuario

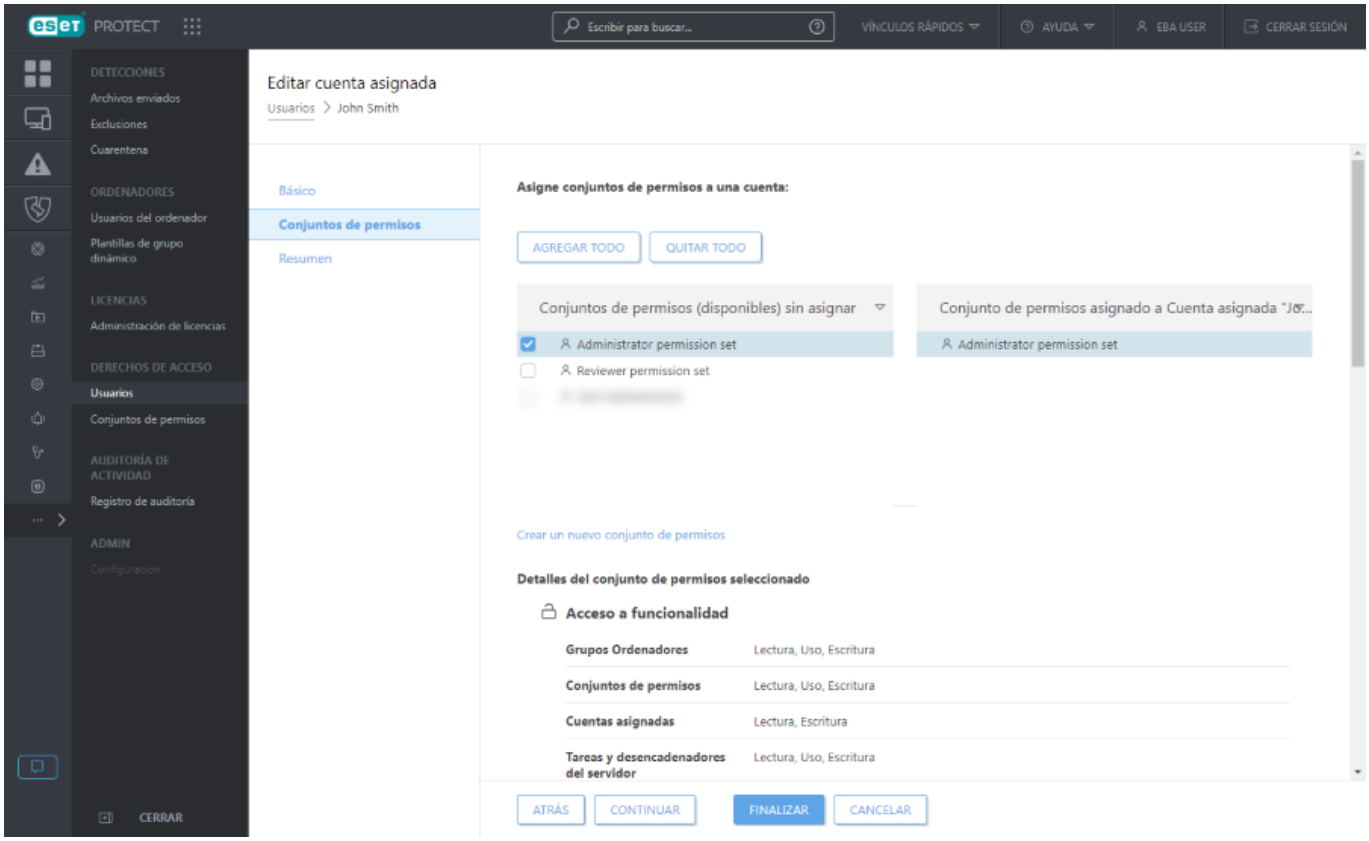
1. Hay dos formas de asignar un conjunto de permisos a un usuario:

   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.



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. 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).

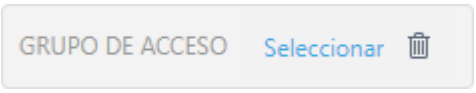
Un usuario puede tener un conjunto de permisos asignado aunque no pueda verlo. Un conjunto de permisos también es un objeto que se almacena automáticamente en el grupo principal del usuario que lo creó. Cuando se crea una cuenta de usuario, el usuario se almacena como objeto en el grupo principal del 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

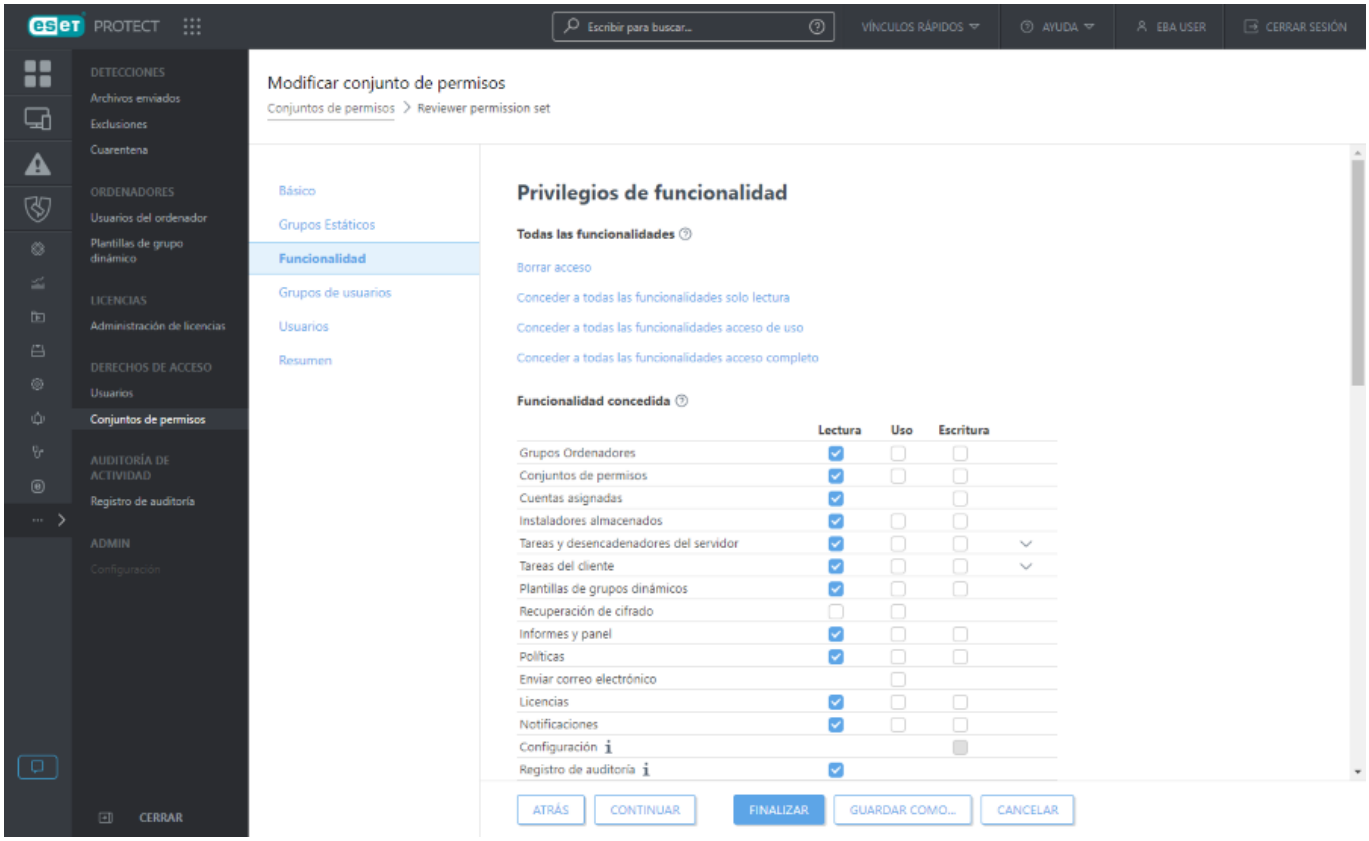
El acceso definitivo que un usuario tiene para un objeto es el resultado de la combinación de todos los conjuntos de permisos que el usuario tiene asignados. Por ejemplo, un usuario cuenta con dos conjuntos de permisos: uno para el grupo doméstico con todos los permisos, y otro para un grupo con ordenadores 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:
• 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** y **Cuentas asignadas**.
• 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, 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.

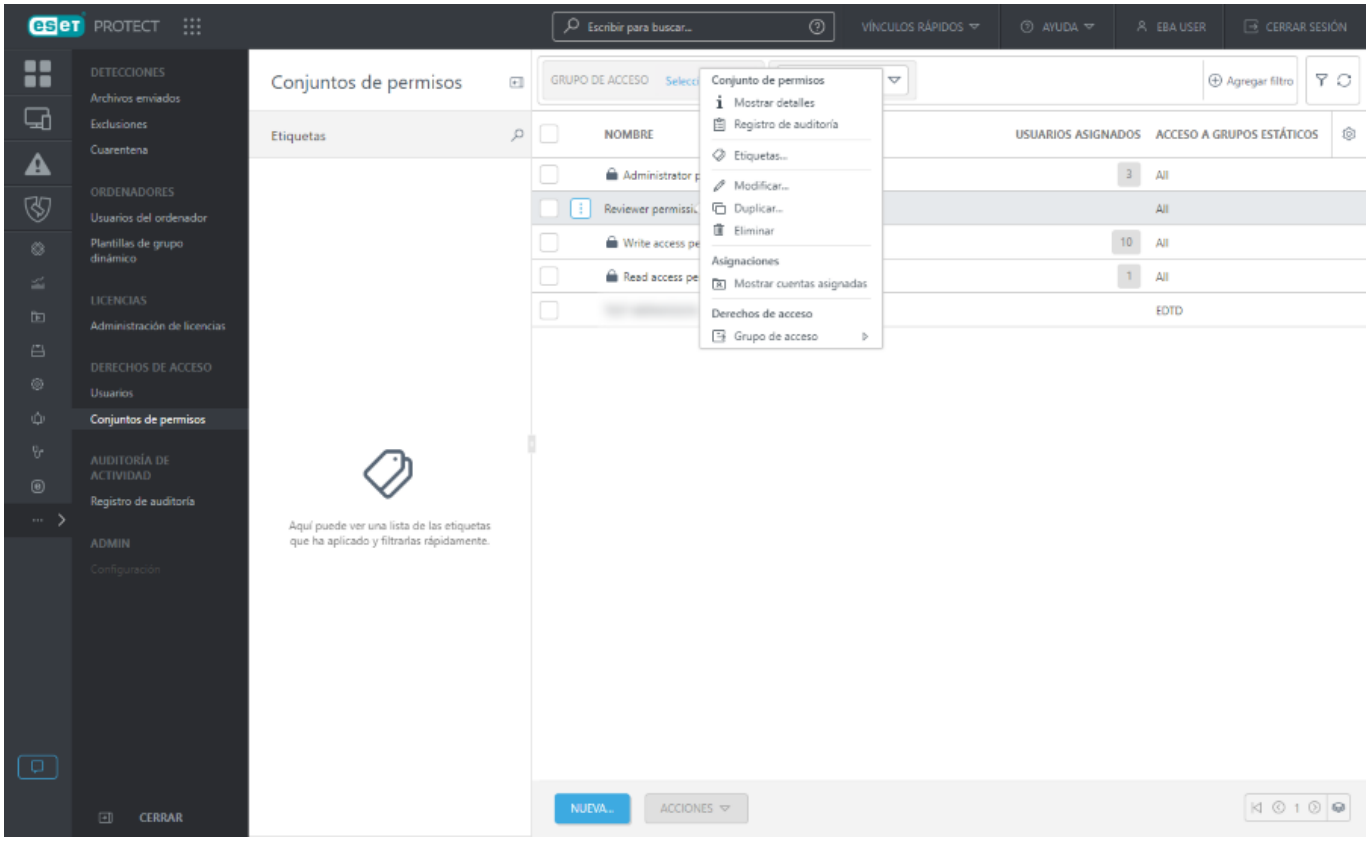
Diferencia entre Uso y Escritura

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 cuentas asignadas**: muestra la lista de cuentas asignadas.

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.

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, 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**
- **Token de acceso del análisis de AD**
- **Informes completos**
- **ESET MDR informes**

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.

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 las **Cuentas asignadas**.

Cuentas asignadas

Lectura: ver las cuentas asignadas.

Escritura: permite otorgar y revocar conjuntos de permisos.

Instaladores almacenados

Lectura: ver los instaladores almacenados.

Uso: exportar los instaladores almacenados.

Escritura: crear, modificar y quitar los instaladores almacenados.

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).

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.

Configuración

Escritura: modificar la ESET PROTECT configuración.

Registro de auditoría

Lectura: ver el Registro de auditoría y leer el informe del Registro de auditoría.

Token de acceso del análisis de AD

Lectura

Escritura: es necesario para la sincronización con AD.

Informes completos

Usar: genere la plantilla de informe de MDR.

ESET MDR informes

Usar: obligatorio para el archivo de informes de MDR.

Escribir: genera los informes de ESET 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**.

Registro de auditoría

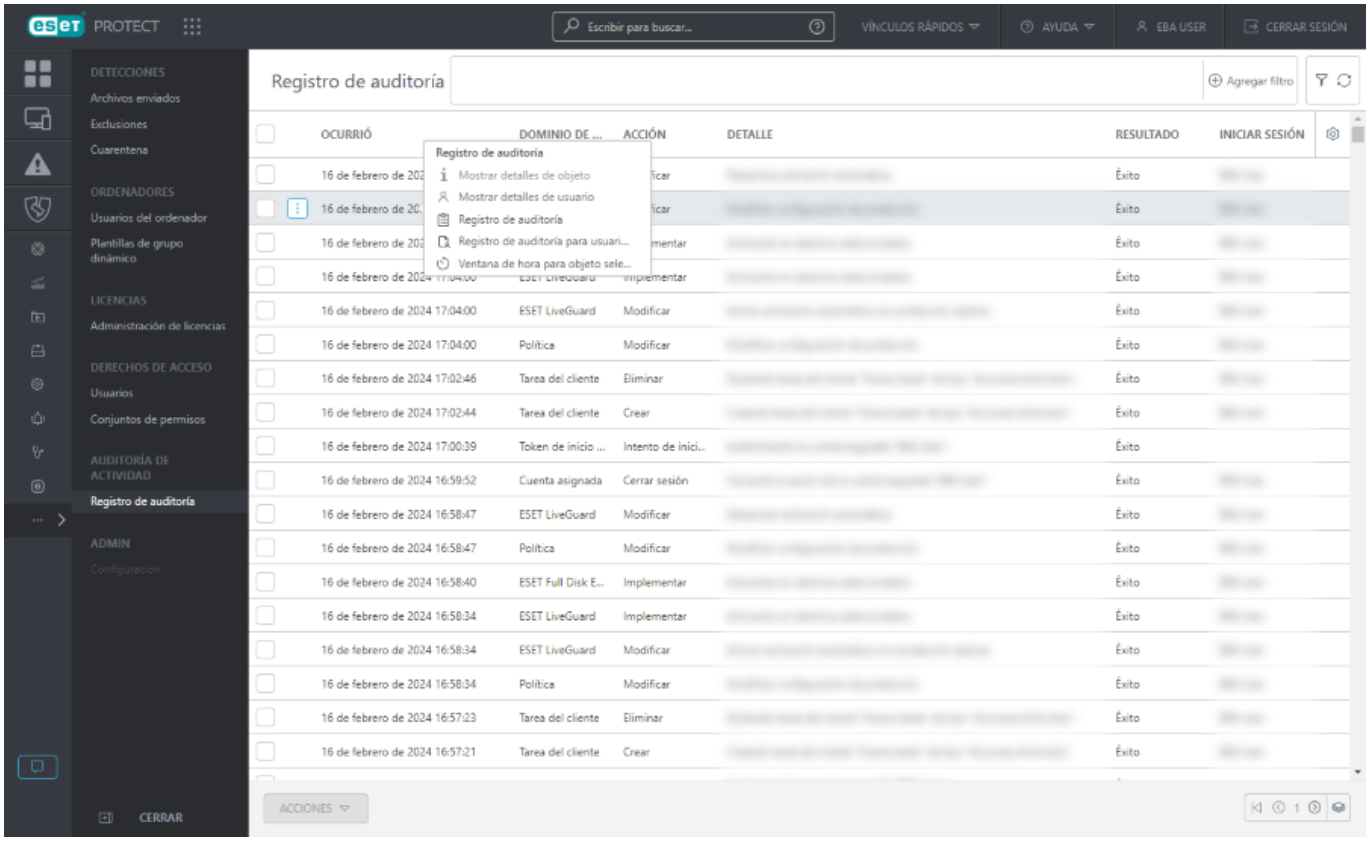
Cuando un usuario realiza una acción en ESET PROTECT Web Console, se registra la acción. Los registros de auditoría se crean si un objeto de ESET PROTECT Web Console (por ejemplo, un ordenador, una política, una detección, etc.) se crea o modifica.

Registro de auditoría es una nueva pantalla disponible en ESET PROTECT. 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

La sección Configuración permite al administrador ajustar las propiedades del envío de información de syslog a su servidor de syslog y especificar la política de retención de datos para los registros de la consola en la nube.

La sección **Configuración** solo está disponible para un usuario con permisos suficientes (por ejemplo, para una cuenta de superusuario [ESET Business Account]/usuario raíz [ESET MSP Administrator]).

General

Syslog

Active ESET PROTECT para enviar notificaciones y mensajes de sucesos a su servidor de Syslog. También puede exportar registros desde el producto de ESET de un ordenador cliente y enviarlos al servidor de Syslog.

Retención de datos

Especifique el periodo de limpieza de tipos específicos de registros almacenados en la consola en la nube. Indique el número de días, semanas, meses o años que se almacenarán los registros en el servidor para cada categoría. 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 • 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.

Límites de almacenamiento:

Tipo de registro	Mínimo	Predeterminado	Máximo
Registros de detección	1 día	90 días	365 días
Registros de administración	1 día	30 días	30 días
Registros de auditoría	1 día	180 días	730 días
Registros de supervisión	1 día	30 días	30 días

Puede obtener más información sobre lo que ocurre con los datos almacenados después de que caduque la última licencia válida.

Protección de la sesión de Web Console

Bloquear solicitudes de direcciones IP distintas:

- **Activar**: si desea limitar el intervalo de direcciones IP que pueden acceder a Web Console.
- **Desactivar**:
  - **Desactivar permanentemente**: esto permitirá a los usuarios acceder a Web Console desde un intervalo de direcciones IP sin filtrar.
  - **Desactivar durante**: seleccione un periodo durante el que se desactivará la limitación de acceso de direcciones IP.

Grupos estáticos

Emparejar automáticamente los ordenadores encontrados: si esta opción está **activada**, se activa el emparejado automático de los ordenadores encontrados con ordenadores ya presentes en los grupos estáticos en función del nombre de host notificado por ESET Management Agent.

- Si el emparejamiento falla, el ordenador se colocará en el grupo Perdidos y encontrados.
- Si el agente no notifica de manera fiable el nombre de host, se recomienda desactivar el emparejado automático.

Administración de dispositivos móviles

Microsoft Entra ID Inscripción

Consulte Inscripción con Microsoft Entra ID (Android o iOS).

Sincronización con Apple Business Manager (ABM)

Consulte Sincronización con Apple Business Manager (ABM) (iOS).

Sincronización con Microsoft Intune

Consulte Sincronización con Microsoft Intune (Android).

VMware Workspace ONE Sincronización

Consulte Sincronización con VMware Workspace ONE (Android).

Migración de dispositivos móviles desde ESET PROTECT (local)

Consulte más detalles en la herramienta de migración de MDM.

Exportar registros a Syslog

ESET PROTECT 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.

1. Para activar el servidor de Syslog, haga clic en **Más** > **Configuración** > **Syslog** > **Activar servidor de Syslog**.

Todos los registros exportados están disponibles para los usuarios de Syslog sin limitaciones.

2. 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.

Para activar el servidor de Syslog:

1.Haga clic en **Más** > **Configuración** > **Syslog** y haga clic en el conmutador de alternancia situado junto a **Activar envío de syslog**.

2.Especifique los siguientes ajustes obligatorios:

a.**Formato de la carga**: JSON, LEEF o CEF.

b.**Formato del envolvente** del registro: **BSD** (especificación), **Syslog** (especificación).

c.**Nivel de registro mínimo**: **Información**, **Advertencia**, **Error** o **Crítico**.

d.**Tipo de registro de eventos**: seleccione el tipo de registros que desee incluir (**Antivirus**, **HIPS**, **Cortafuegos**, **Protección web**, **Registro de auditoría**, **Archivos bloqueados**, **Alertas de ESET Inspect**).

e.**IP de destino o FQDN del servidor de syslog compatible con TLS**: dirección IPv4 o nombre de cliente del destino de los mensajes de Syslog.

f.**Validar certificados raíz de CA de conexiones TLS**: haga clic en el conmutador de alternancia si desea activar la validación de certificados para la conexión entre su servidor de Syslog y ESET PROTECT. Cuando la validación esté activada, se mostrará un nuevo campo de texto en el que puede copiar y pegar la cadena de certificados requerida. El certificado del servidor debe cumplir los siguientes requisitos:

- La cadena de certificados completa en formato PEM se carga y guarda en la configuración de

exportación de Syslog (esto incluye la autoridad certificadora raíz, ya que no hay certificados de confianza integrados).

- El certificado de su servidor de Syslog proporciona una extensión de nombre alternativo del sujeto (DNS=/IP=), en la que al menos un registro corresponde a la configuración del nombre de host de IP/FQDN.

> Necesita la autoridad certificadora versión 3 (y posterior) con la extensión de certificado de restricciones básicas para pasar la validación.
> La validación de conexiones TLS solo se aplica a los certificados. La desactivación de la validación no afecta a los ajustes TLS de ESET PROTECT.

Tras realizar los cambios pertinentes, haga clic en **Aplicar configuración**. La configuración se aplica 10 minutos después.

> 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.

Restricciones y límites de seguridad de syslog

Debido a los requisitos de seguridad de la conexión del servidor de Syslog, los siguientes ajustes son fijos y no se pueden modificar:

- Protocolo de transporte: TLS
- Puerto TCP: 6514

Por el mismo motivo, hay requisitos adicionales en el servidor de Syslog receptor:

- Dirección IP: Dirección IPv4 enrutable globalmente
- Nombres IDN: Debe utilizar representación ASCII ("xn--").
- NOMBRE DE DOMINIO COMPLETO: Debe traducirse a una sola dirección IPv4 fija.

> Uso de FQDN
> Si su servidor de Syslog funciona en varios equipos o direcciones IP (CDN), no hay ninguna garantía respecto a cuándo y con qué frecuencia se volverá a resolver el FQDN. No obstante, se garantiza que la primera resolución del FQDN se completará en una ventana de 10 minutos tras el inicio del servidor, siempre que la exportación de Syslog esté activada y correctamente configurada.

Ajustes de seguridad adicionales

El administrador debe configurar el cortafuegos de su servidor de Syslog para permitir los sucesos de exportación del Syslog entrantes solo de los siguientes rangos de IP:

- Direcciones IP salientes de ESET PROTECT en la región de Europa: 51.136.106.164/30
- Direcciones IP salientes de ESET PROTECT en la región de EE. UU.: 40.81.8.148/30

- Direcciones IP salientes de ESET PROTECT en la región de Japón: 20.78.10.184/30

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.
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 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
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 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.

event	cadena	opcional	Nombre del evento
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.
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 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
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 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 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
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
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 reenvía los archivos bloqueados por ESET Inspect 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 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	ProtectCloud	
Device Version	10.0.5.1	ESET PROTECT 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.
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	

Nombre de la extensión	Ejemplo	Descripción
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	
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	

Nombre de la extensión	Ejemplo	Descripción
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=0000000000000000000000000000000000000000 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)

Nombre de la extensión	Ejemplo	Descripción
cnt	3	El número de los mismos mensajes generados por el equipo entre dos replicaciones consecutivas entre ESET PROTECT 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 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
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 Web Console
cs4Label	EI Console Link	

Nombre de la extensión	Ejemplo	Descripción
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

Nombre de la extensión	Ejemplo	Descripción
cs2	Blocked by Administrator	Causa
cs2Label	Cause	

Ejemplo de registro de CEF de evento de archivos bloqueados:

```
CEF:0|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

ESET PROTECT para proveedores de servicios administrados (MSP)

¿Qué es un MSP?

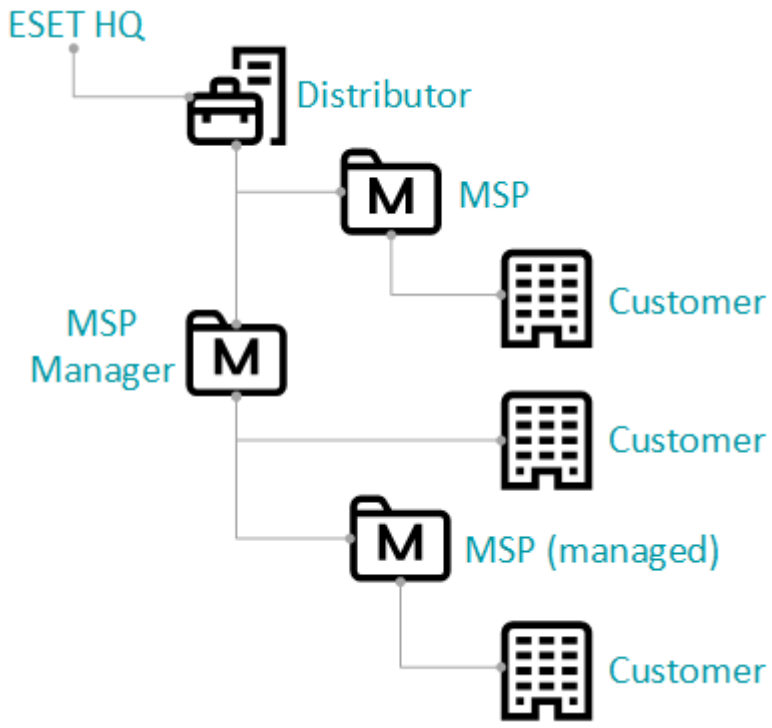
La abreviatura MSP hace referencia a "Proveedor de servicios administrados". Los usuarios MSP ofrecen servicios de TI a sus clientes, por ejemplo, la administración de sus productos de seguridad (como ESET Endpoint Antivirus).

- Los usuarios MSP tienen distintos requisitos y distintas formas de usar ESET PROTECT 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 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.

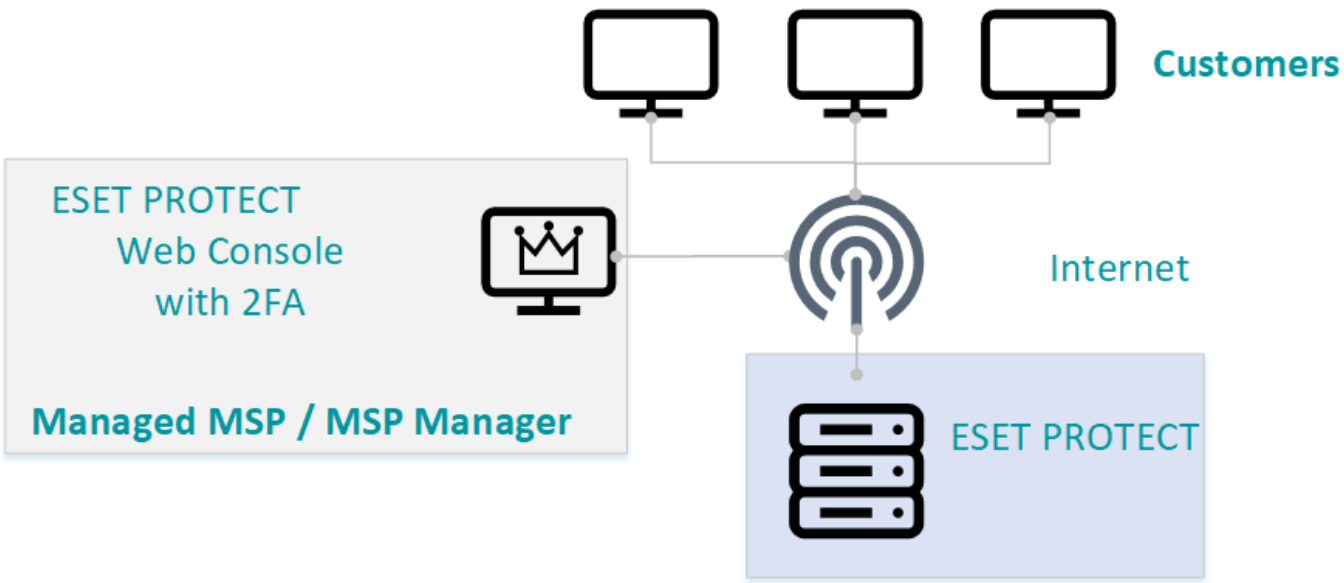
o : se ha eliminado el cliente.

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.

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. Las instancias de ESET Management Agent instaladas en los ordenadores de los clientes deben tener conectividad con ESET PROTECT a través del Internet público. Asegúrese de abrir ciertos puertos para que ESET PROTECT esté visible.

La configuración estándar de MSP tiene la siguiente estructura:



ESET PROTECT implementada desde una cuenta mixta

Una cuenta mixta utiliza las mismas credenciales para acceder a ESET Business Account y ESET MSP Administrator. En ese caso, puede crear el ESET PROTECT desde cada una de ellas. Después de crear la instancia, puede acceder a la misma instancia desde ambos servicios (EMA 2 y EBA). El derecho de eliminación de la instancia de ESET

PROTECT está reservado para el servicio que creó la instancia.

Funciones de ESET PROTECT para usuarios MSP

ESET PROTECT ofrece un conjunto de funciones centradas en los usuarios MSP. Las funciones para MSP están disponibles para los usuarios que implementaron la instancia de ESET PROTECT desde:

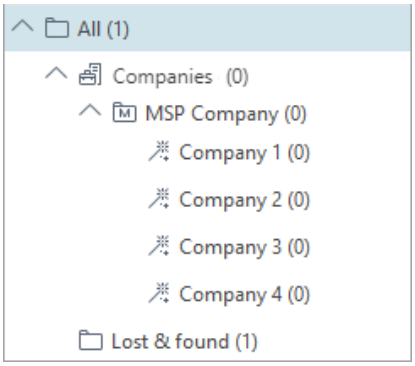
- Cuenta de ESET MSP Administrator (EMA 2)
- ESET Business Account (EBA) mientras tiene una cuenta de EMA 2 con las mismas credenciales

Asistente de instalación de clientes

La función MSP principal en ESET PROTECT . es la configuración de clientes MSP. Esta función le ayuda a crear un instalador personalizado de ESET Management Agent para su cliente.

Árbol MSP

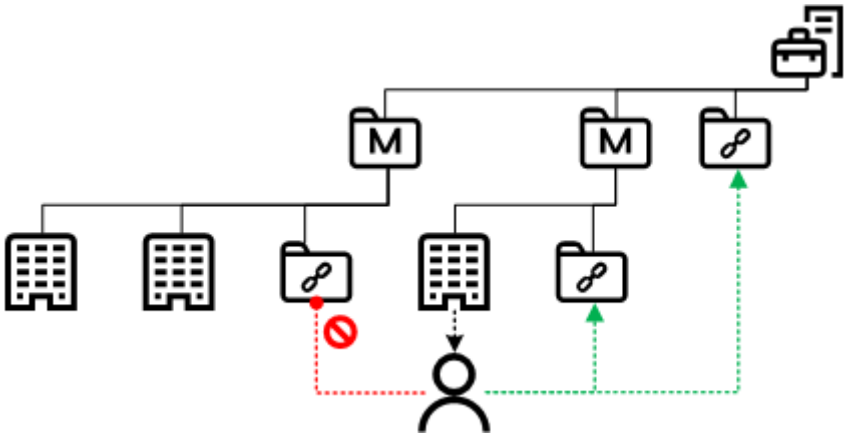
ESET PROTECT se sincroniza con el Portal de ESET MSP (EMA 2) y crea el árbol MSP. El árbol MSP es una estructura del menú Ordenadores que representa la estructura de las empresas de su cuenta de EMA 2. Los elementos de los árboles MSP usan iconos diferentes a los iconos estándar de los dispositivos y grupos de ESET PROTECT. No puede modificar la estructura del árbol MSP en Web Console.



Grupo Objetos compartidos

Tras la sincronización de la cuenta MSP, ESET PROTECT 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.

MSP en Resumen del estado

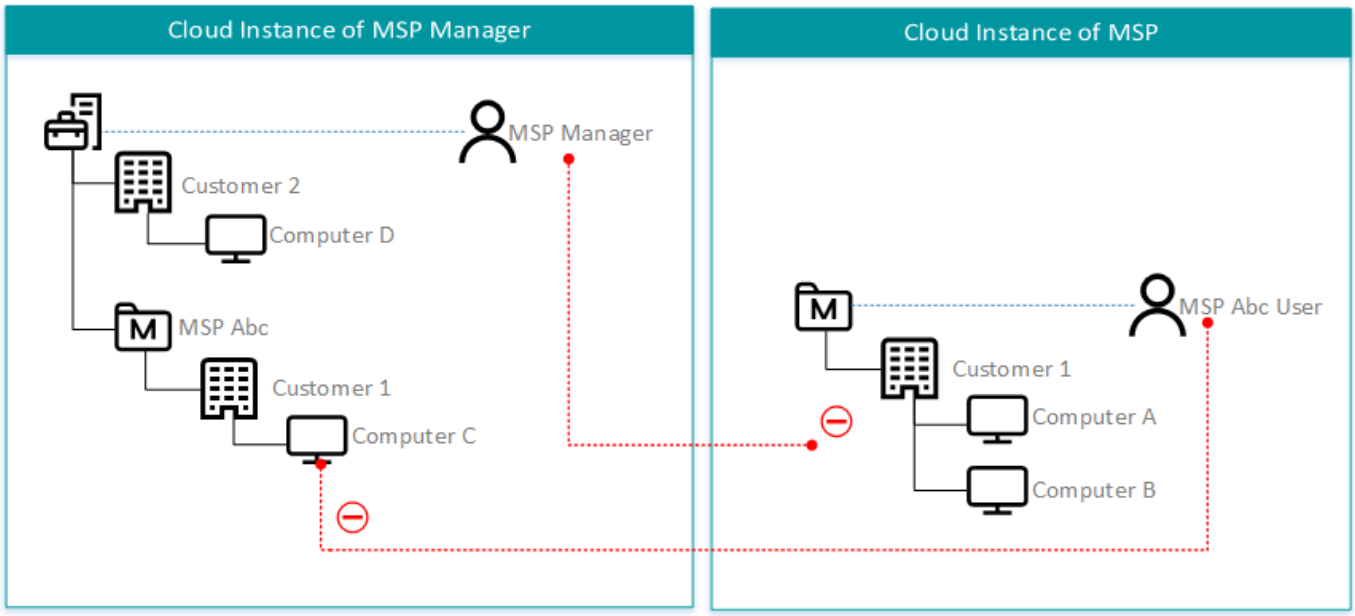
Podrá acceder a la nueva ventana dinámica de MSP en Resumen del estado. La ventana dinámica de MSP muestra información básica sobre su cuenta.

Tiene varias instancias de ESET PROTECT en la estructura MSP

Si usa la instancia de nube implementada desde una cuenta MSP, se separa de otras instancias de MSP. La instancia de su responsable de MSP no está conectada. Comparten la misma estructura de empresa (árbol MSP), pero no comparten ordenadores ni otros objetos, como las tareas o las políticas. Las licencias son la única excepción. Se comparten de forma jerárquica, igual que ESET MSP Administrator. El responsable de MSP puede acceder a las licencias desde Web Console y asignarlas a las máquinas.

Consulte el siguiente ejemplo:

El usuario de MSP no tiene acceso a los ordenadores de la instancia del responsable de MSP, incluso si estos ordenadores se encuentran en el grupo estático de los clientes de MSP. Esto se debe a que las instancias en la nube están separadas.



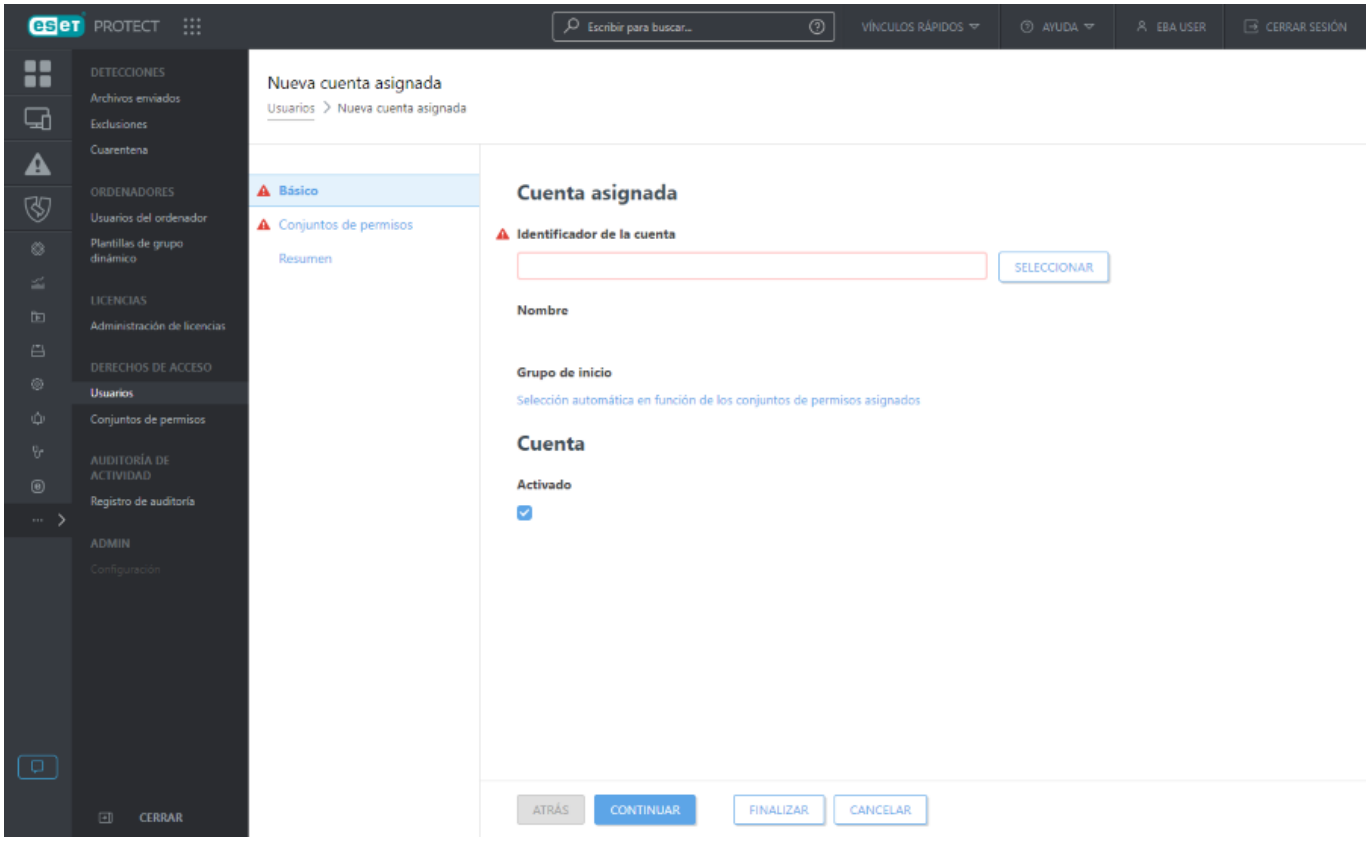
Crear un nuevoESET PROTECT usuario en ESET MSP Administrator

Para crear un nuevo usuario para ESET PROTECT Web Console, este usuario debe crearse antes en ESET MSP Administrator (EMA 2). Consulte la ayuda en línea de EMA 2 si desea una guía paso a paso sobre cómo agregar un usuario. Puede agregar el nuevo usuario durante la configuración de clientes MSP o siguiendo los pasos que se indican a continuación.

- Vea cómo funcionan los permisos de usuario en EMA 2 y ESET PROTECT en la ayuda en línea de EMA 2.
- Vea la guía paso a paso sobre cómo crear la instancia de ESET PROTECT.

1. Abra Web Console.

2. Vaya a **Usuarios**.

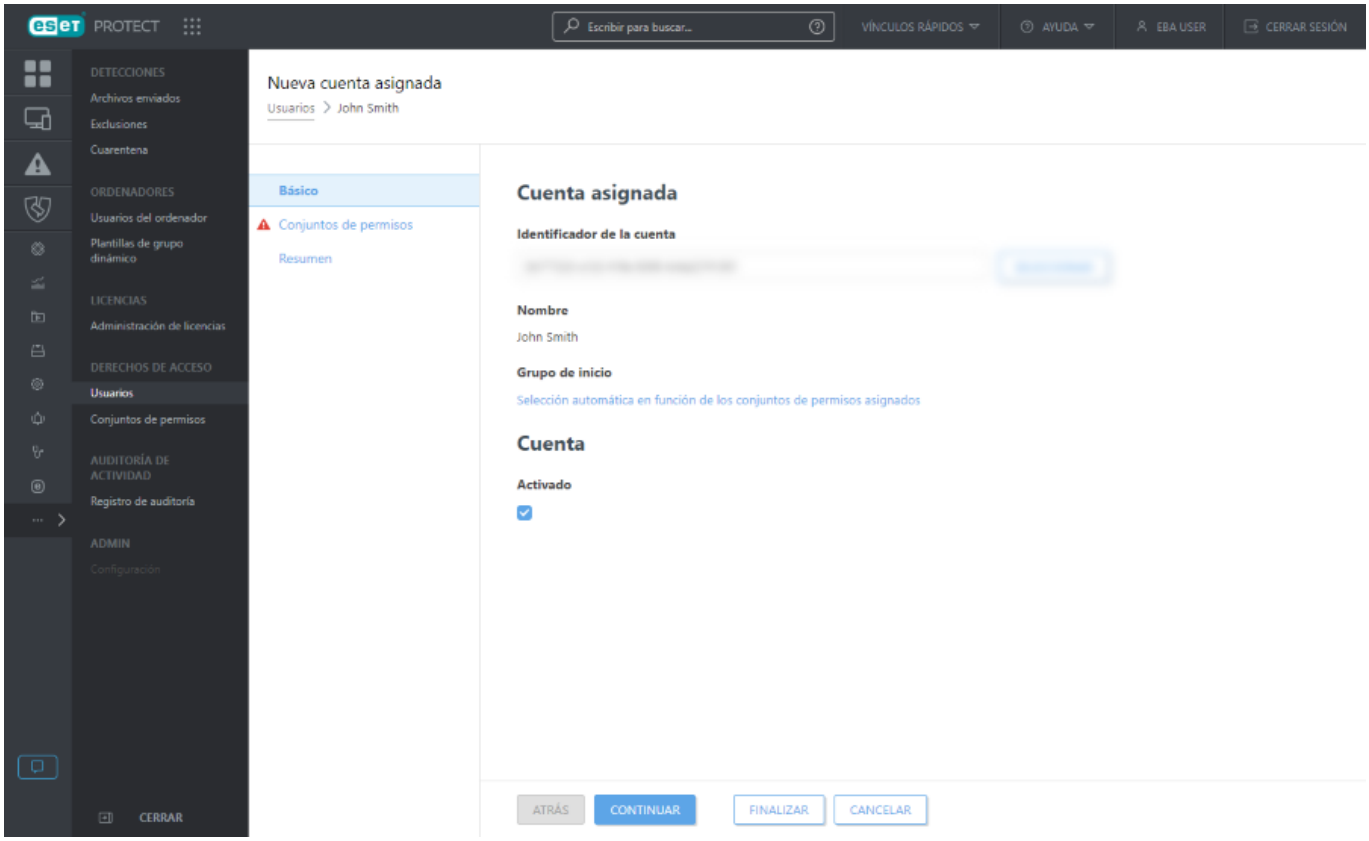


3. Haga clic en **Seleccionar** junto al campo **Identificador de la cuenta** y seleccione el usuario que desee activar en ESET PROTECT.

4. Puede agregar etiquetas, nuevas o existentes, al usuario.

5. Haga clic en **Seleccionar** junto al campo **Grupo de inicio**. El grupo de inicio es el grupo estático en el que se almacenan de forma predeterminada los objetos creados por el usuario.

6. Haga clic en **Conjuntos de permisos**.



7. Seleccione un conjunto de permisos para el nuevo usuario. Los conjuntos de permisos determinan los derechos de acceso del usuario. Cada conjunto de permisos ofrece a los usuarios derechos sobre determinados grupos estáticos. Los grupos se definen en cada conjunto de permisos. Un usuario puede asignarse a uno o varios conjuntos. Puede seleccionar uno de los conjuntos de permisos ofrecidos o crear uno nuevo.

> **Conjunto de permisos para el grupo de inicio**
> Agregue conjuntos de permisos al grupo de inicio que ha seleccionado para el usuario. Sin los derechos de acceso para el grupo de inicio, el usuario no puede acceder a los objetos del grupo de inicio ni crear objetos en dicho grupo.

8. Haga clic en **Finalizar** para guardar los cambios.

El nuevo usuario ya puede iniciar sesión en ESET PROTECT Web Console utilizando sus credenciales de EMA 2.

Proceso de implementación para MSP

1. Complete la configuración de clientes MSP. Cuando se le solicite, seleccione el instalador **Solo agente**.
2. Distribuya e instale el instalador de ESET Management de forma local o remota.
3. 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 agente (*.exe* para Windows y *.sh* para Linux) incluye toda la información necesaria para que un equipo cliente descargue e instale el agente ESET Management. Asegúrese de que el equipo Linux 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.

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 agente (*.exe* para Windows y *.sh* para Linux) incluye toda la información necesaria para que un equipo cliente descargue e instale el agente ESET Management. Asegúrese de que el equipo Linux 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 instalador.

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

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

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. Los usuarios que se crean con la configuración de clientes MSP solo pueden ver y usar sus licencias.

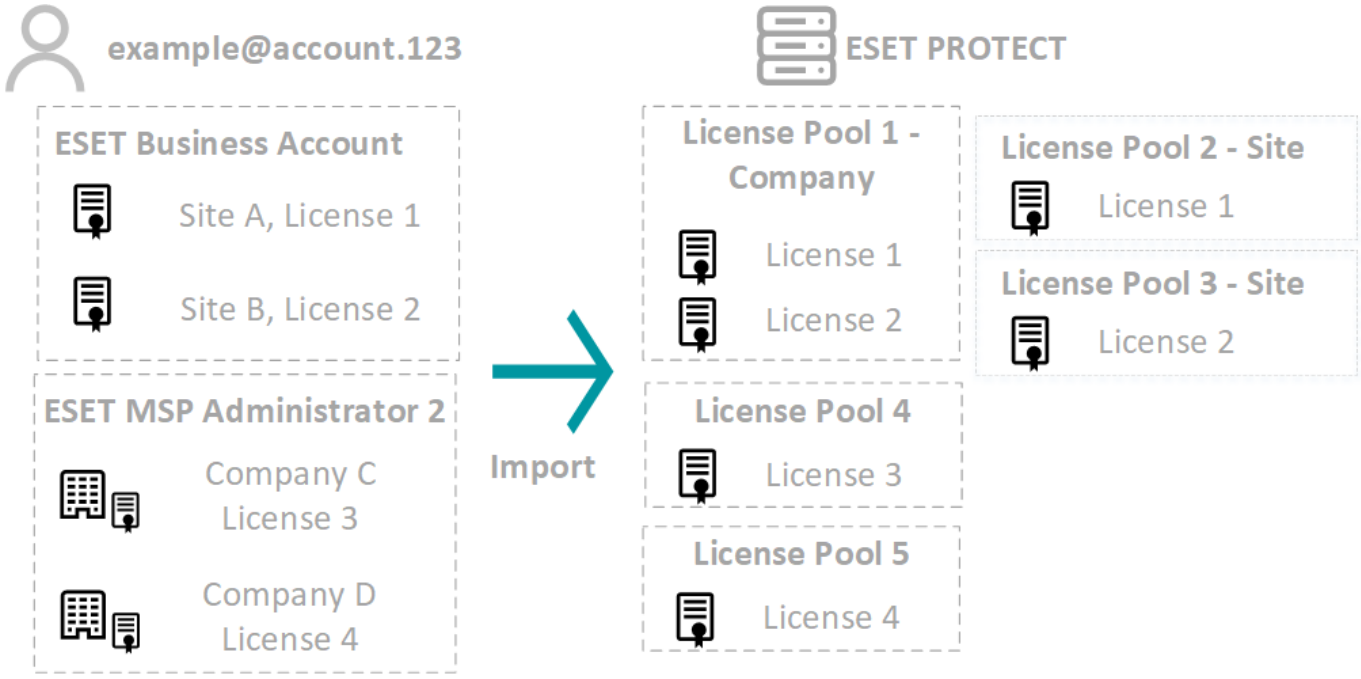
- Si hay una empresa en su estructura MSP que no tenga licencias cuando llegue el momento de la sincronización, esa empresa se sincronizará únicamente en el árbol MSP del ordenador, y no en el árbol MSP de la Administración de licencias.

- Si agrega una nueva empresa en ESET MSP Administrator 2, ESET PROTECT 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.

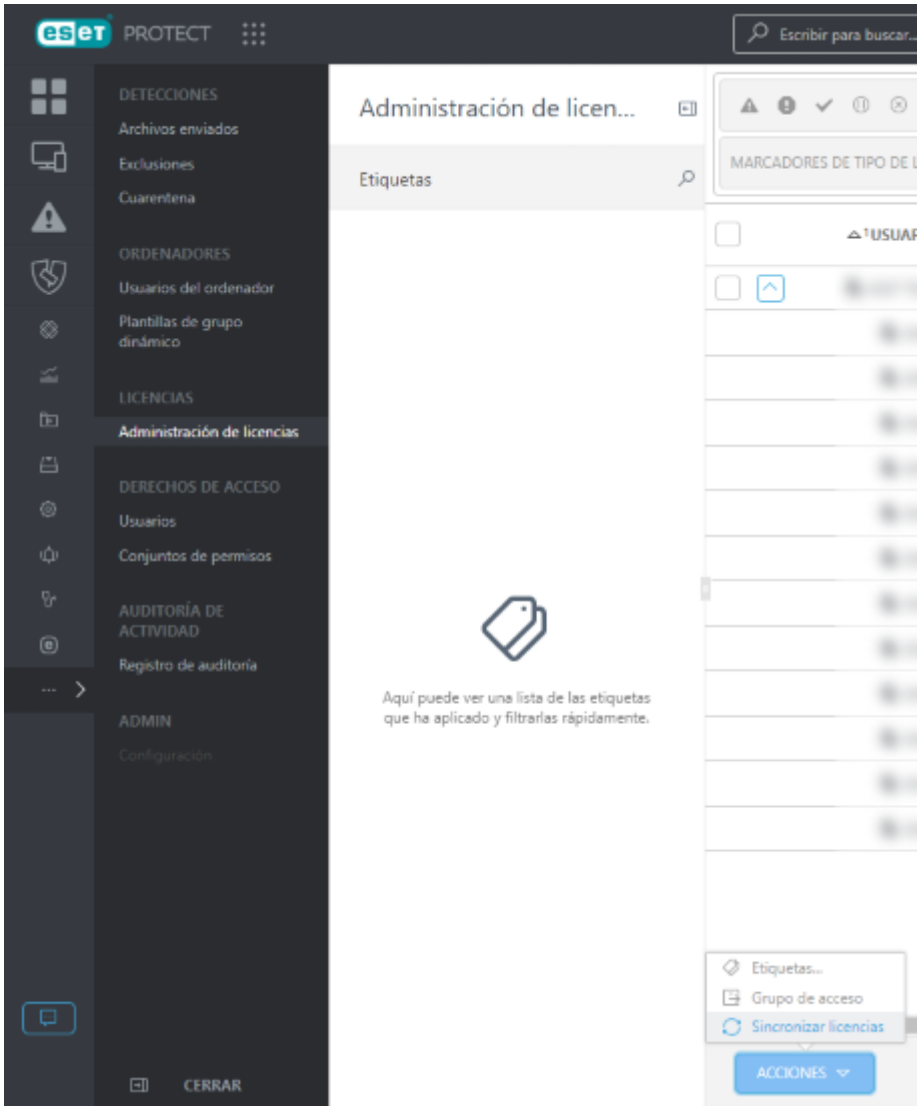
- Puede encontrar nombres de empresas y sitios en la columna **Usuario de la licencia** de Administración de licencias. Puede utilizar los datos del **Usuario de la licencia** al crear un informe.

- Si tiene licencias en ESET Business Account y ESET MSP Administrator 2 con las mismas credenciales, ESET PROTECT 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.



Sincronización a petición

ESET PROTECT 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**.



Iniciar configuración de cliente MSP

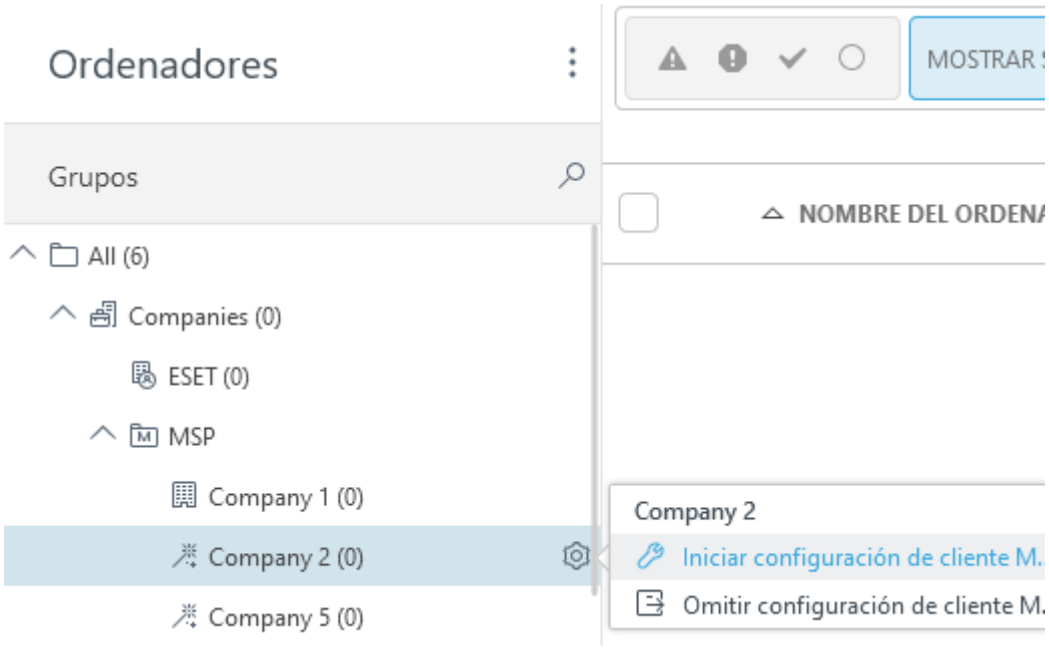
Después de crear la instancia de ESET PROTECT con una cuenta MSP, el árbol MSP se sincroniza y puede empezar a configurar empresas. La configuración de clientes MSP crea:

- 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.

También puede omitir la configuración de clientes MSP, pero le recomendamos que la complete.

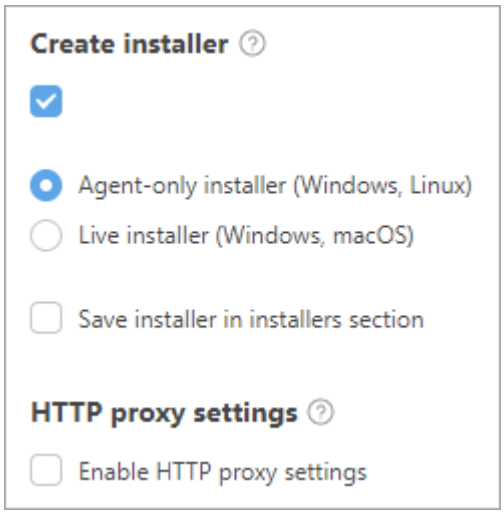
Solo puede configurar una empresa que tenga al menos 1 puesto de licencia válido.

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 para agente (Windows, Linux)**.

- **Instalador todo en uno (Windows, macOS)**: el instalador contiene ESET Management Agent y el producto de seguridad empresarial de ESET seleccionado.

Instalador todo en uno (Windows, macOS)

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**.

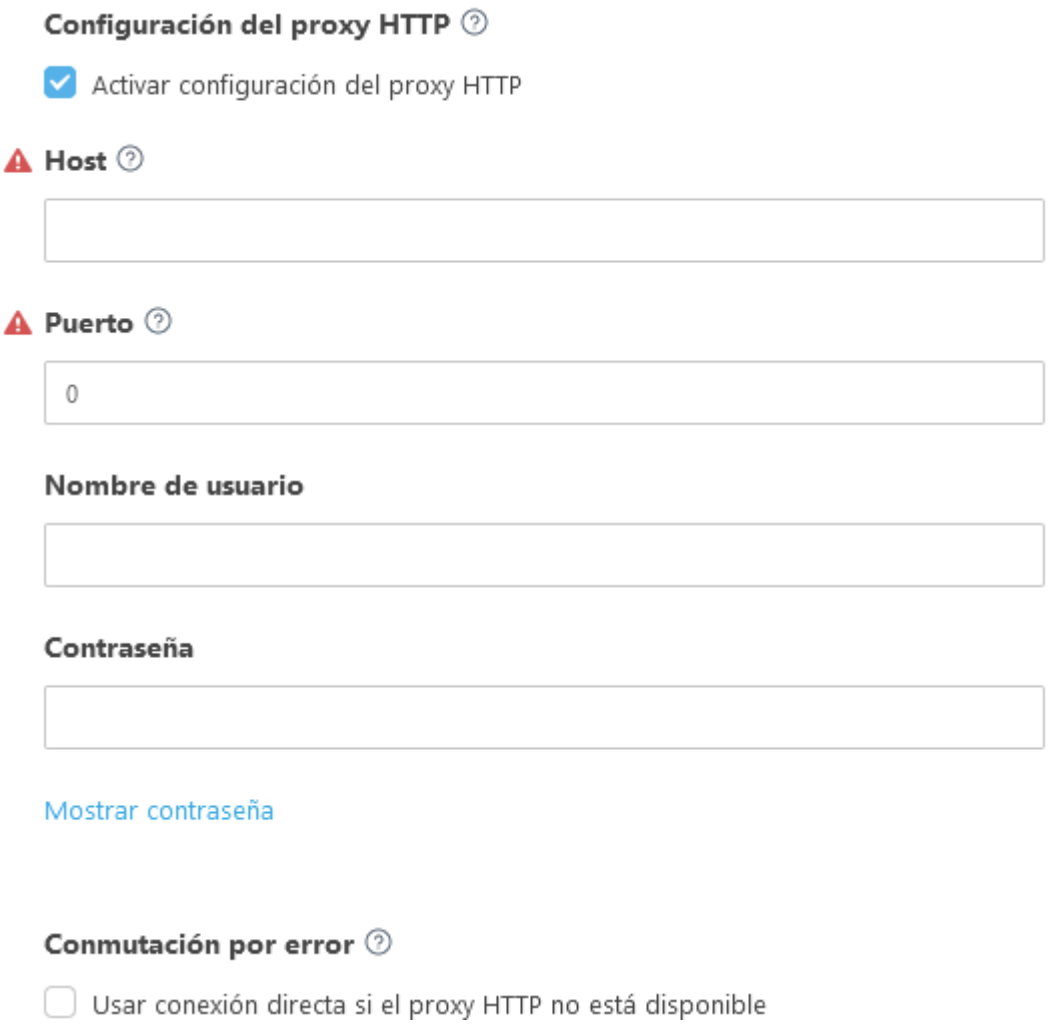
Activar configuración del proxy HTTP

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.



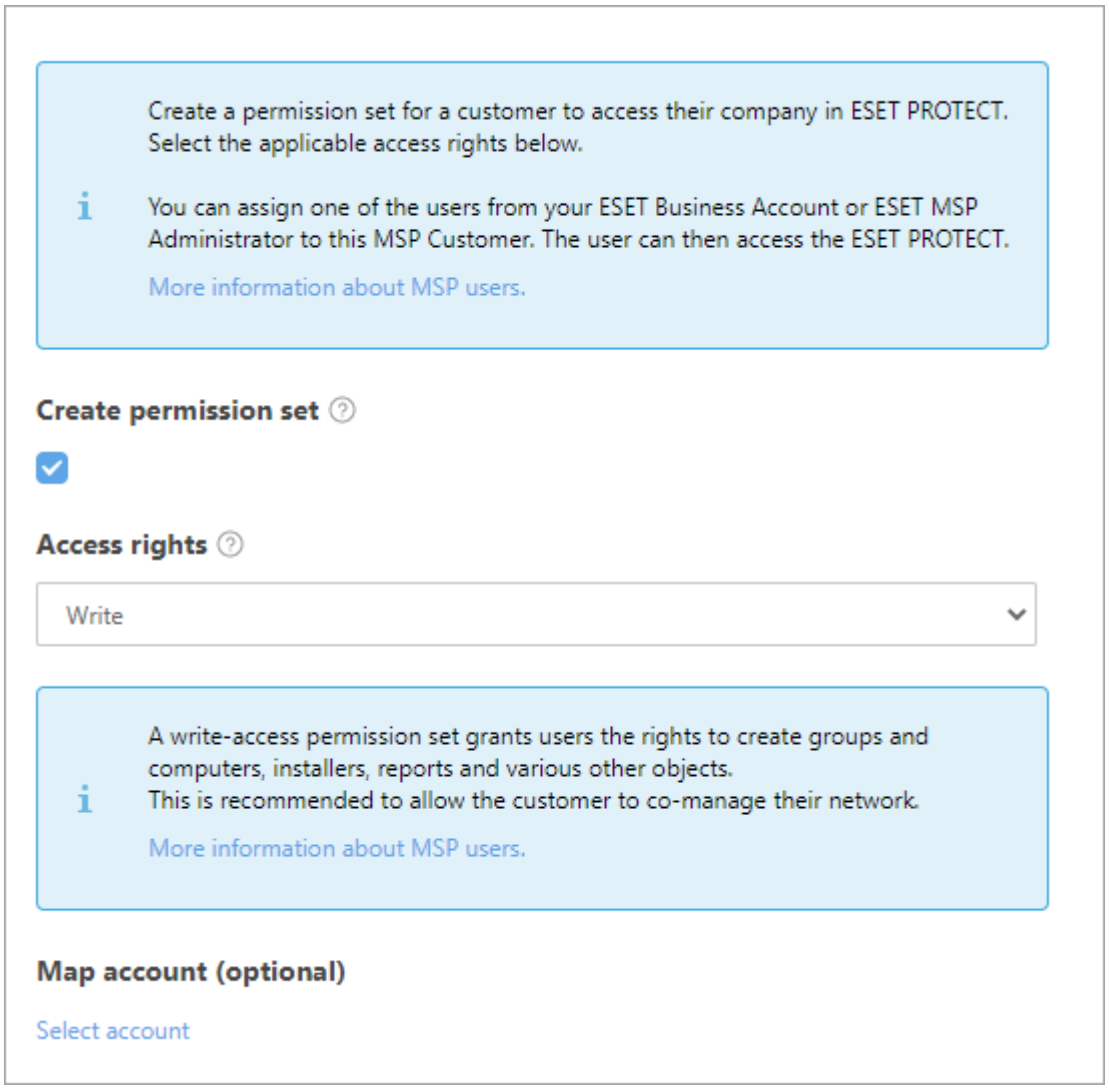
5. Haga clic en **Continuar** para ir a la sección **Usuario**.

6.Puede seleccionar un usuario de su EMA 2 y permitir que el usuario coadministre el ESET PROTECT.

a)Marque la casilla de verificación situada debajo de **Crear conjunto de permisos**.

b)**Derechos de acceso**: El usuario puede iniciar sesión en Web Console y administrar los dispositivos de la empresa. Seleccione el nivel de derechos de acceso de **Lectura** o **Escritura**.

c)**Asignar cuenta (opcional)**: haga clic en **Seleccionar cuenta** y seleccione una de las cuentas disponibles.



¿Problemas para crear un usuario? Asegúrese de que tiene los permisos necesarios.

Haga clic en **Finalizar** para preparar los instaladores. También puede volver a descargar el instalador desde el menú Instaladores si ha seleccionado guardar el instalador.Puede distribuir el paquete de Live Installer de varias formas:

- Haga clic en para copiar el vínculo de descarga del paquete de Live Installer, distribuir el vínculo entre los usuarios y permitir que descarguen e instalen el paquete de Live Installer.
- También puede **Descargar** el paquete Live Installer y distribuirlo personalmente o cargarlo en una ubicación compartida para que accedan los usuarios.
- Solo Windows: Utilice la Remote Deployment Tool para implementar el paquete de Live Installer de forma remota.
- Haga clic en para usar el servidor SMTP de ESET PROTECT y enviar un mensaje de correo electrónico

con el vínculo de descarga del paquete de Live Installer a los usuarios especificados.

- Para agregar un usuario, haga clic en **Agregar** > rellene el campo **Dirección de correo electrónico** > pulse **Entrar** o haga clic en . Si lo desea, haga clic en **Crear usuario,** > escriba el **nombre** del usuario > haga clic en **Guardar**. Puede editar los detalles del usuario en Usuarios del ordenador. Haga clic en **Ver vista previa de mensaje de correo electrónico**, seleccione el **idioma del correo electrónico** en el menú desplegable y haga clic en **Guardar**.

- 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).

Tras la creación, Live Installer se comportará como se muestra en esta tabla.
Live Installer requiere una conexión a Internet, y no funciona en un ordenador sin conexión.
Live Installer en macOS requiere una conexión a Internet directa (para conectarse a los servidores de ESET), y no funciona en un ordenador macOS conectado a Internet mediante proxy sin conexión a Internet directa.

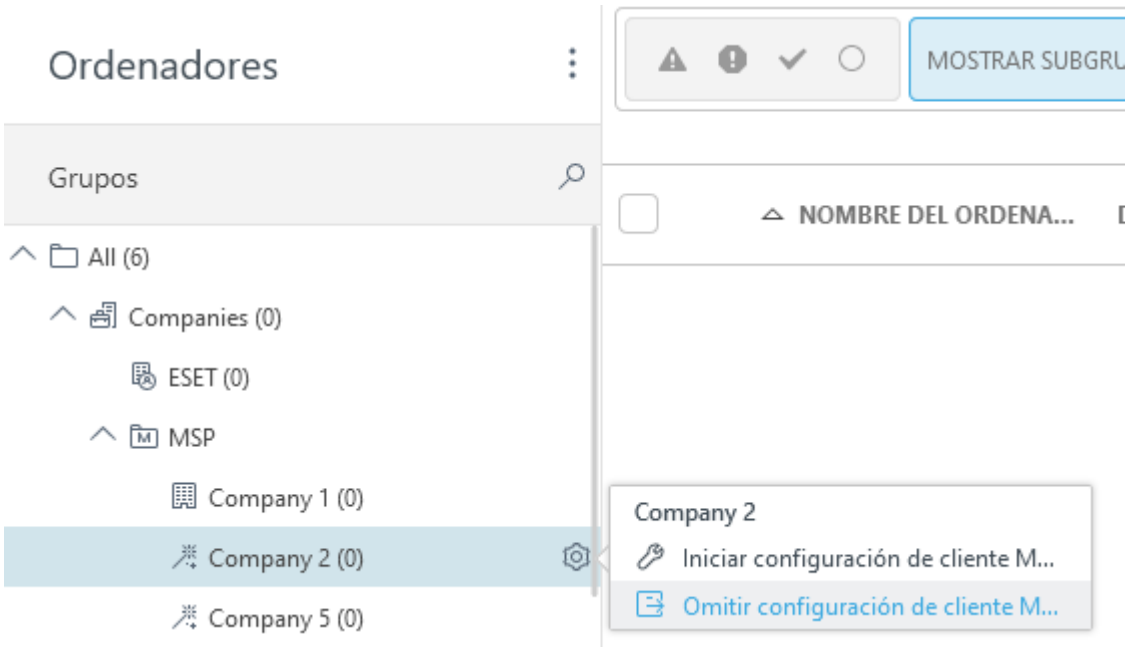
Consulte cómo implementar ESET Management Agent de forma local o remota.

Omitir configuración de cliente MSP

Puede **omitir la configuración de clientes MSP** si no desea configurarlo. También puede crear un instalador más tarde. No le recomendamos omitir la configuración.

Después de omitir la configuración, el icono de la empresa cambia como si se hubiera configurado:

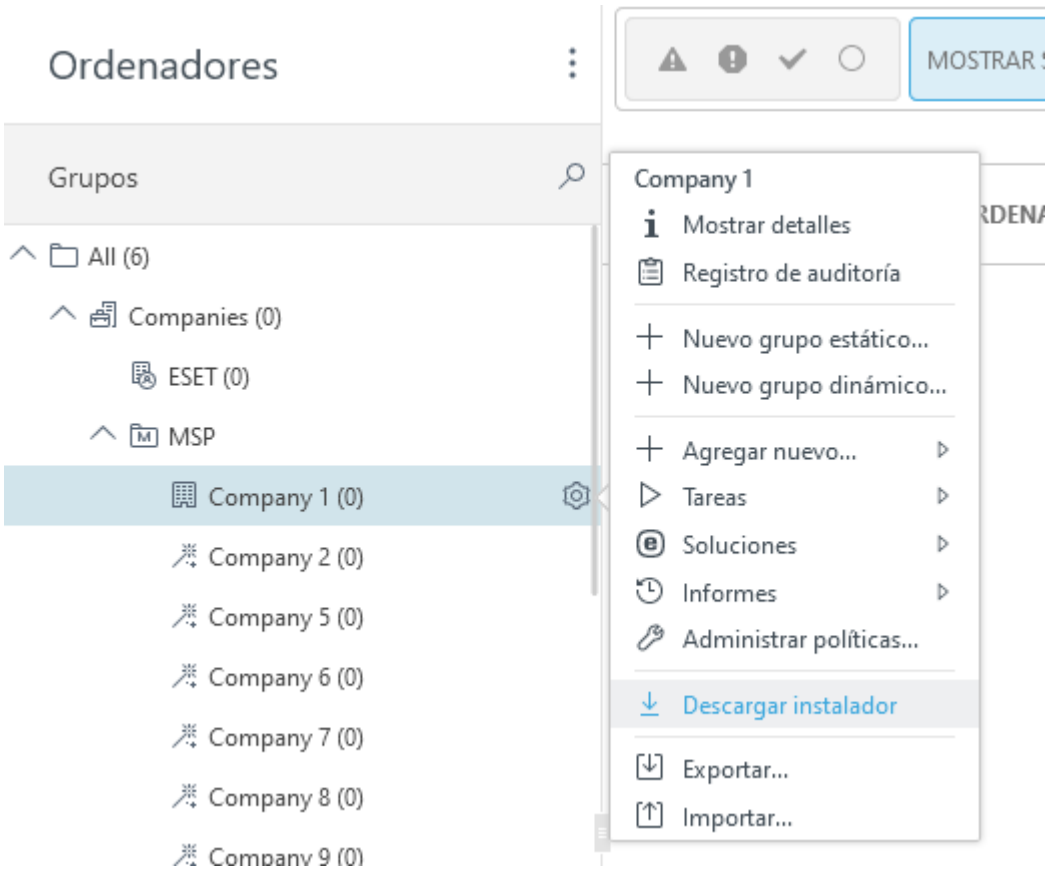
Si omite la configuración, no podrá volver a ejecutar el asistente de instalación para la empresa en la misma instancia de ESET PROTECT.



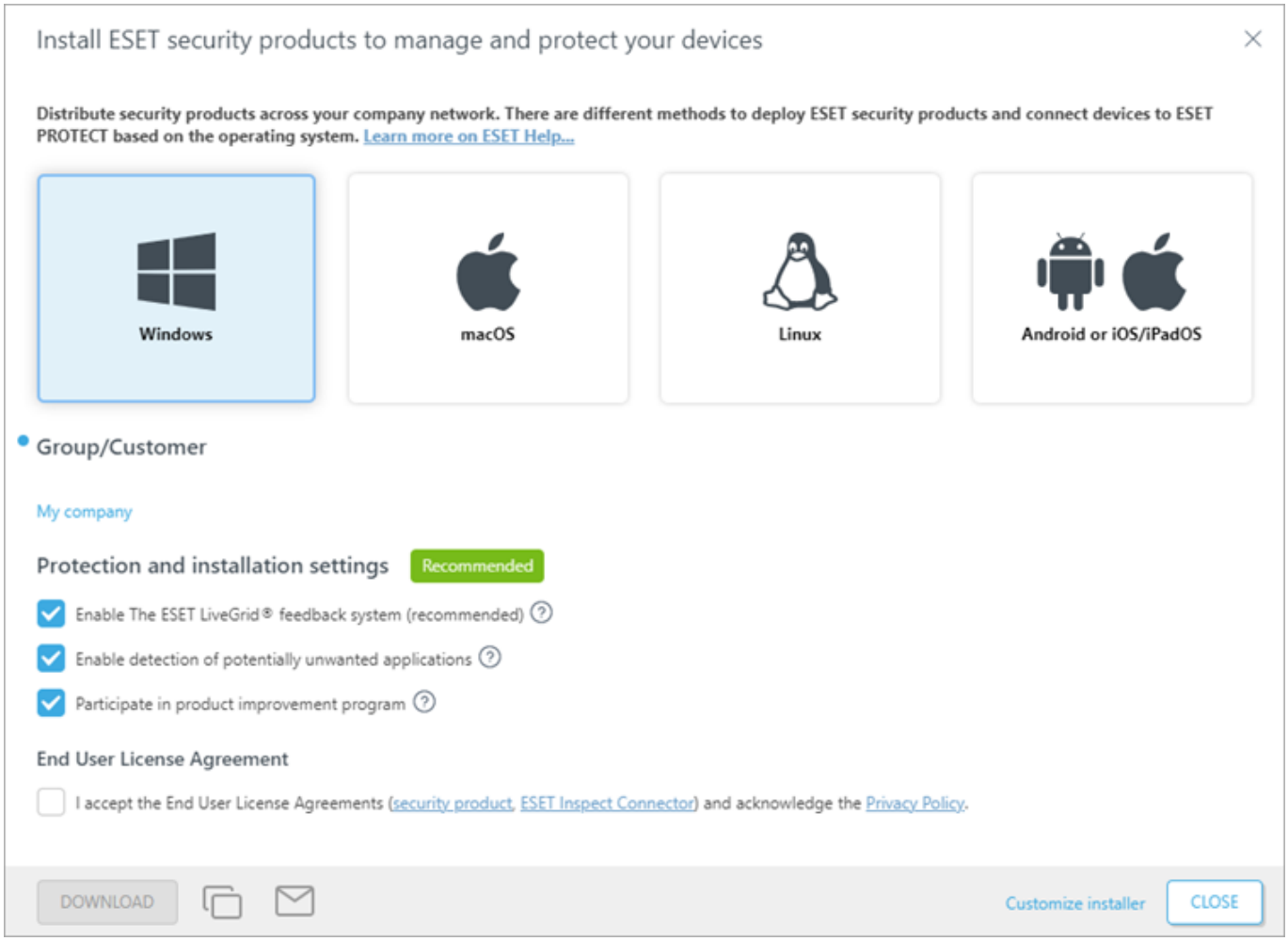
Crear un instalador personalizado

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. Cree y personalice el instalador, y descárguelo.



Usuarios MSP

Durante la configuración de un cliente MSP, puede agregar un usuario existente de EMA2 o EBA a ESET PROTECT. Para revisar y editar el usuario, vaya al menú **Más** > **Derechos de acceso** > **Usuarios**.

Permisos necesarios

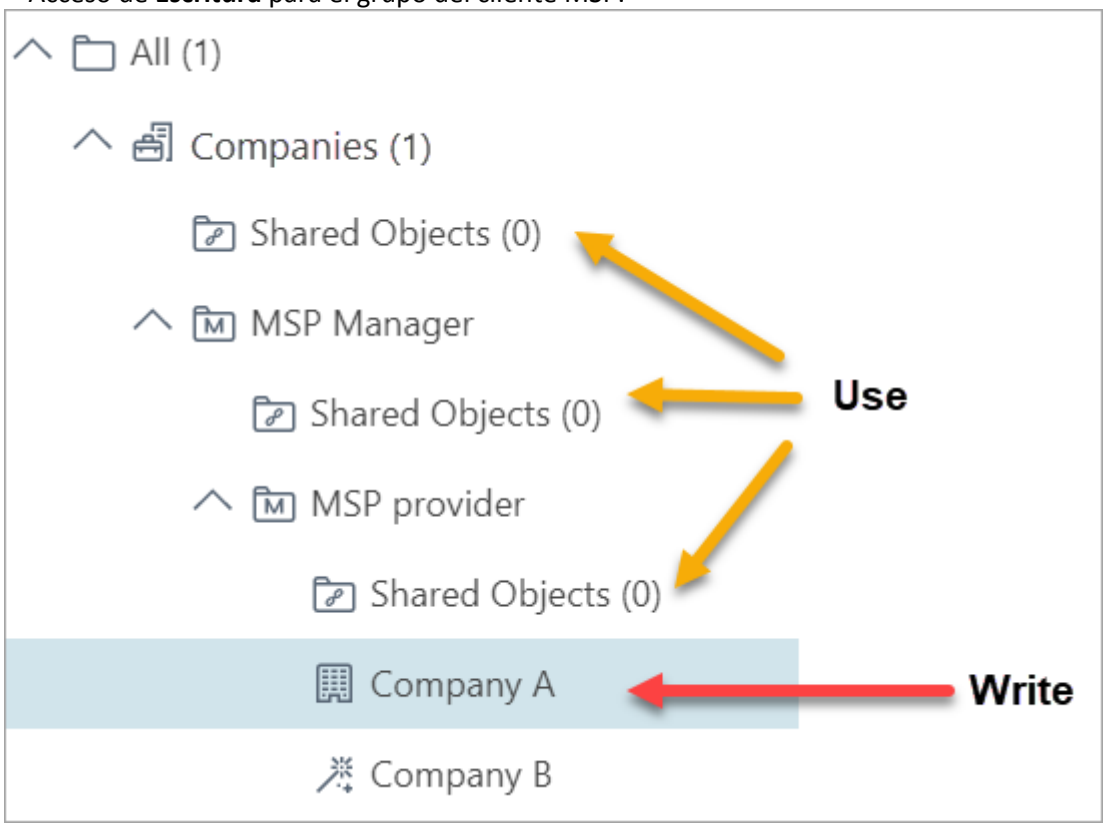
Para crear el nuevo usuario en la configuración de clientes MSP, necesita los derechos de acceso a la empresa que ha configurado y los grupos de **Objetos compartidos**.

Esquema de permisos detallado

Configurar una sola empresa

Derechos de acceso necesarios para crear un usuario durante la configuración de la *Empresa A*:

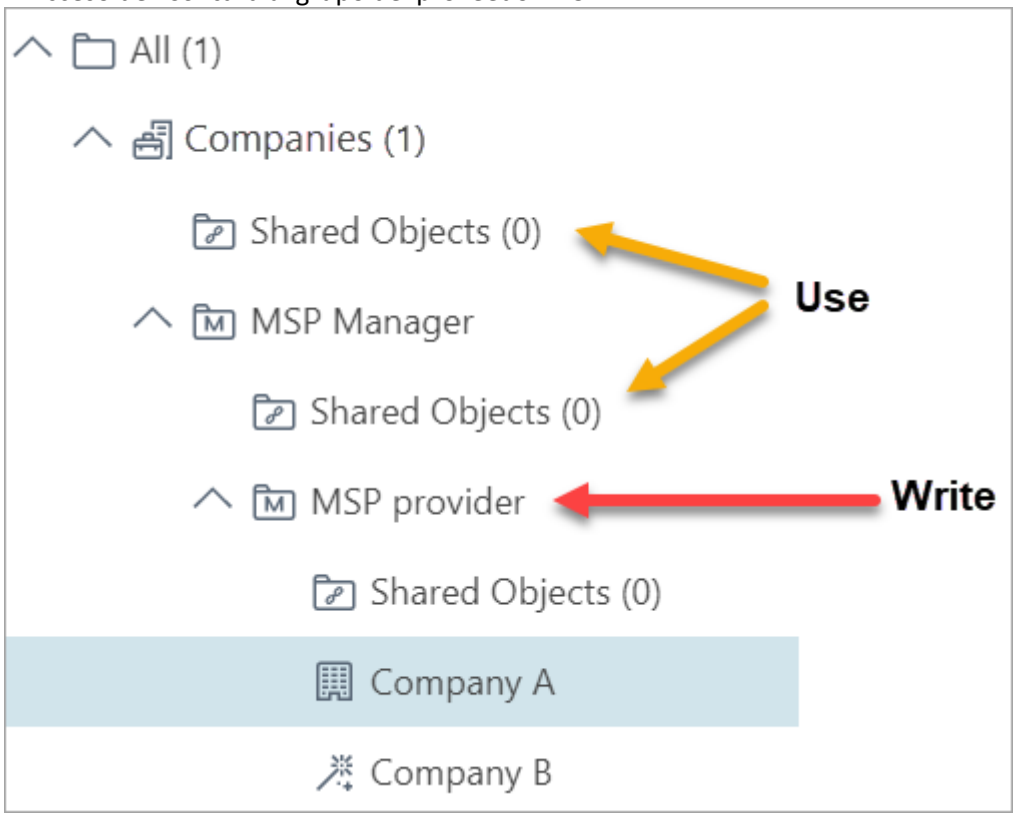
- Acceso de **Uso** para todos los grupos de **Objetos compartidos**.
- Acceso de **Escritura** para el grupo del cliente MSP.



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.

ESET PROTECT 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**.

Etiquetado de objetos MSP

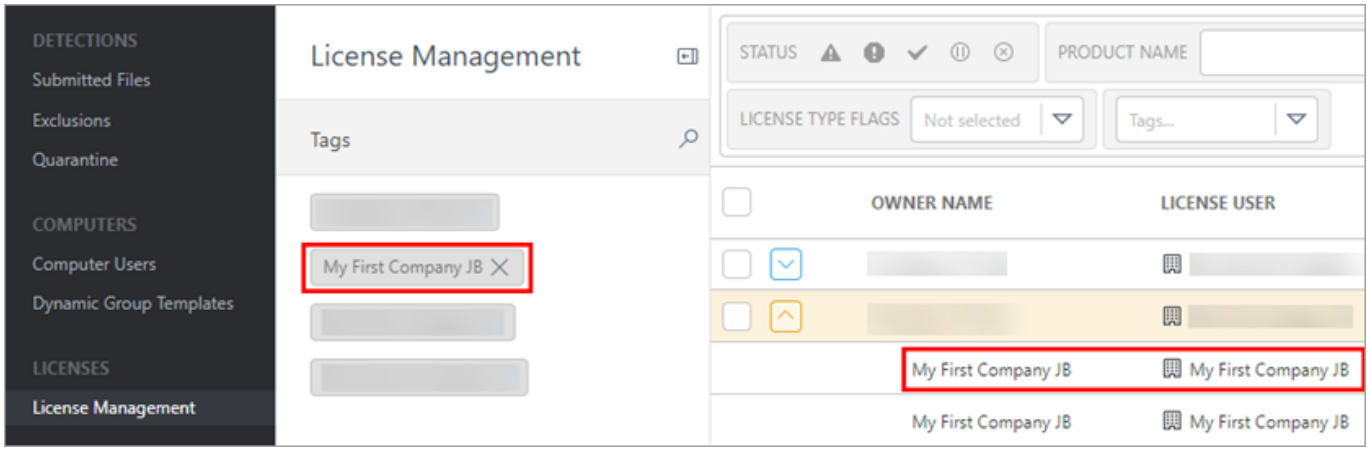
Si utiliza ESET PROTECT con una cuenta EMA 2, activará el etiquetado automático de objetos MSP. Los siguientes objetos se etiquetan de forma automática:

- 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 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**.



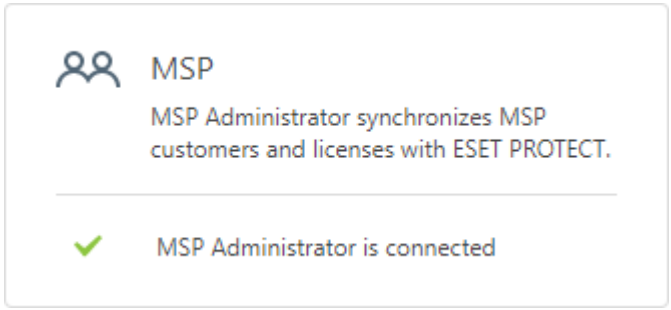
Resumen del estado de MSP

La sección Resumen del estado ofrece información detallada sobre el estado de ESET PROTECT. Si crea su instancia de ESET PROTECT con una cuenta EMA 2 o combinada (EMA 2 y EBA), hay una ventana dinámica de MSP disponible con información relacionada con MSP.

Estados de MSP

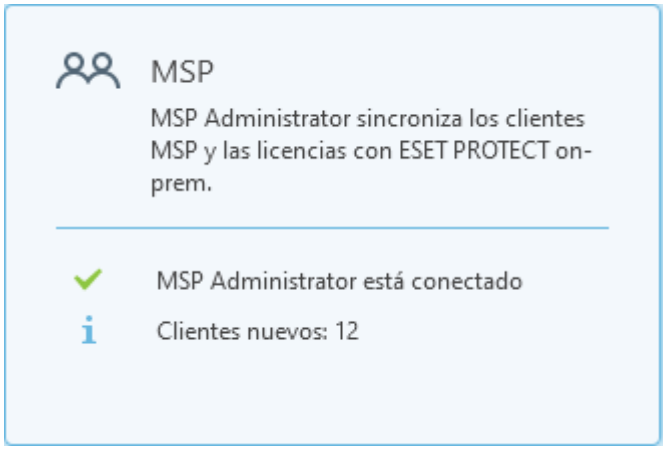
Cuenta sincronizada

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.



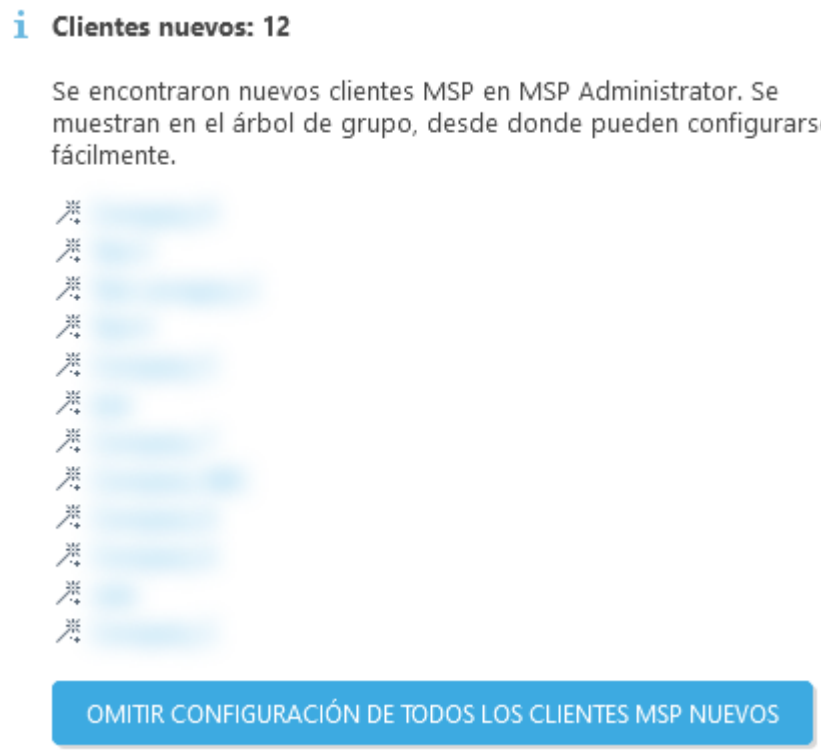
Acciones disponibles

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.



Cloud Mobile Device Management

ESET Cloud Mobile Device Management (Cloud MDM) es una función adicional nativa de ESET PROTECT. ESET Cloud MDM ofrece administración de dispositivos móviles Android y iOS y administración de seguridad móvil.

ESET Cloud MDM ofrece una solución sin agente, en la que el agente de administración no se ejecuta

directamente en el dispositivo móvil (para ahorrar batería y el rendimiento del dispositivo móvil). En su lugar, el agente de administración del dispositivo móvil se virtualiza en la nube de ESET.

ESET administra toda la seguridad y los certificados de conexión, por lo que el administrador no tiene que preocuparse del proceso de renovación de certificados ni de que los certificados cumplan las normas de seguridad más recientes.

Compruebe que la versión del SO del dispositivo móvil es compatible con la administración mediante Cloud MDM y que cumple los requisitos de red.

> Los dispositivos móviles inscritos deben conectarse a ESET PROTECT cada 120 días para evitar problemas de conexión. Puede ver esta información en el vínculo del correo electrónico o el código QR de inscripción. No inscriba un dispositivo de repuesto por adelantado. Recomendamos inscribir solo un dispositivo de repuesto, que se utilizará antes de 120 días.

El proceso de administración de dispositivos móviles consta de las partes siguientes:

- Inscripción de dispositivos móviles: según el tipo de dispositivos móviles que planee administrar y en qué modo, debe completar diferentes pasos antes de poder comenzar a administrar los dispositivos móviles. Cloud MDM admite estos tipos de inscripción de dispositivos móviles:
  - Inscripción de Android
  - Inscripción de propietario del dispositivo Android
  - Inscripción con Microsoft Entra ID (Android o iOS)
  - Sincronización con Microsoft Intune (Android)
  - Sincronización con VMware Workspace ONE (Android)
  - Inscripción de iOS
  - Sincronización de Apple Business Manager (ABM) (iOS)
- Administración de dispositivos móviles: después de inscribir sus dispositivos móviles Android, puede comenzar a administrarlos.

Inscripción: agregar dispositivos móviles

Si desea administrar un dispositivo móvil, inscriba el dispositivo en la consola web de la nube, para lo cual deberá hacer clic en **Ordenadores** > **Agregar dispositivo** > **Android o iOS/iPadOS**.

Acuerdo de licencia para el usuario final: marque la casilla de verificación si acepta el EULA y la política de privacidad.

a)Haga clic en **Inscribir con código QR** para generar el código QR de inscripción:

1.En la ventana nueva, especifique el **Nombre del dispositivo** del nuevo dispositivo móvil que desee inscribir y haga clic en **Generar código QR**.

2.Escanee el código QR mostrado con el dispositivo móvil que desea inscribir.

3.Tras inscribir correctamente el dispositivo móvil seleccionado, haga clic en **Inscribir siguiente** para generar otro código QR para otro dispositivo móvil o en **Cerrar** si ha terminado de inscribir dispositivos móviles.

b)Haga clic en ✉ para abrir la ventana **Inscribir un dispositivo móvil por correo electrónico**:

Especifique los dispositivos móviles que desee inscribir; puede utilizar las opciones que se indican a continuación para agregar dispositivos móviles.

• **Agregar**: Entrada única: debe escribir manualmente el nombre del dispositivo y una dirección de correo electrónico asociada al dispositivo móvil. (Si se entrega por correo electrónico, se enviará un mensaje de correo electrónico de inscripción a esta dirección). 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 **Más** > Usuarios del ordenador. Si desea agregar otro dispositivo móvil, haga clic de nuevo en **Agregar** y envíe la información necesaria.

• **Más**:

- **Agregar usuarios**: puede agregar dispositivos marcando las casillas de verificación de los usuarios correspondientes en **Más** > Usuarios del ordenador.

- **Importar CSV**: utilice esta opción para agregar muchos dispositivos móviles fácilmente. 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 especifique el **nombre del dispositivo** en cada entrada cuando utilice el método de **importación de CSV**. Lo verá como **Nombre del ordenador** en **Ordenadores**. Si deja vacío el campo **Nombre del dispositivo**, se utilizará en su lugar la dirección de correo electrónico, y aparecerá como **Nombre del ordenador** en **Ordenadores** y en **Grupos**. Evite usar la misma dirección de correo electrónico para inscribir varios dispositivos, ya que le impedirá distinguir un dispositivo de otro.

Haga clic en **Personalizar correo electrónico** para ver la vista previa del correo electrónico y personalizar el **Asunto** y el **Contenido**.

c)Haga clic en **Personalizar inscripción** para utilizar un asistente de inscripción más detallado (véase a continuación).

Básico

Seleccione un tipo de inscripción:

- **Android o iOS/iPadOS**: se trata de un procedimiento de inscripción estándar para dispositivos Android o iOS/iPadOS.

- **Propietario del dispositivo Android**: controle totalmente el dispositivo Android administrado.

- **Dispositivos Android con opciones de entrada limitadas**: procedimiento de inscripción alternativo para inscribir dispositivos Android sin una cámara (lo que limita la inscripción con código QR) o sin servicio de correo electrónico (lo que limita la inscripción por correo electrónico).

> Consulte también los pasos de sincronización para:
> - Dispositivos Android y iOS administrados por Microsoft Entra ID
> - Dispositivos Android administrados por Microsoft Intune
> - Dispositivos iOS administrados por ABM
> - Dispositivos Android administrados por VMware Workspace ONE

Distribución

En la sección **Distribución**, puede seleccionar el método de entrega del vínculo de inscripción adecuado para los dispositivos en función de su accesibilidad y del número de dispositivos.

- **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 dispositivos móviles a los que no tiene acceso físico. Para utilizar esta opción se necesita participación activa del usuario o propietario del dispositivo móvil.

- **Escanear código QR**: inscripción de un solo dispositivo móvil. Podrá inscribir un dispositivo móvil cada vez,

y tendrá que repetir el proceso con cada dispositivo. Recomendamos esta opción solo cuando tenga que inscribir menos 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. También puede utilizar esta opción si tiene dispositivos móviles nuevos que va a entregar a los usuarios después de configurarlos.

- **Insertar código de seguridad**: inscripción de un solo dispositivo móvil que se usa específicamente si un dispositivo móvil Android no tiene cámara ni cliente de correo electrónico.

Grupo principal: seleccione el grupo principal inicial al que se asignará el dispositivo móvil después de la inscripción.

Personalizar más configuraciones

Licencia – Seleccione la licencia adecuada para la activación del producto de seguridad móvil.

Etiquetas: seleccione o agregue las etiquetas pertinentes para identificar el dispositivo móvil.

Configuración del producto

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.

Puede configurar ajustes adicionales para el propietario del dispositivo Android:

- Marque la casilla **Mantener las aplicaciones del sistema instaladas en dispositivos móviles** para mantener las aplicaciones preinstaladas por el proveedor de telefonía móvil.

- Marque la casilla **Configurar red Wi-Fi** para configurar la conexión Wi-Fi del dispositivo. Escriba el **SSID** (nombre) y seleccione el **Tipo de seguridad**:**Ninguno WPA** o **WEP**. Si ha seleccionado WPA o WEP, escriba la **contraseña**.

No comparta ni almacene el código QR, ya que contiene la contraseña de la red Wi-Fi.

Lista

Especifique los dispositivos móviles que desee inscribir; puede utilizar las opciones que se indican a continuación para agregar dispositivos móviles.

- **Agregar**: Entrada única: debe escribir manualmente el nombre del dispositivo y una dirección de correo electrónico asociada al dispositivo móvil. (Si se entrega por correo electrónico, se enviará un mensaje de correo electrónico de inscripción a esta dirección). 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 **Más** > Usuarios del ordenador. Si desea agregar otro dispositivo móvil, haga clic de nuevo en **Agregar** y envíe la información necesaria.

- **Más**:

  o**Agregar usuarios**: puede agregar dispositivos marcando las casillas de verificación de los usuarios correspondientes en **Más** > Usuarios del ordenador.

- **Importar CSV**: utilice esta opción para agregar muchos dispositivos móviles fácilmente. 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 especifique el **nombre del dispositivo** en cada entrada cuando utilice el método de **importación de CSV**. Lo verá como **Nombre del ordenador** en **Ordenadores**. Si deja vacío el campo **Nombre del dispositivo**, se utilizará en su lugar la dirección de correo electrónico, y aparecerá como **Nombre del ordenador** en **Ordenadores** y en **Grupos**. Evite usar la misma dirección de correo electrónico para inscribir varios dispositivos, ya que le impedirá distinguir un dispositivo de otro.

Haga clic en **Personalizar correo electrónico** para ver la vista previa del correo electrónico y personalizar el **Asunto** y el **Contenido**.

Inscripción

En esta sección puede consultar todos los parámetros del proceso de inscripción.

> El vínculo de inscripción del correo electrónico o el código QR es válido durante 14 días.

- **Enviar correo electrónico**: consulte la lista de dispositivos con sus direcciones de correo electrónico correspondientes. Haga clic en **Vista previa de mensaje de correo electrónico** para ver la plantilla de correo electrónico que se entregará en cada una de las direcciones de correo electrónico de la lista. Haga clic en **Enviar** para enviar el mensaje de correo electrónico a las direcciones de correo electrónico especificadas. Haga clic en **Ver más** en la ventana de confirmación para ver la lista de direcciones de correo electrónico a las que envió el correo electrónico de inscripción. Haga clic en **Exportar** para exportar la lista de dispositivos y correos electrónicos como CSV.

- **Escanear código QR**: consulte la lista de dispositivos que se pueden inscribir. En la parte derecha de la pantalla puede ver el código QR específico del dispositivo seleccionado en la lista.

- **Insertar código de seguridad**: inserte el código de seguridad generado en el dispositivo móvil que desea inscribir.

> Los dispositivos móviles inscritos deben conectarse a ESET PROTECT cada 120 días para evitar problemas de conexión. Puede ver esta información en el vínculo del correo electrónico o el código QR de inscripción. No inscriba un dispositivo de repuesto por adelantado. Recomendamos inscribir solo un dispositivo de repuesto, que se utilizará antes de 120 días.

Para completar la inscripción de dispositivos móviles, siga estos pasos:

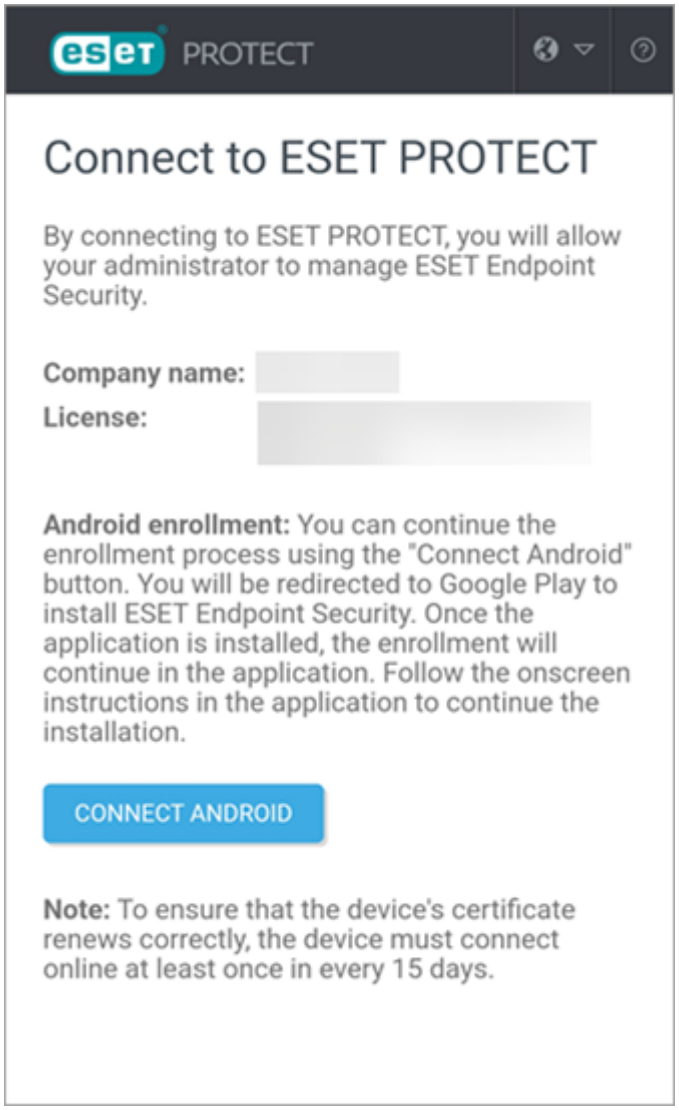
- Inscripción de dispositivo Android
- Inscripción de Android: propietario del dispositivo
- Inscripción de dispositivo

Inscripción de dispositivo Android

Siga los pasos que se indican a continuación para inscribir un dispositivo Android en ESET PROTECT:

Los dispositivos móviles inscritos deben conectarse a ESET PROTECT cada 120 días para evitar problemas de conexión. Puede ver esta información en el vínculo del correo electrónico o el código QR de inscripción. No inscriba un dispositivo de repuesto por adelantado. Recomendamos inscribir solo un dispositivo de repuesto, que se utilizará antes de 120 días.

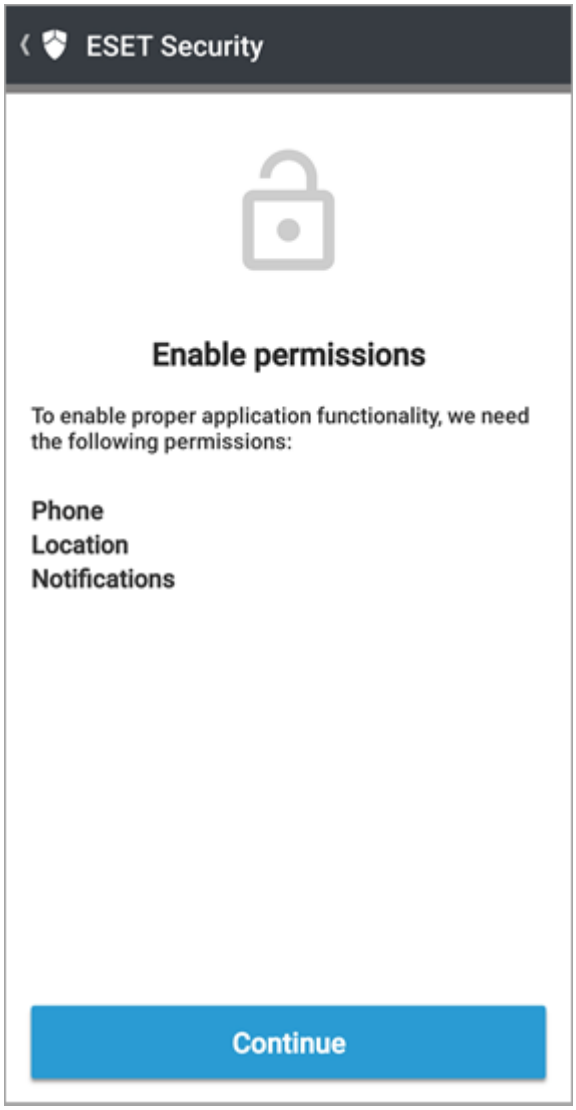
1. Abra el enlace de inscripción desde un correo electrónico o código QR y pulse **Conectar Android**.



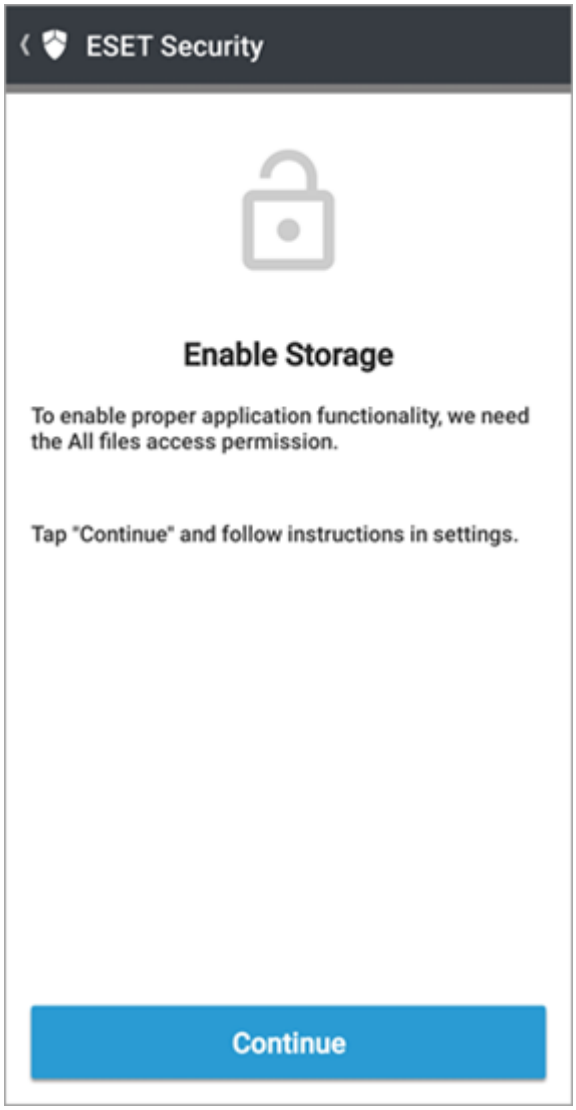
Si no tiene ESET Endpoint Security para Android instalado en el dispositivo móvil, se le redirigirá automáticamente a Google Play para que descargue la aplicación.

Si le aparece la notificación **No se encontró ninguna aplicación para abrir la URL**, pruebe a abrir el vínculo de inscripción en el navegador web predeterminado de Android.

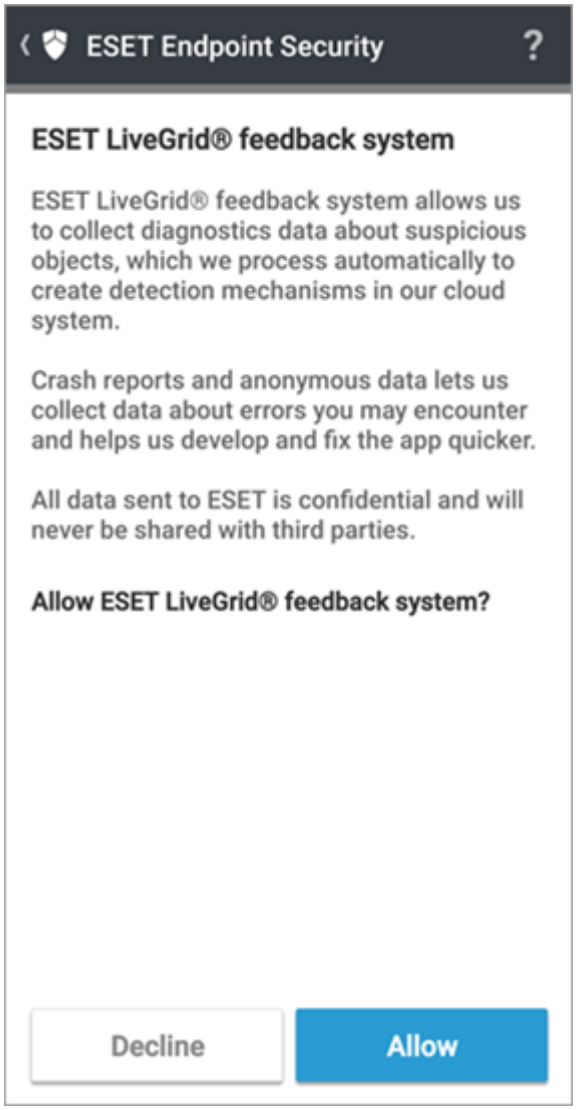
2. Pulse **Continuar** para activar los permisos de **Teléfono**, **Ubicación** y **Notificaciones** necesarios:



3. Pulse **Continuar** para habilitar el permiso de acceso a todos los archivos.

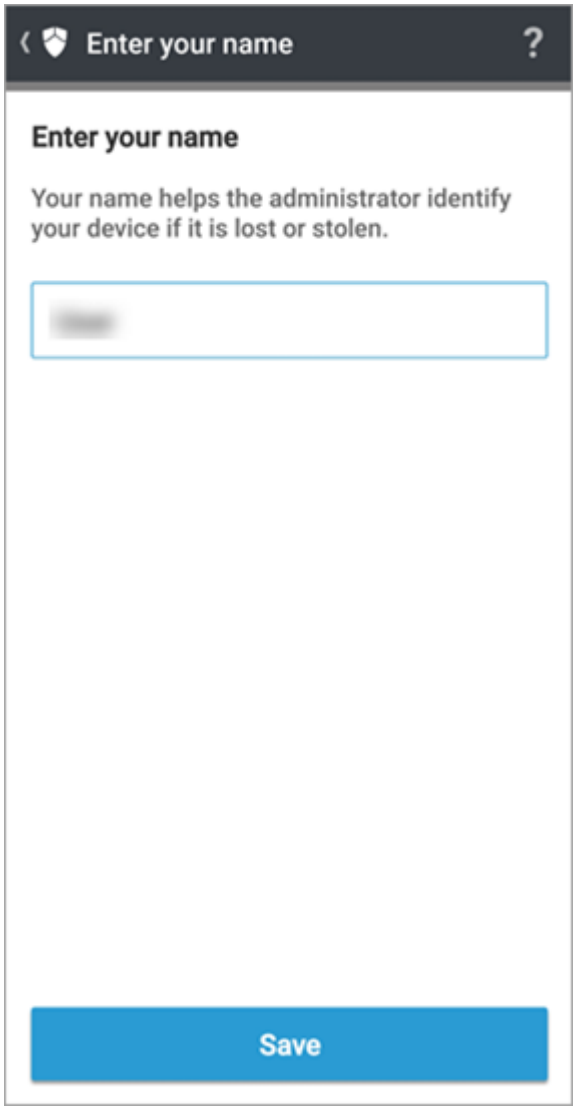


4. Pulse **Permitir** o **Rechazar** para activar ESET LiveGrid®.

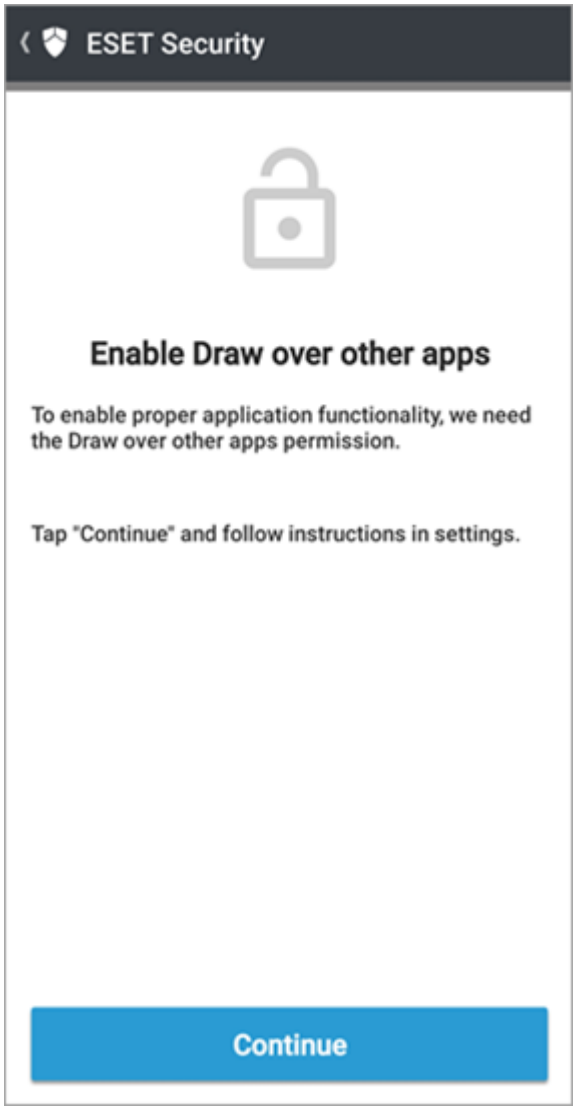


5. Escriba su nombre y pulse **Guardar**.

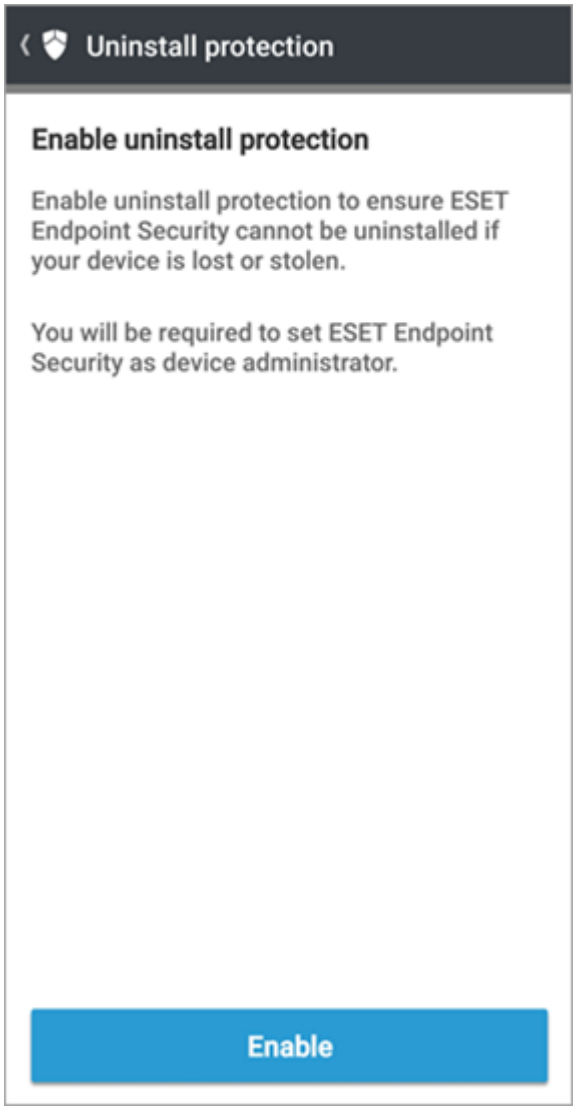
El nombre no se muestra en ESET PROTECT, se utiliza para Antirrobo y para el registro de diagnóstico.



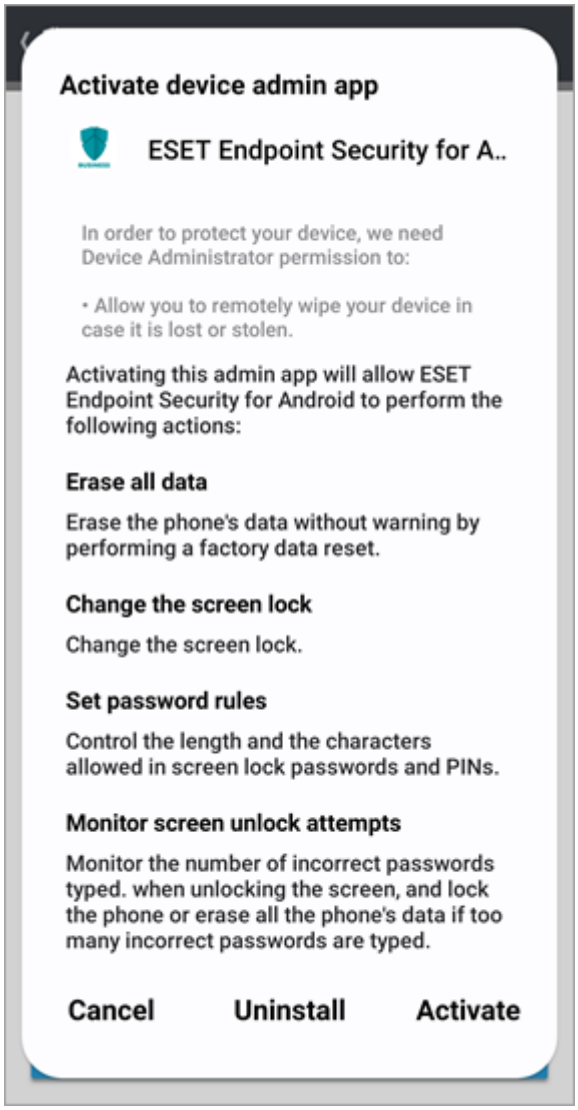
6. Pulse **Continuar** para habilitar el permiso Mostrar sobre otras aplicaciones.



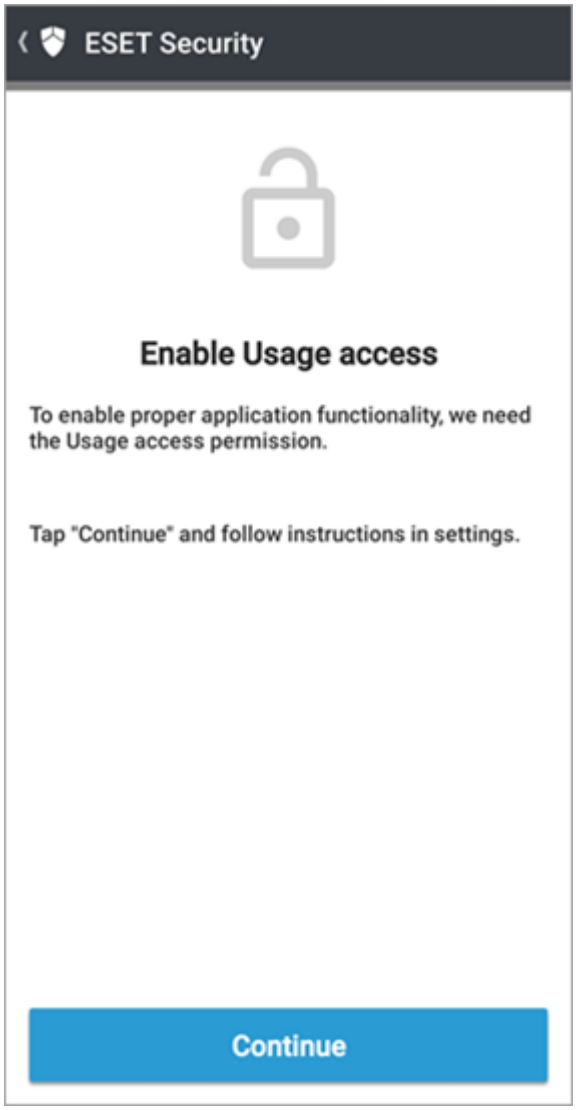
7. Pulse **Habilitar** para activar la protección contra desinstalación y asegurarse de que ESET Endpoint Security para Android no se pueda desinstalar si el dispositivo se pierde o se lo roban.



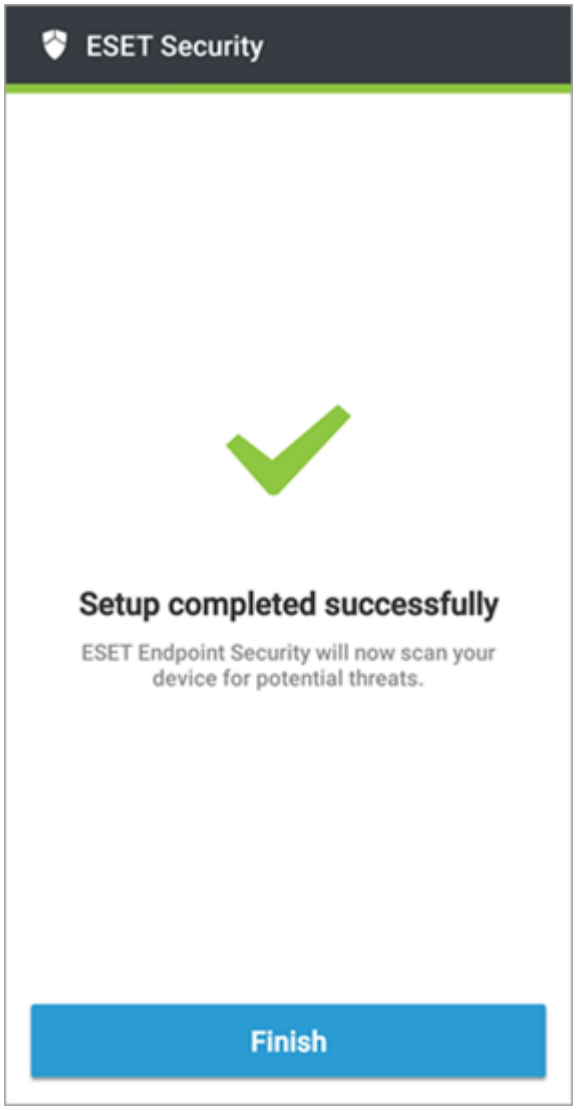
8. Pulse **Activar** para habilitar el permiso de administrador del dispositivo en ESET Endpoint Security para Android.



9. Pulse **Continuar** para habilitar el permiso de acceso de uso.



10. Pulse **Finalizar**.



ESET Endpoint Security for Android se abre y ESET PROTECT administra ahora el dispositivo móvil.

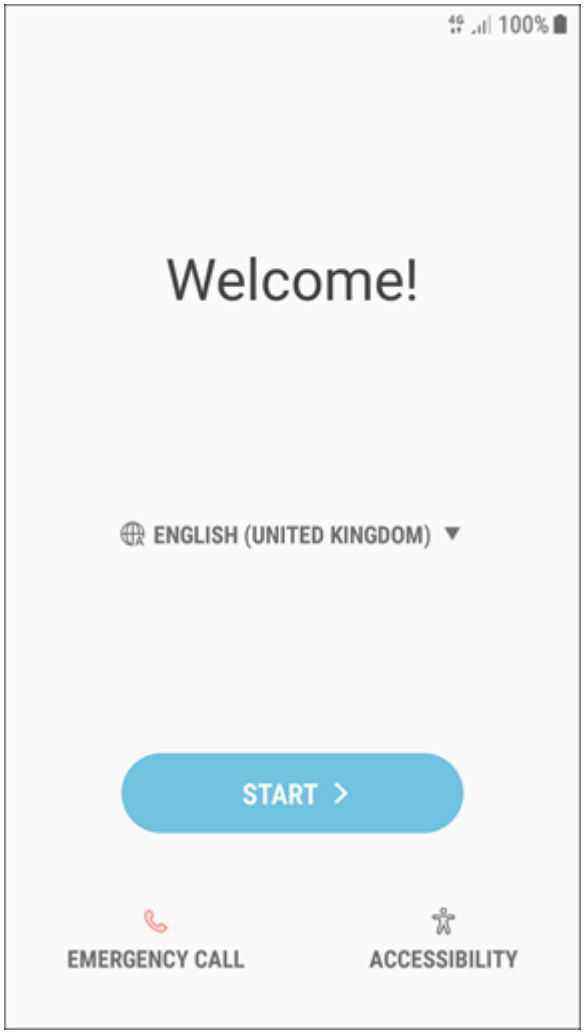
Inscripción de Android: propietario del dispositivo

El tipo de inscripción Propietario del dispositivo solo está disponible para dispositivos Android con Android 7 y versiones posteriores.
El dispositivo Android debe ser nuevo o haberse borrado o restablecido su configuración predeterminada para poder realizar los pasos de inscripción que se indican a continuación.

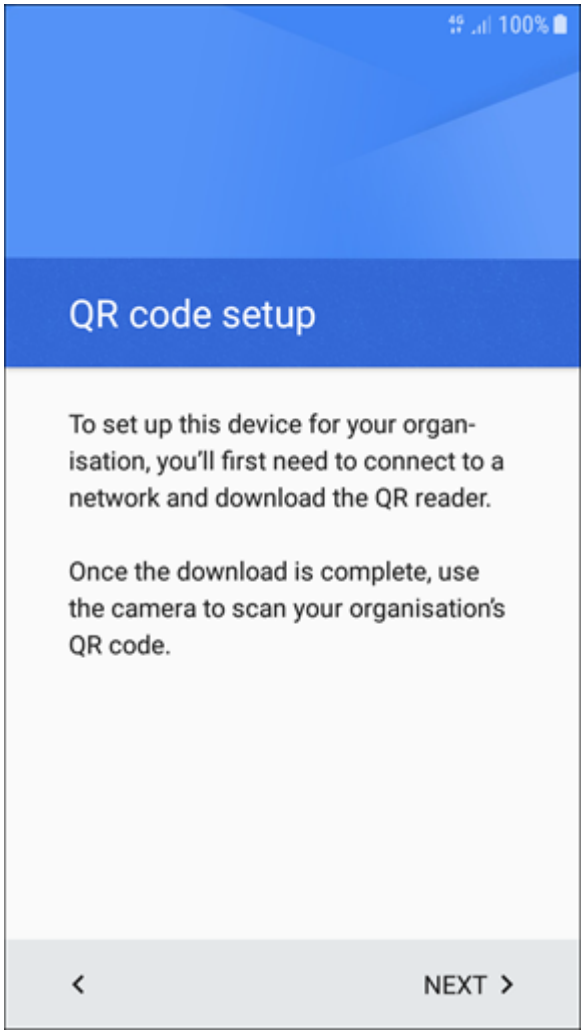
1. Encienda el dispositivo móvil.

2. Introduzca el pin de la tarjeta SIM.

3. En la pantalla de bienvenida, seleccione el idioma preferido y toque la pantalla seis (6) veces cerca del texto **«Bienvenido»** para iniciar la configuración del código QR.

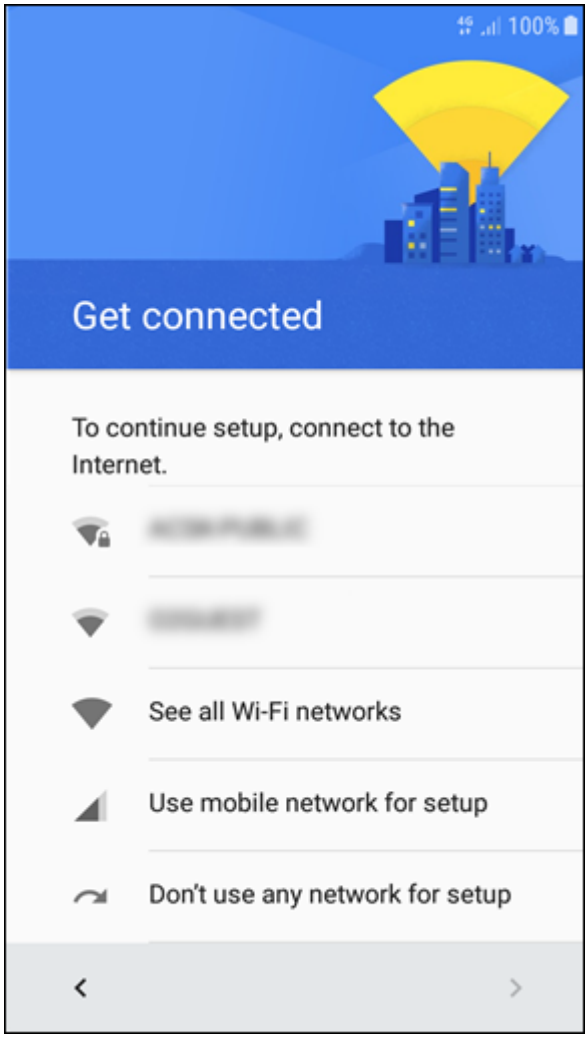


4. Aparecerá la pantalla **Configuración del código QR**. Toque **Siguiente** para continuar.



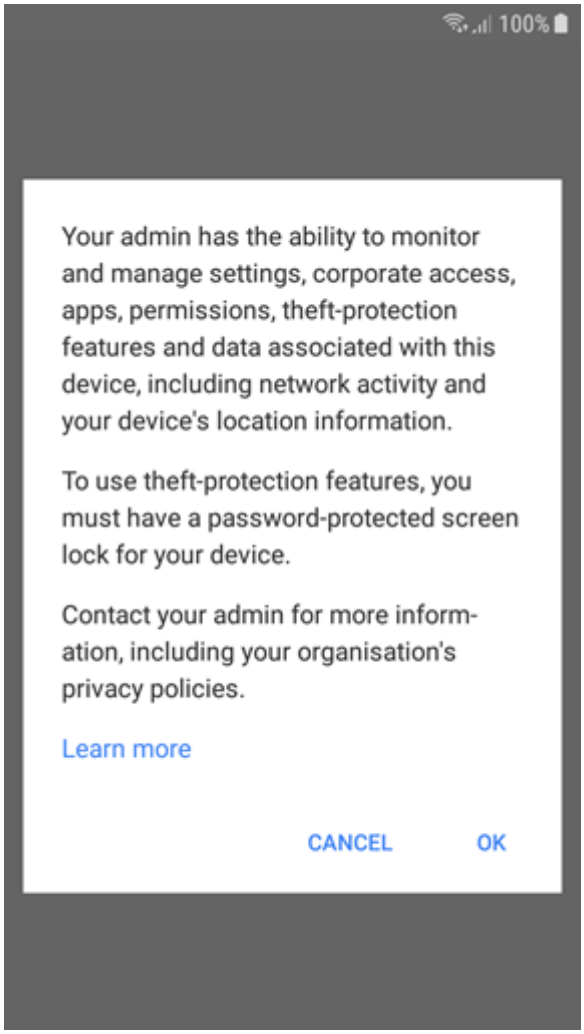
Algunos dispositivos pueden requerir que cifre el almacenamiento del dispositivo (a veces, también es necesario conectar el cargador). Seleccione el tipo de cifrado que desee y siga las instrucciones de la pantalla.

5. Seleccione una conexión a Internet para descargar el lector de códigos QR necesario para el siguiente paso.

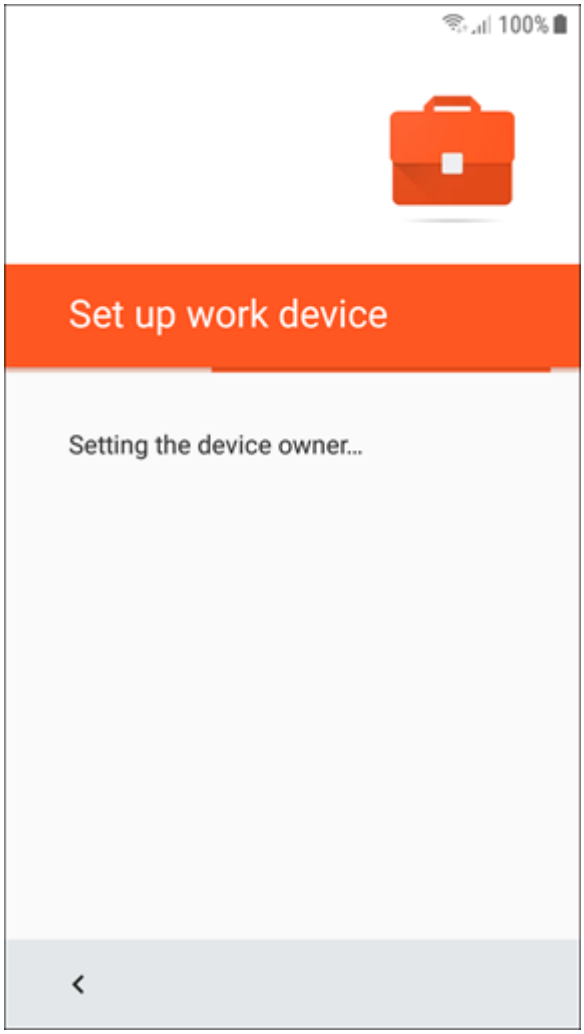


6. Ahora se instalará el lector de códigos QR. Después de terminar la instalación, lea el código QR que se generó en la Consola Web de ESET PROTECT.

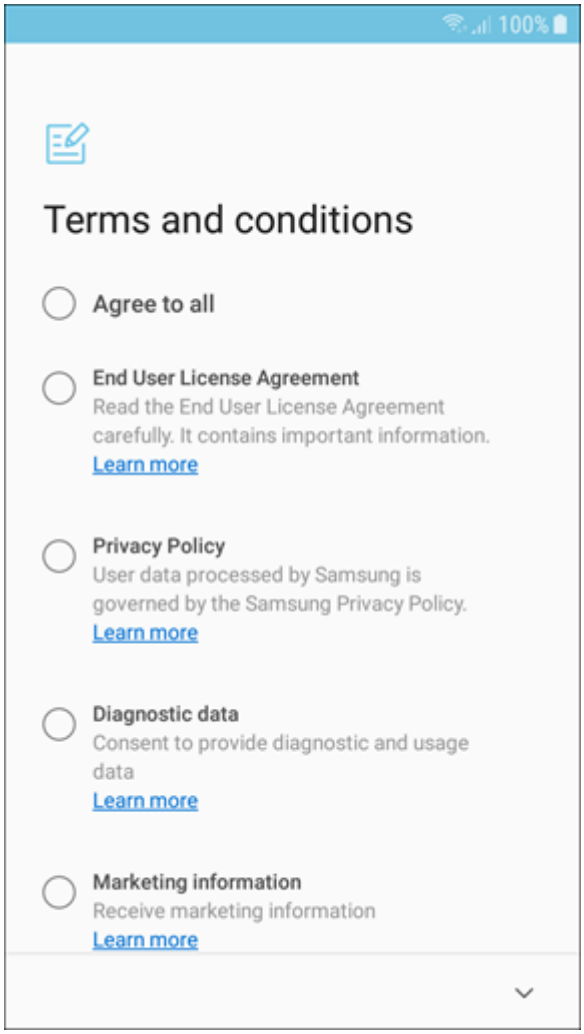
7. Se le pedirá que confirme que comprende que está concediendo más derechos de propietario del dispositivo al administrador. Pulse **Aceptar** para continuar.



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.



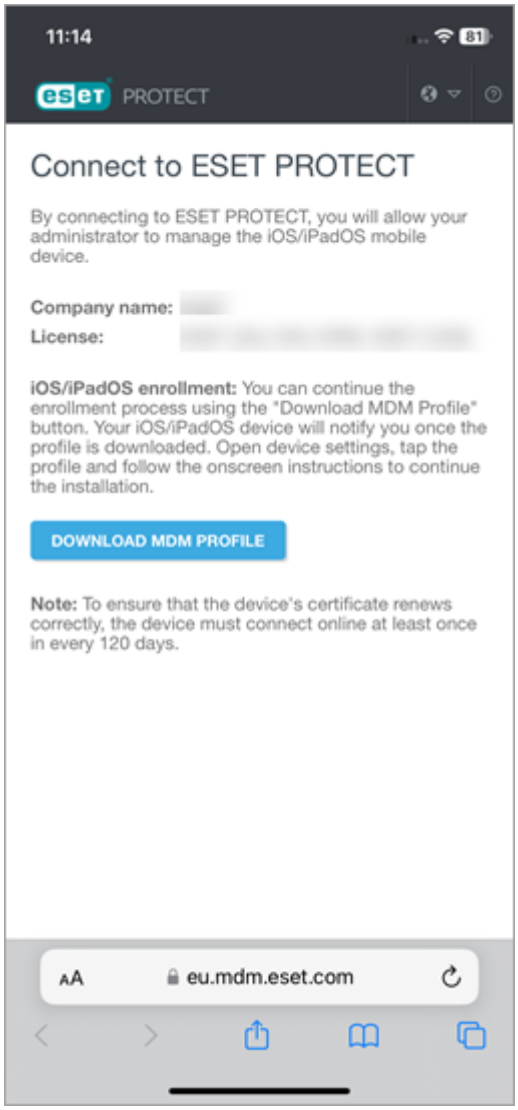
10. El dispositivo está inscrito en el modo Propietario del dispositivo.

Inscripción de dispositivo iOS

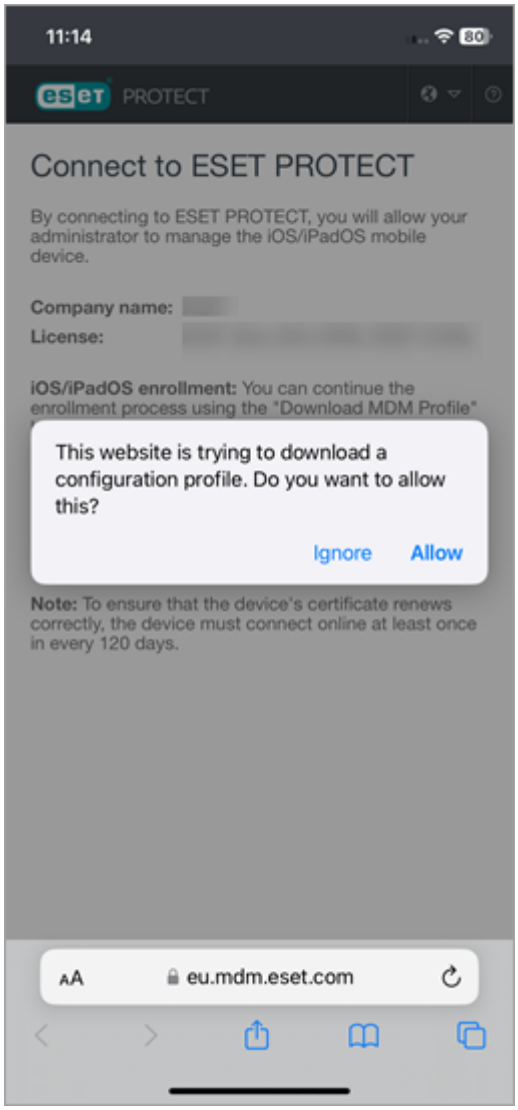
Siga los pasos indicados a continuación para inscribir un dispositivo iOS en ESET PROTECT:

> Los dispositivos móviles inscritos deben conectarse a ESET PROTECT cada 120 días para evitar problemas de conexión. Puede ver esta información en el vínculo del correo electrónico o el código QR de inscripción. No inscriba un dispositivo de repuesto por adelantado. Recomendamos inscribir solo un dispositivo de repuesto, que se utilizará antes de 120 días.

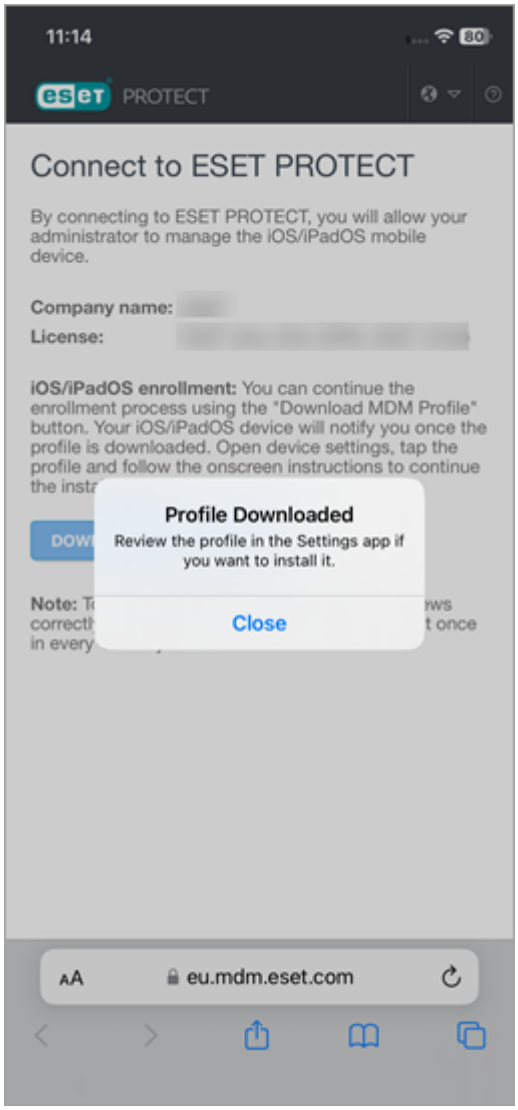
1. Abra el enlace de inscripción desde un correo electrónico o código QR y pulse **Descargar perfil MDM**.



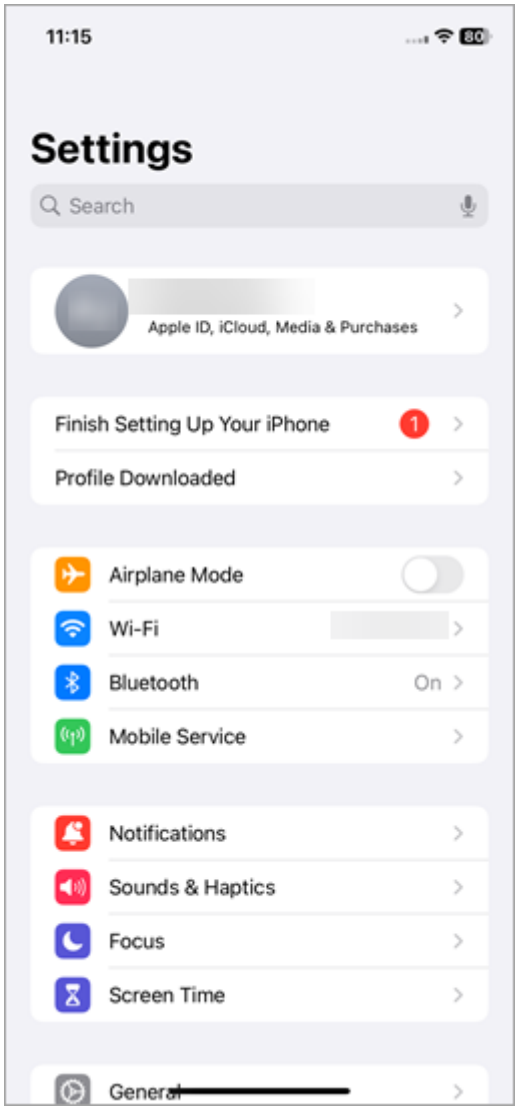
2. Pulse **Permitir**.



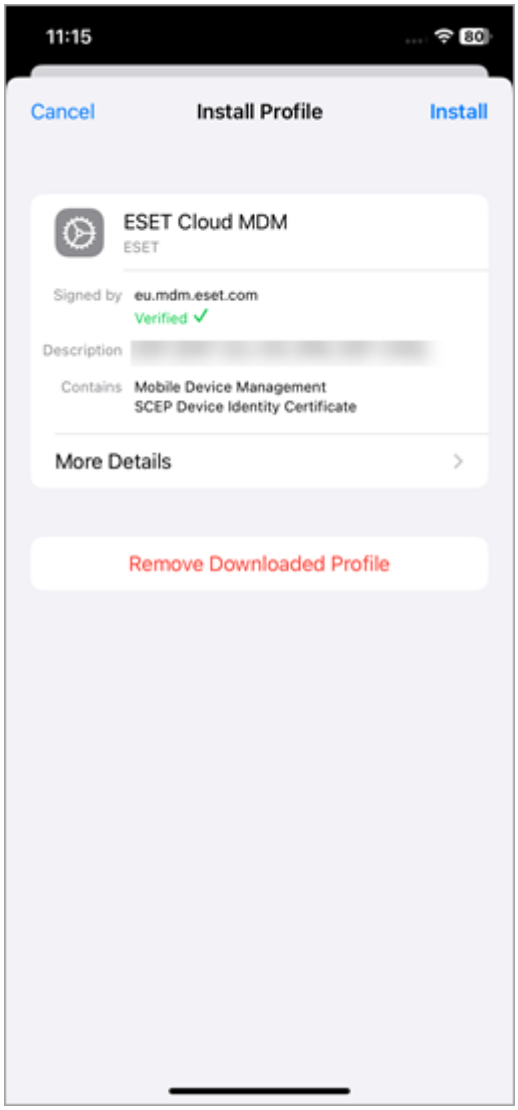
3. Pulse **Cerrar**.



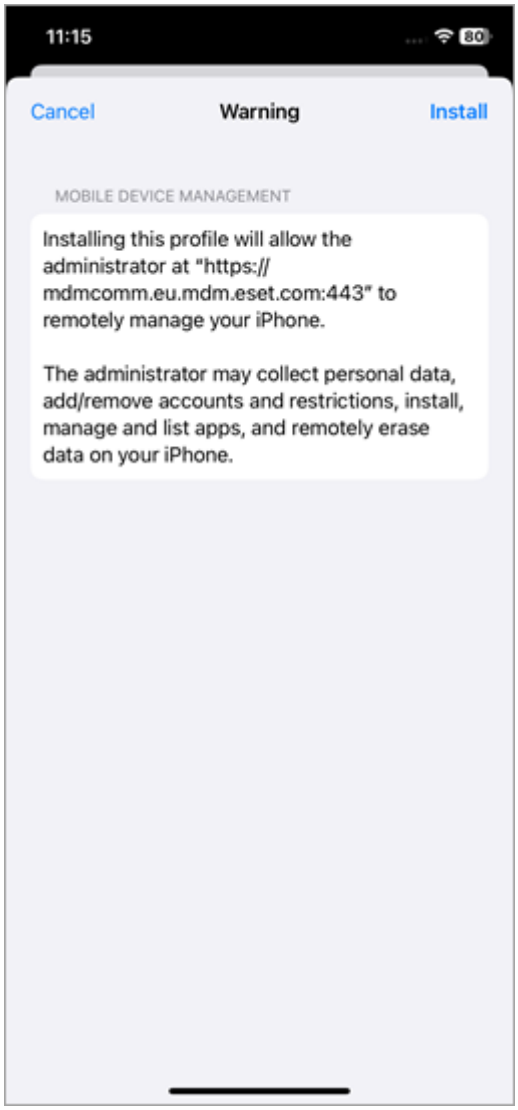
4. Abra la aplicación **Ajustes** y pulse **Perfil descargado**.



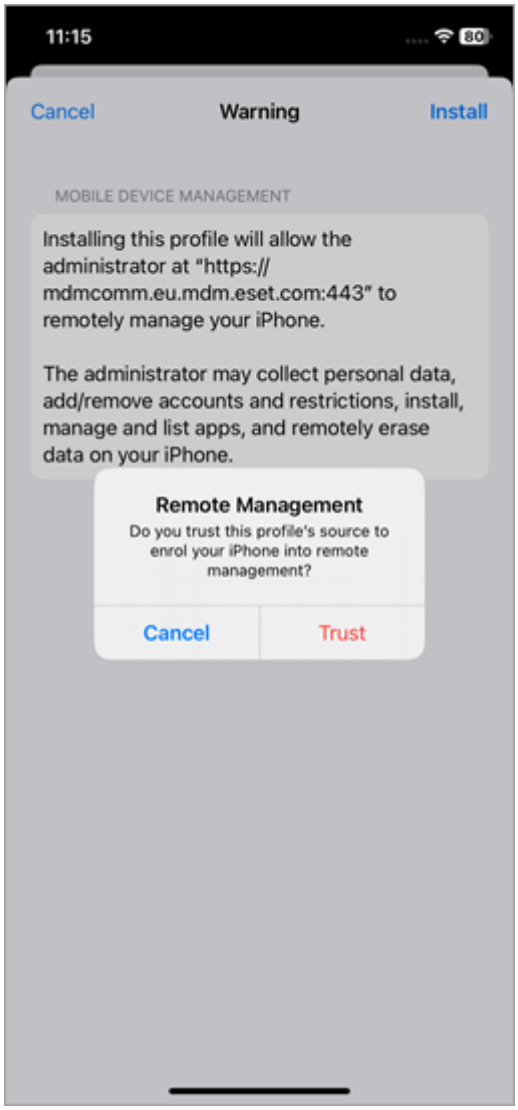
5. Pulse **Instalar** para instalar el perfil de ESET Cloud MDM.



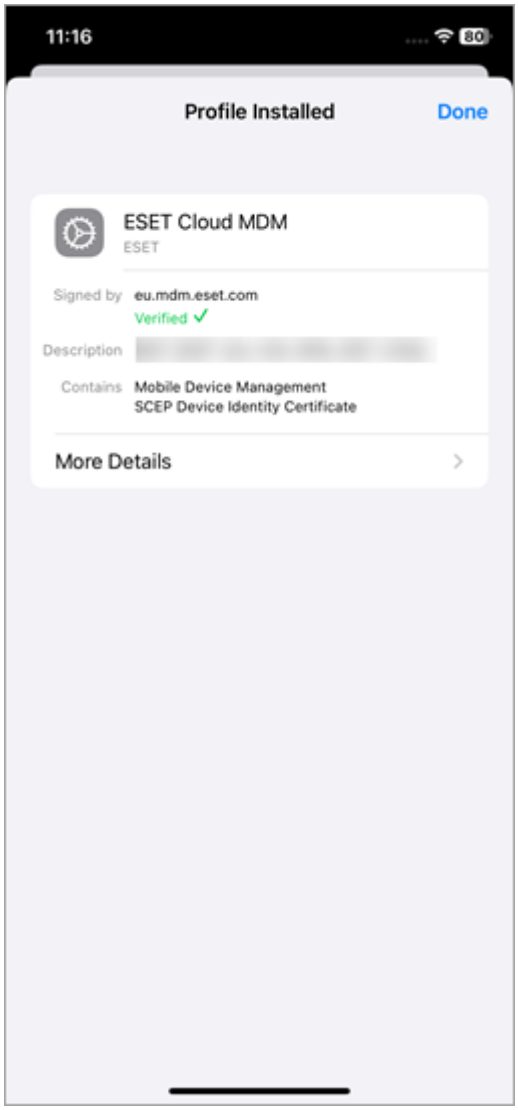
6. Pulse **Instalar**.



7. Pulse **Confiar** para instalar el perfil nuevo.



8. Pulse **Listo**.

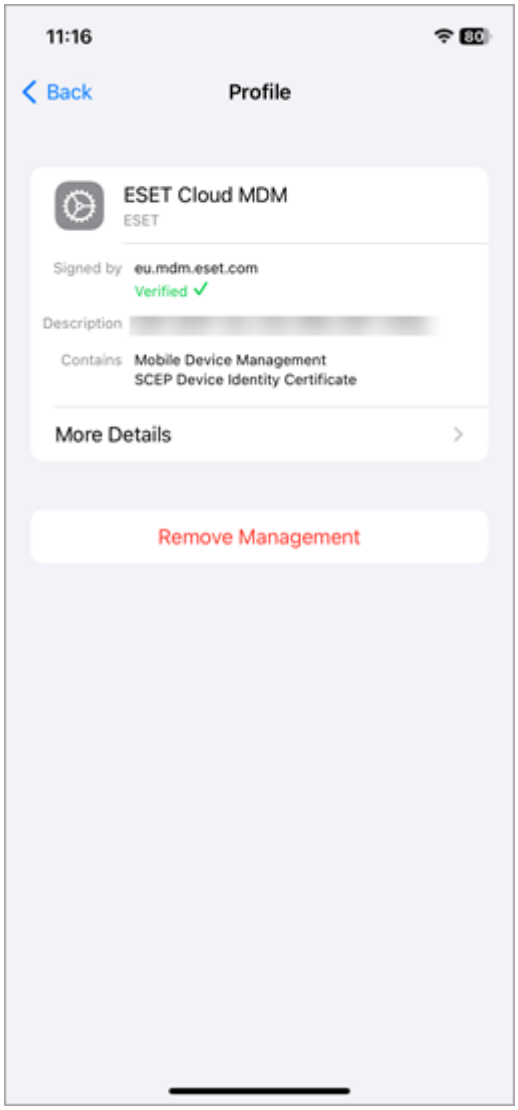


Ahora, ESET PROTECT se encarga de administrar el dispositivo móvil. Este perfil de inscripción le permite configurar dispositivos y establecer políticas de seguridad para usuarios o grupos. Los detalles del perfil están en la aplicación **Ajustes** > **General** > **VPN y gestión de dispositivos**.

Quitar el perfil de inscripción

Para quitar el perfil de inscripción, abra la aplicación **Ajustes** > **General** > **VPN y gestión de dispositivos** y pulse **Quitar administración**.

Al quitar el perfil de inscripción se quitan todos los ajustes de la empresa (Correo, Calendario, Contactos, etc.) y el dispositivo móvil iOS se suprime de la infraestructura de administración. El dispositivo deja de conectarse a ESET PROTECT y el estado del dispositivo cambia a una señal de advertencia y, después de 14 días, a una alerta roja.



Inscripción con Microsoft Entra ID (Android o iOS)

Puede verificar un usuario de Microsoft Entra ID (antes Azure Active Directory) para inscribir dispositivos móviles Android o iOS en ESET PROTECT.

Necesita una cuenta de usuario de Microsoft Entra ID para este tipo de inscripción de dispositivos móviles. Puede inscribir todos los dispositivos móviles a través de un enlace.

1. En ESET PROTECT Web Console, haga clic en **Más** > **Configuración** > **Inscripción con Microsoft Entra ID**.

2. Haga clic en **Obtener token** para obtener un token de autorización.

3. Inicie sesión con su cuenta de Microsoft Entra ID y acepte el permiso solicitado.

4. En **Usuarios permitidos**, seleccione los usuarios de Microsoft Entra ID que pueden inscribir dispositivos móviles:

   • **Todos los usuarios**: todos los usuarios de Microsoft Entra ID pueden inscribir.

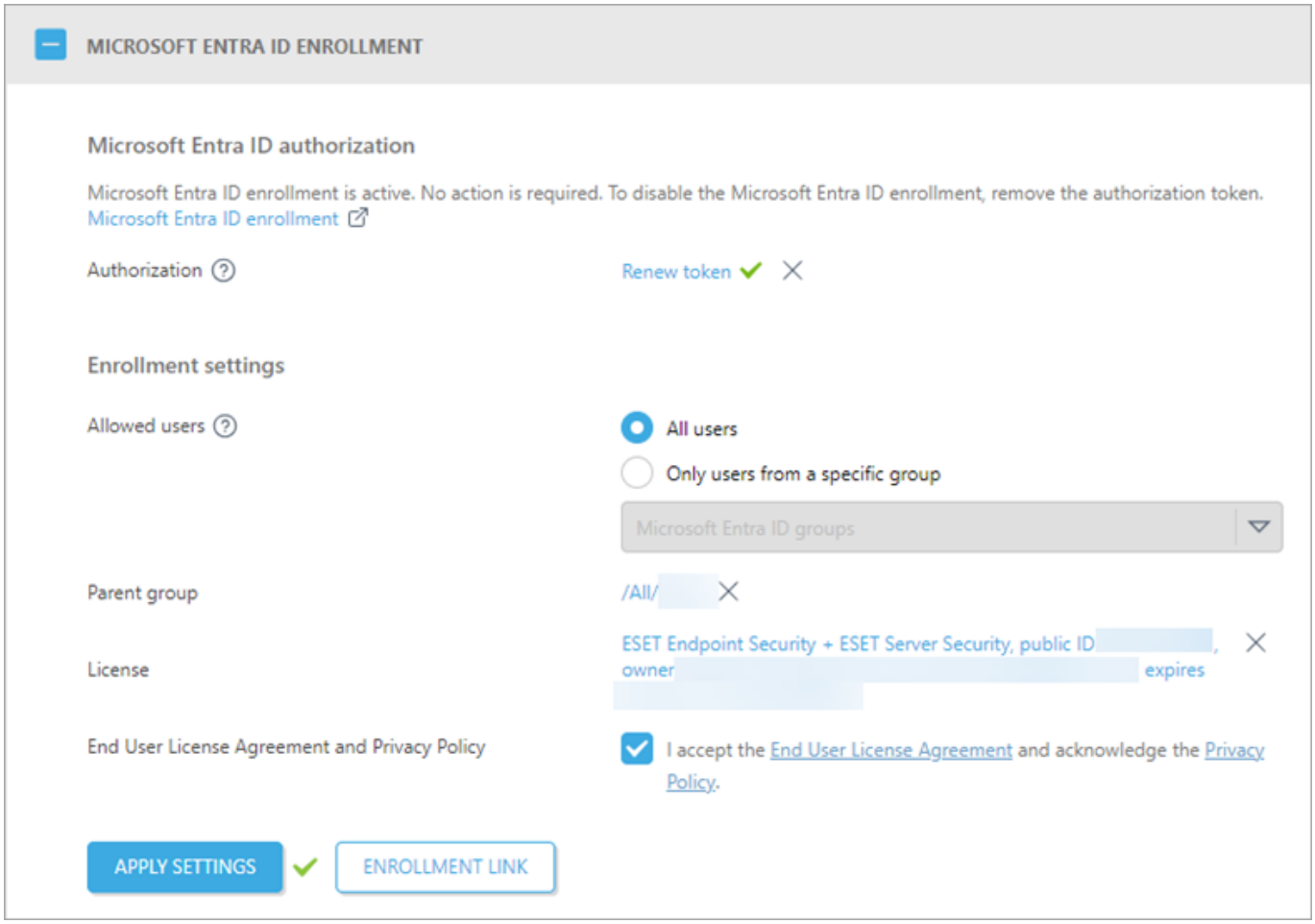
   • **Solo usuarios de un grupo específico**: seleccione un grupo de Microsoft Entra ID desde el que los usuarios puedan inscribir.

5. Seleccione el **Grupo principal** al que pertenecerán los dispositivos móviles inscritos tras la inscripción.

6. Seleccione la **Licencia** para activar los dispositivos móviles inscritos.

7. 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.

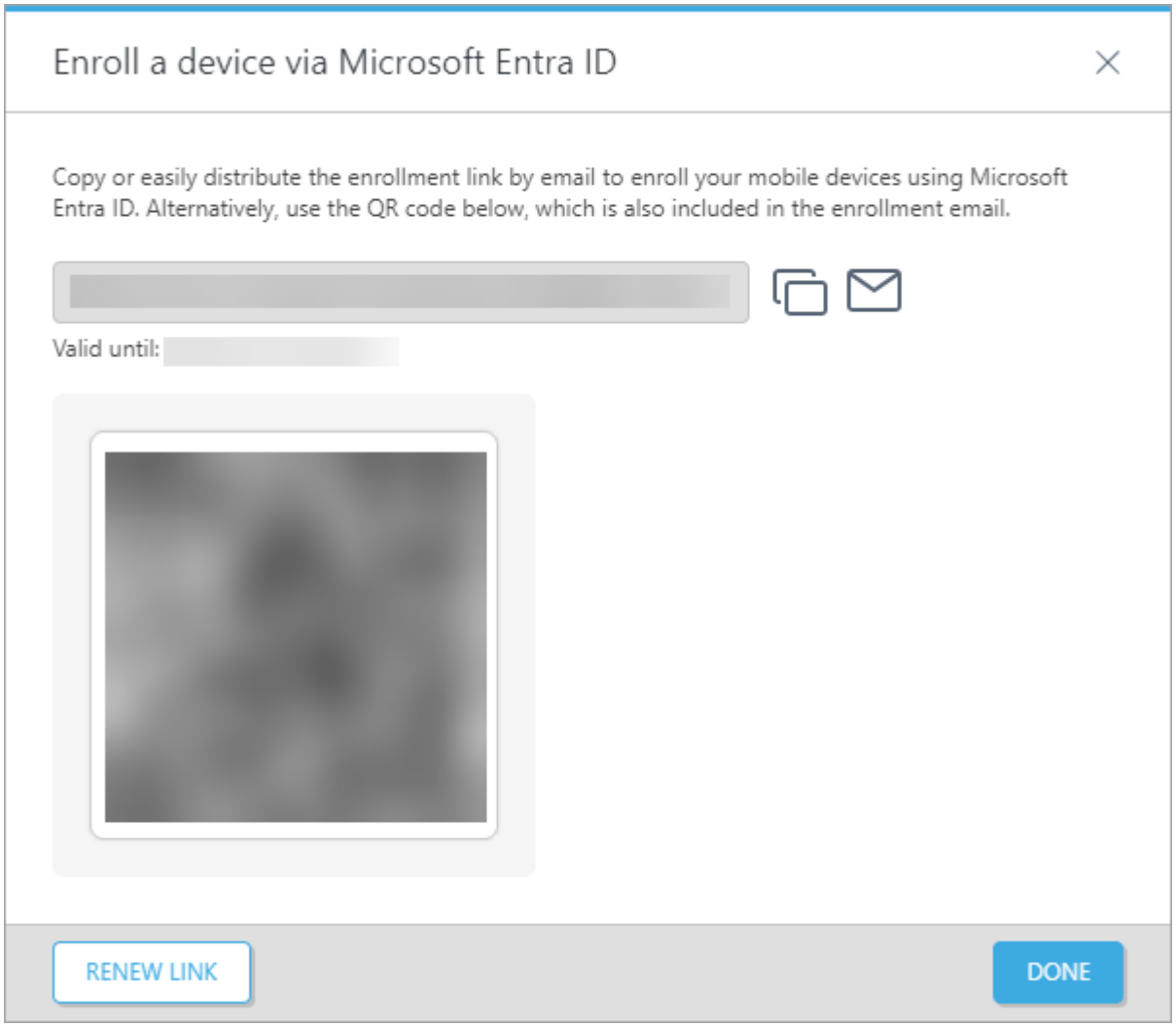
8. Haga clic en **Aplicar configuración** para guardar y aplicar todos los parámetros de inscripción seleccionados. Sus dispositivos móviles de Microsoft Entra ID aparecerán en ESET PROTECT Web Console en **Ordenadores** con los mismos nombres de dispositivo. Puede cambiar el nombre de un dispositivo en los detalles del dispositivo.



9. Haga clic en **Vínculo de inscripción** para mostrar un vínculo de inscripción:

- Puede copiar el vínculo, escanearlo mediante un código QR o enviarlo por correo electrónico. Hay un vínculo de inscripción que no es específico del usuario.

- El vínculo de inscripción es válido durante un año. Haga clic en **Renovar vínculo** para renovar el vínculo de inscripción.



10. Abra el vínculo de inscripción en un dispositivo móvil, inicie sesión en su cuenta de Microsoft Entra ID y acepte el permiso solicitado. A continuación, siga los pasos de inscripción para Android o iOS.

Para inscribir dispositivos Android con opciones de entrada limitadas:
1.Abra el vínculo de inscripción en un navegador web de un ordenador.
2.Inserte el código de seguridad generado en la aplicación ESET Endpoint Security para Android en el dispositivo móvil que desea inscribir.
3.Complete la inscripción.

11. Ahora puede administrar los dispositivos móviles de Microsoft Entra ID en ESET PROTECT.

Todos los dispositivos móviles de Microsoft Entra ID están en grupos dinámicos específicos: **Inscripción de Microsoft Entra ID** (dispositivos Android dispositivos) y **Dispositivos Microsoft Entra ID** (dispositivos iOS).

Sincronización con Microsoft Intune (Android)

Si utiliza Microsoft Intune, puede sincronizar su cuenta de Microsoft Intune con ESET PROTECT para administrar sus dispositivos Microsoft Intune Android con ESET PROTECT.

Requisitos previos

- Prepare su Microsoft Intune para la inscripción de Android.
- Conecte Microsoft Intune con su cuenta de Google Play administrado.
- Inscriba dispositivos como Android Enterprise.
- Migre los dispositivos inscritos como **administrador de dispositivos Android** antes de la inscripción.

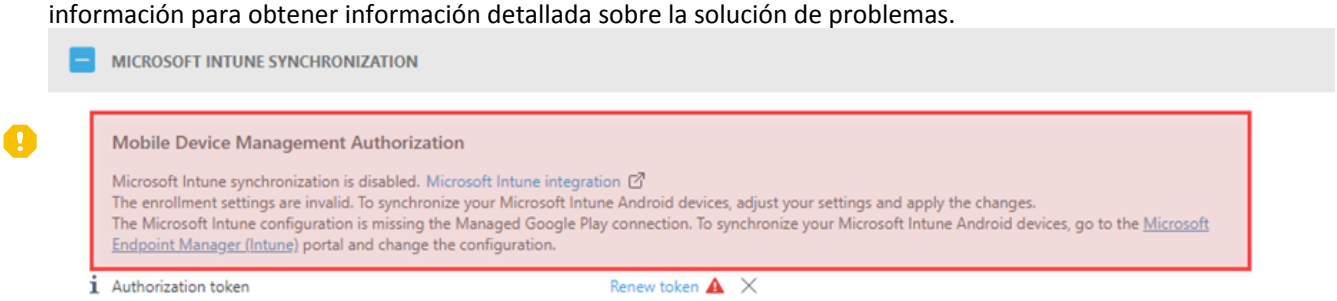
1. En ESET PROTECT Web Console, haga clic en **Más** > **Configuración** > **Sincronización con Microsoft Intune**.

2. Haga clic en **Obtener token**.

3. Inicie sesión con su cuenta de Microsoft Intune.

4. Tras iniciar sesión correctamente, debe utilizar **Solicitud de permisos** para ESET PROTECT. Revise la información proporcionada y haga clic en **Aceptar** para continuar y agregar un token de autenticación válido a la instancia de ESET PROTECT.

Si tiene algún problema con el proceso de importación del token de autorización, consulte el cuadro de información para obtener información detallada sobre la solución de problemas.



5. En **Configuración de inscripción**, seleccione uno de los métodos de inscripción:

- **Inscribir todos los dispositivos Android**: todos los dispositivos Android de Microsoft Intune se inscribirán automáticamente en su ESET PROTECT.
- **Inscribir dispositivos Android para todos los usuarios**: inscriba solo los dispositivos Android con el usuario asignado en Microsoft Intune en su ESET PROTECT.
- **Inscribir dispositivos Android de grupos Microsoft Intune**: inscriba solo los dispositivos Android que formen parte de los grupos de Microsoft Intune seleccionados en su ESET PROTECT.

6. Seleccione la **Licencia** utilizada para activar los dispositivos Android inscritos.

7. Seleccione el **Grupo principal** al que pertenecerán los dispositivos Android inscritos tras la inscripción.

8. **Notificaciones** (habilitadas de forma predeterminada): envíe notificaciones automáticamente a cada dispositivo cuando la protección no se haya activado. Las notificaciones informan a los usuarios de que la protección está instalada en sus dispositivos, y deben activarla abriendo la aplicación ESET Endpoint Security desde su perfil de trabajo. El dispositivo puede recibir hasta tres notificaciones: cinco días, siete días y nueve días después de la inscripción. Haga clic en **Personalizar** para personalizar el mensaje de la notificación.

9. **Aplicar configuración de inscripción** para guardar y aplicar todos los parámetros de inscripción seleccionados.

Los dispositivos Microsoft Intune ya están disponibles para la administración en ESET PROTECT y Microsoft Intune.

Cuando inscribe un dispositivo con Android 9 o posteriores mediante Microsoft Intune o VMware Workspace ONE, ESET Endpoint Security para Android versión 3.5 y posteriores ignora los siguientes ajustes de la política:

- Seguridad del dispositivo
- Control de aplicaciones
- Antirrobo

Sincronización con VMware Workspace ONE (Android)

Si administra dispositivos Android con VMware Workspace ONE (consulte Cómo registrar Android con VMware Workspace ONE), puede sincronizar su cuenta de VMware Workspace ONE con ESET PROTECT para proteger los dispositivos Android VMware Workspace ONE. Siga los pasos indicados a continuación para configurar la sincronización:

I. Activación del acceso a la API de REST en VMware Workspace ONE

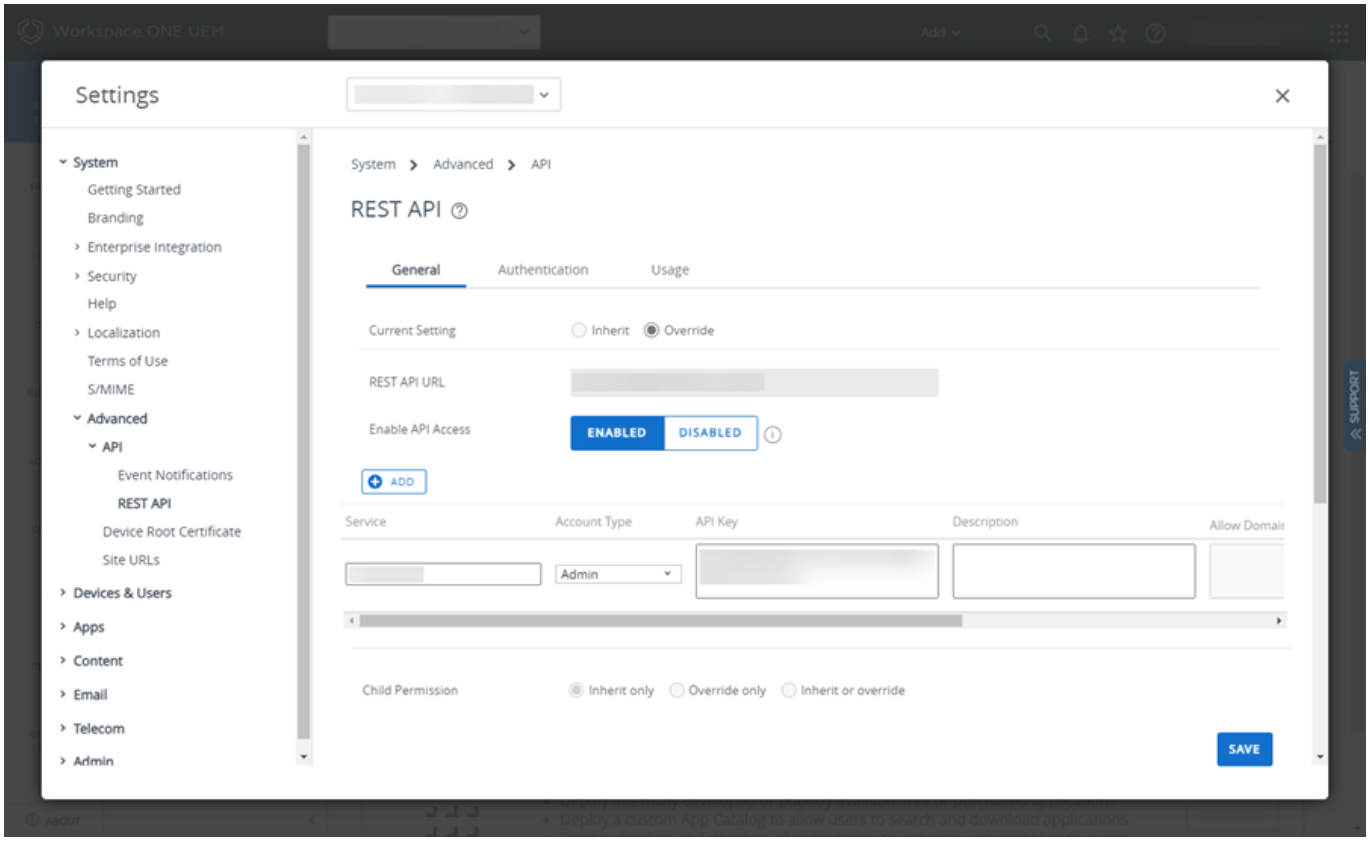
II. Creación de un cliente OAuth en VMware Workspace ONE

III. Sincronización ESET PROTECT con VMware Workspace ONE

I. Activación del acceso a la API de REST en VMware Workspace ONE

1. Inicie sesión en la VMware Workspace ONE:
2. Haga clic en **Introducción** > **Configuración**.
3. Haga clic en **Avanzado** > **API** > **API de REST**.
4. Copie el valor de **URL de API de REST**.
5. Seleccione **Activado** junto a **Activar acceso a la API**.
6. Haga clic en **Agregar**, escriba el nombre en **Servicio** y copie el valor de **Clave de la API**.
7. Haga clic en **Guardar**.

Obtenga más información sobre la API de REST para VMware Workspace ONE.



II. Creación de un cliente OAuth en VMware Workspace ONE

1. Haga clic en **Grupos y ajustes** > **Configuraciones**.
2. Escriba **OAuth** en el cuadro de búsqueda **Introducir un nombre o una categoría**.
3. Haga clic en **Administración de clientes OAuth**.
4. Haga clic en **Agregar**.
5. En la ventana **Registrar un nuevo cliente**:

   a.Escriba los valores de **Nombre**, **Descripción** y **Grupo de organización**.

   b.Seleccione el ajuste de **Administrador de la consola** en el menú desplegable **Rol**.

   c.Asegúrese de que el valor de **Estado** sea **Activado**.

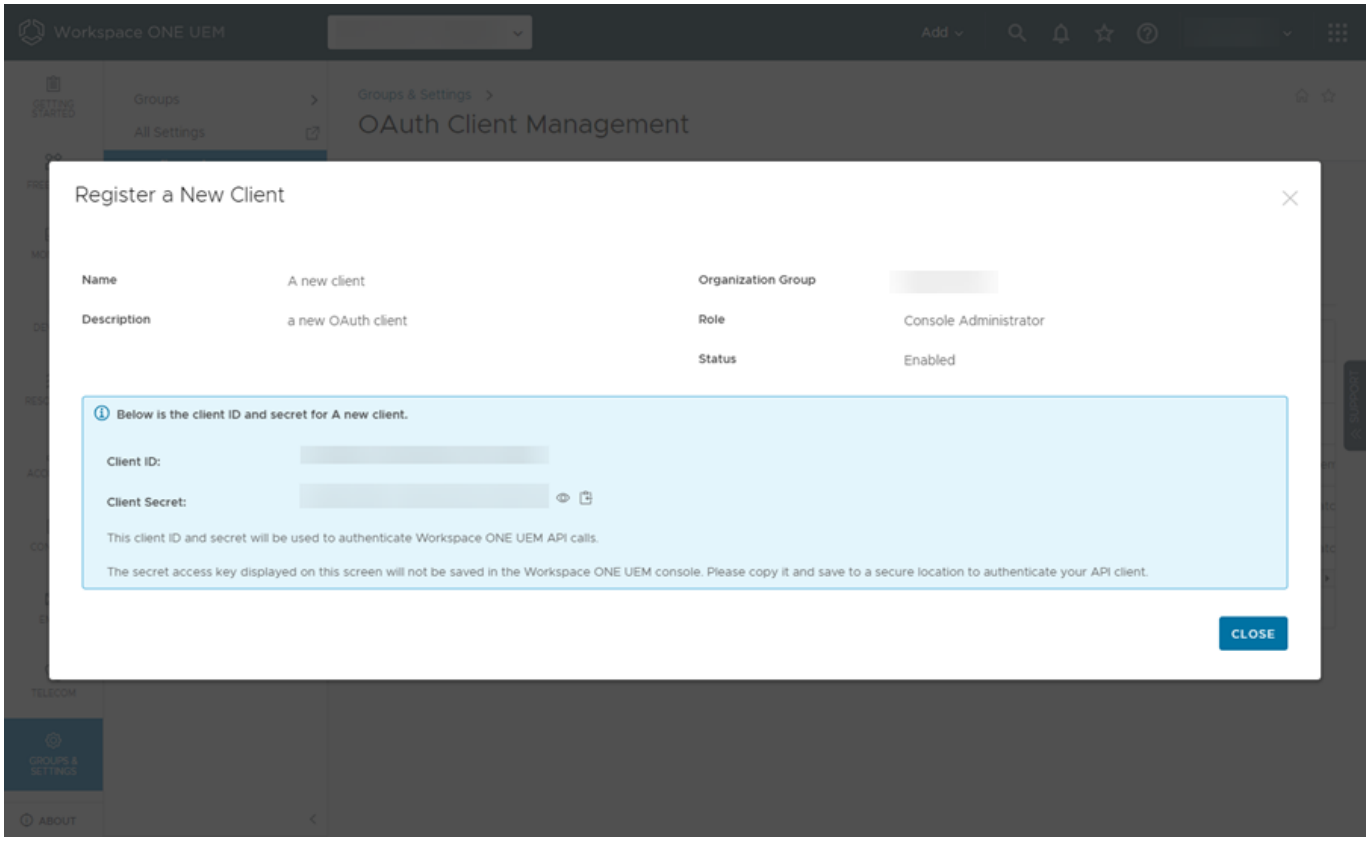
   d.Haga clic en **Guardar**.

6. Copie el valor de **ID del cliente** y **Secreto del cliente**.

> Asegúrese de haber copiado y guardado los valores de **ID del cliente** y **Secreto del cliente** antes de cerrar la ventana. No puede recuperar los valores de **ID del cliente** ni de **Secreto del cliente** después de hacer clic en **Cerrar**.

7. Haga clic en **Cerrar**.

Obtenga más información sobre la administración de clientes OAuth en la documentación de VMware Workspace ONE.



III. Sincronización ESET PROTECT con VMware Workspace ONE

1. En la Consola Web de ESET PROTECT, haga clic en **Más** > **Configuración**.

2. Expanda **Sincronización con VMware Workspace ONE**.

3. Haga clic en **Configurar** junto a **Autorización**.

4. Escriba o pegue la configuración de autorización necesaria:

   a.**URL de API de REST**: escriba o pegue el vínculo que copió en el paso 4 de la sección I anterior.

   b.**Clave de API de REST**: escriba o pegue el valor de **Clave de la API** que copió en el paso 6 de la sección I anterior.

   c.**ID del cliente OAuth**: escriba o pegue el valor de **ID del cliente** que copió en el paso 6 de la sección II anterior.

   d.**Secreto del cliente OAuth**: escriba o pegue el valor de **Secreto del cliente** que copió en el paso 6 de la sección II anterior.

5. Haga clic en **Configurar**. Cuando la configuración de autorización sea correcta, verá **Actualización** ✔ con una marca de verificación verde junto a **Autorización**.

6. En **Asignaciones**, seleccione los dispositivos Android que desea sincronizar:

a.**Inscribir todos los dispositivos Android**: sincronice todos los dispositivos Android desde su VMware Workspace ONE.

> La opción **Inscribir todos los dispositivos Android** crea el grupo inteligente de VMware Workspace ONE **Todos los dispositivos Android protegidos por ESET**. **Asignación de protección de ESET** instalará ESET Endpoint Security para Android en los dispositivos móviles del grupo. Si más adelante selecciona la opción **Inscribir solo dispositivos Android de un grupo específico**, se eliminará el grupo inteligente **Todos los dispositivos Android protegidos por ESET**.

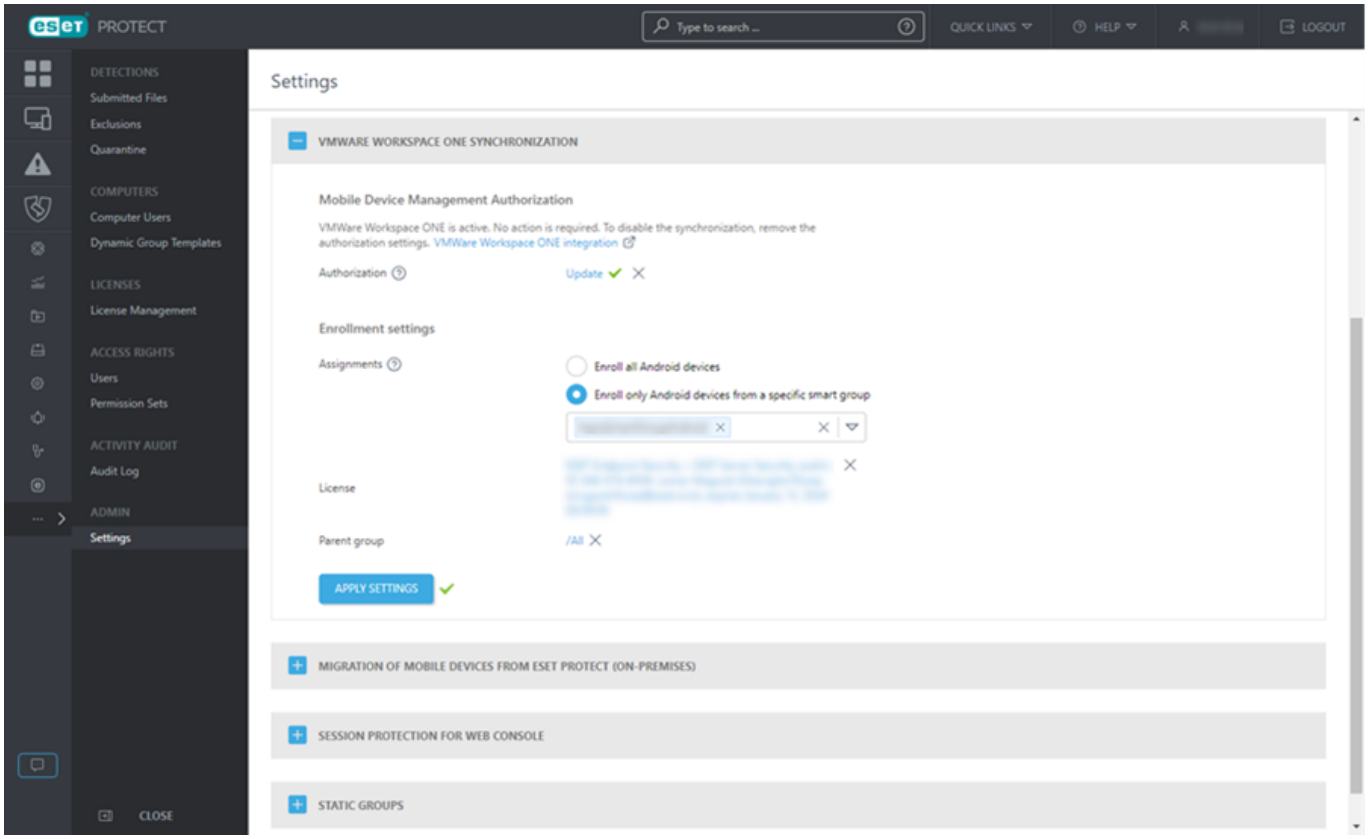
b.**Inscribir solo dispositivos Android de un grupo inteligente específico**: sincronice los dispositivos Android de los grupos inteligentes de VMware Workspace ONE seleccionados en el menú desplegable.

7. **Licencia**: la licencia adecuada está preseleccionada. Puede seleccionar otra licencia. La licencia activará ESET Endpoint Security para Android durante la instalación.

8. **Grupo principal**: seleccione el grupo principal de ESET PROTECT en el que se sincronizarán los dispositivos Android.

9. **Notificaciones** (habilitadas de forma predeterminada): envíe notificaciones automáticamente a cada dispositivo cuando la protección no se haya activado. Las notificaciones informan a los usuarios de que la protección está instalada en sus dispositivos, y deben activarla abriendo la aplicación ESET Endpoint Security desde su perfil de trabajo o pulsando el vínculo de la notificación. El dispositivo puede recibir hasta tres notificaciones: cinco días, siete días y nueve días después de la inscripción. Haga clic en **Personalizar** para personalizar el mensaje de la notificación.

10. Haga clic en **Aplicar configuración**.



Los dispositivos Android de su VMware Workspace ONE aparecerán en la sección Ordenadores debajo del grupo principal seleccionado, y puede administrar el ESET Endpoint Security para Android instalado mediante una política.

Cuando inscribe un dispositivo con Android 9 o posteriores mediante Microsoft Intune o VMware Workspace ONE, ESET Endpoint Security para Android versión 3.5 y posteriores ignora los siguientes ajustes de la política:

- Seguridad del dispositivo
- Control de aplicaciones
- Antirrobo

Sincronización de Apple Business Manager (ABM) (iOS)

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.

Antes de realizar la inscripción de ABM de iOS, debe activar la sincronización de ABM en ESET PROTECT Web Console. Para ello, diríjase a **Más** > **Configuración** > **Sincronización con Apple Business Manager (ABM)**.

Sincronizar su ESET PROTECT MDM con el servidor de Apple ABM:

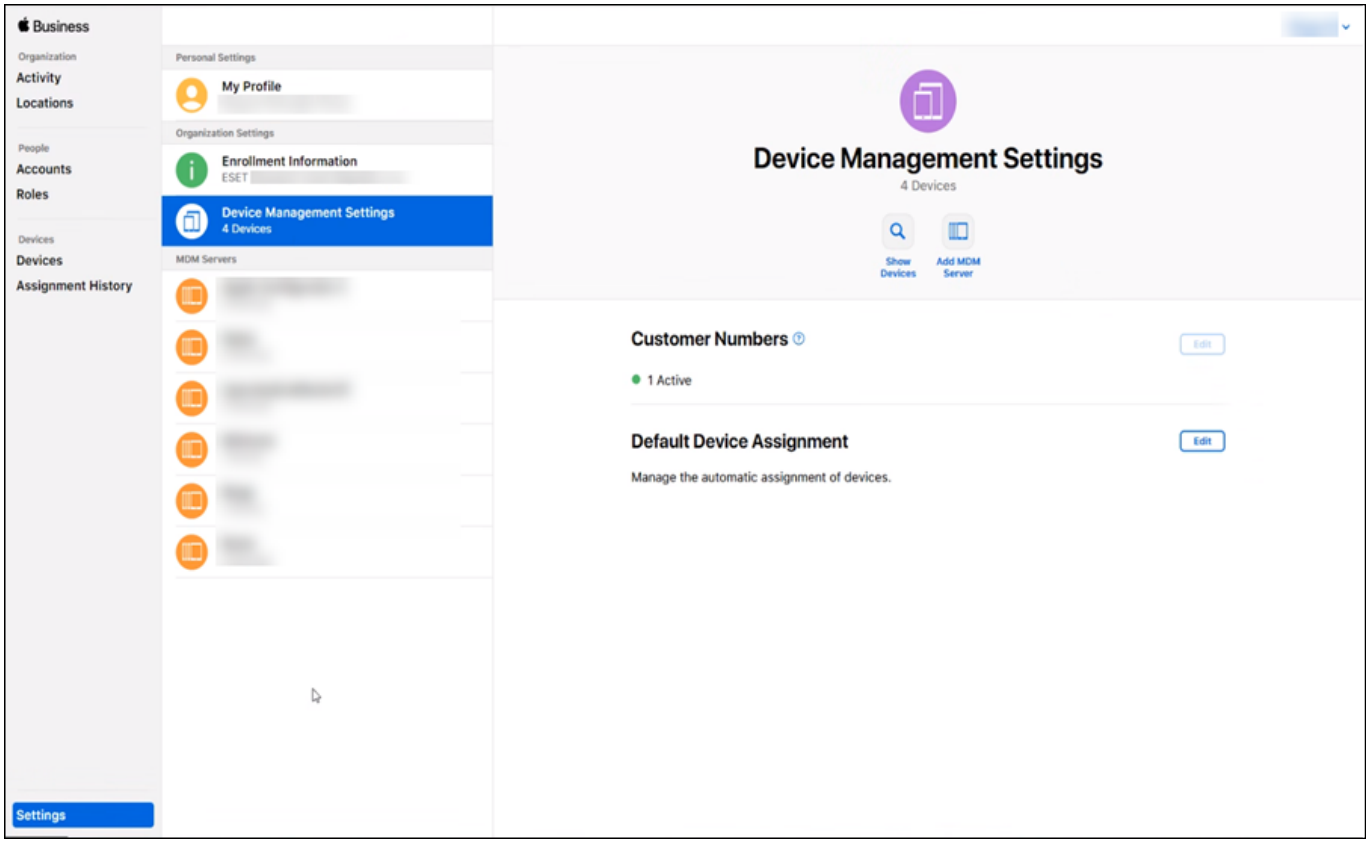
1. Compruebe que se cumplan todos los requisitos de ABM de Apple, tanto los requisitos de la cuenta como los requisitos del dispositivo.

Cuenta de ABM:

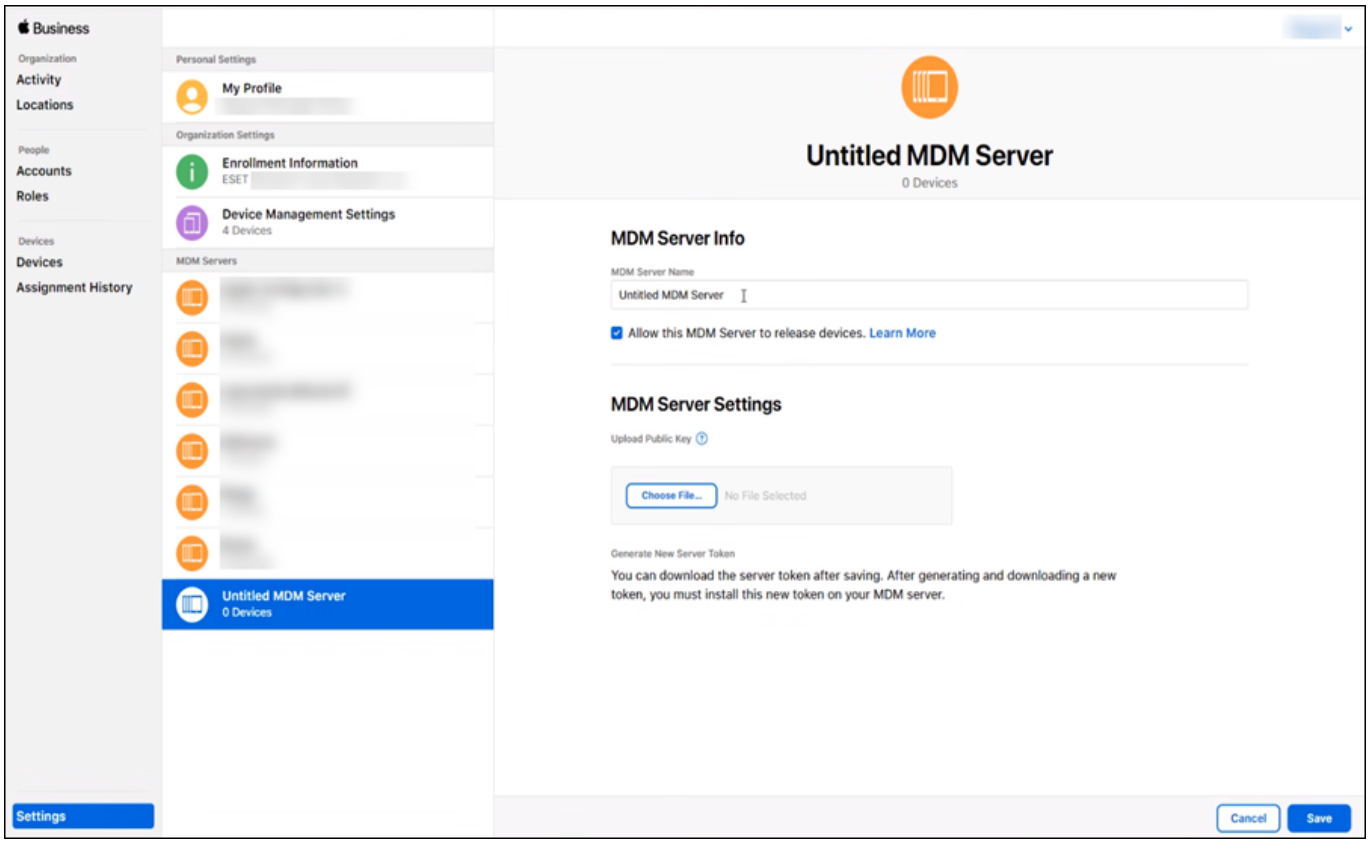
- El programa solo está disponible en determinados países. Visite la Página web de Apple ABM para ver si ABM está disponible en su país.
- Los requisitos de la cuenta de Apple ABM están disponibles en estos sitios web: Requisitos del Programa de implementación de Apple y Requisitos del Programa de inscripción 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).

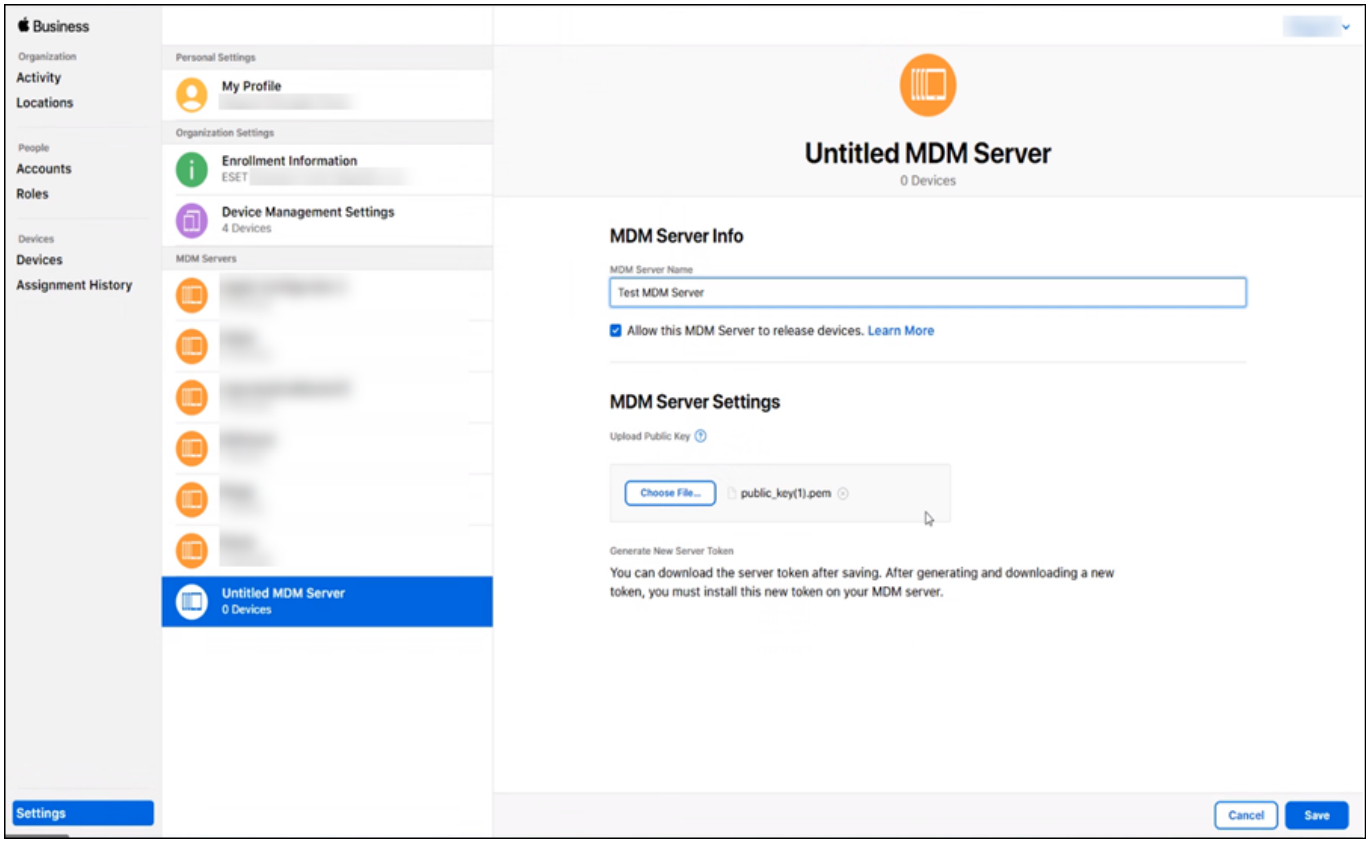
3. En la sección **Ajustes de gestión de dispositivos,** seleccione **Agregar servidor MDM**.



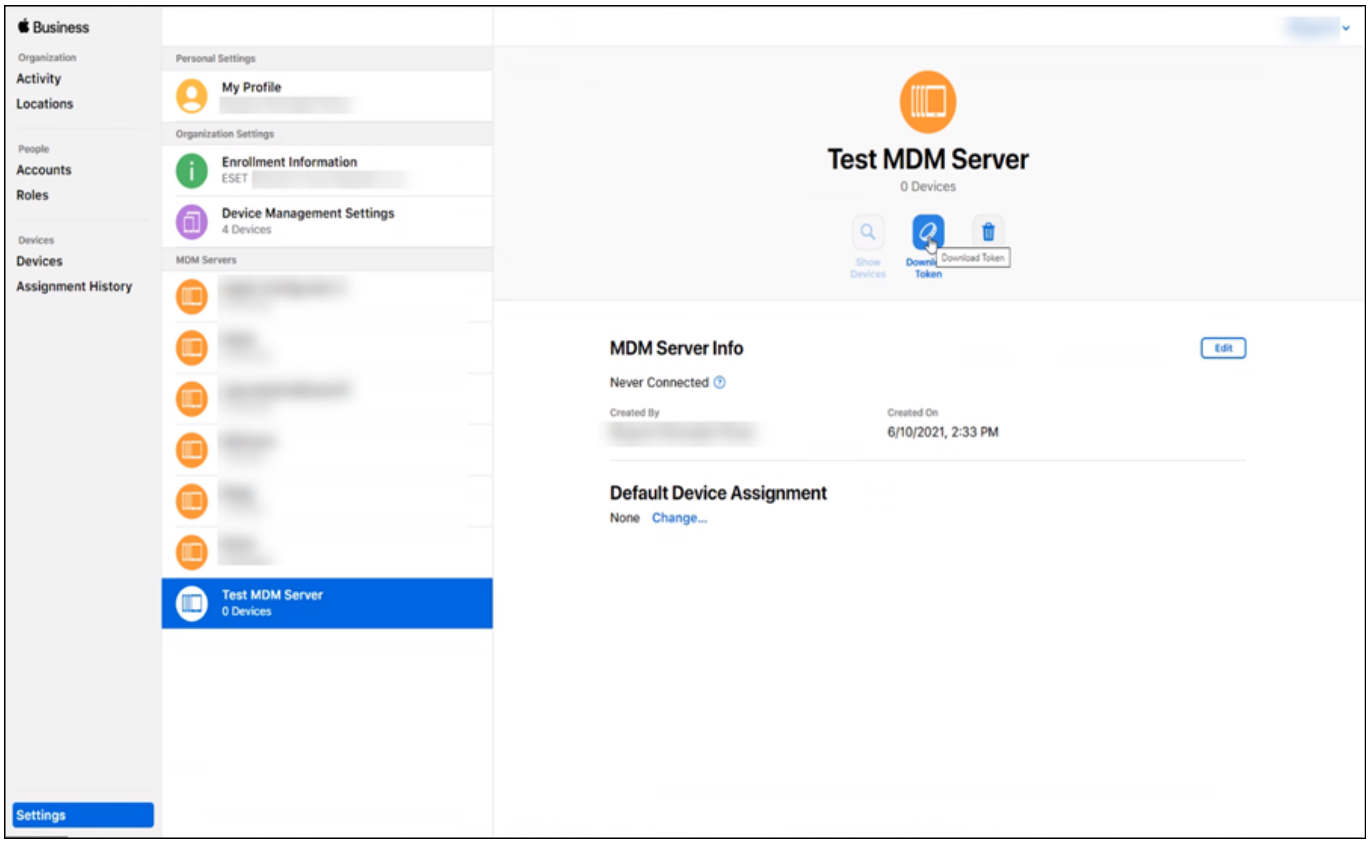
4. En la pantalla Servidor MDM sin título, escriba el **nombre del servidor MDM**, por ejemplo: "MDM_Server".



5. Cargue su clave pública en el portal de ABM. Haga clic en **Elegir archivo**, seleccione el archivo de clave pública (el archivo de clave pública que descarga de la pantalla de configuración de ABM en ESET PROTECT) y haga clic en **Guardar**.



6. Haga clic en **Descargar token** para descargar su token ABM de Apple. Este archivo se cargará en la configuración de ESET PROTECT, en el **token del servidor ABM** > **Cargar**.

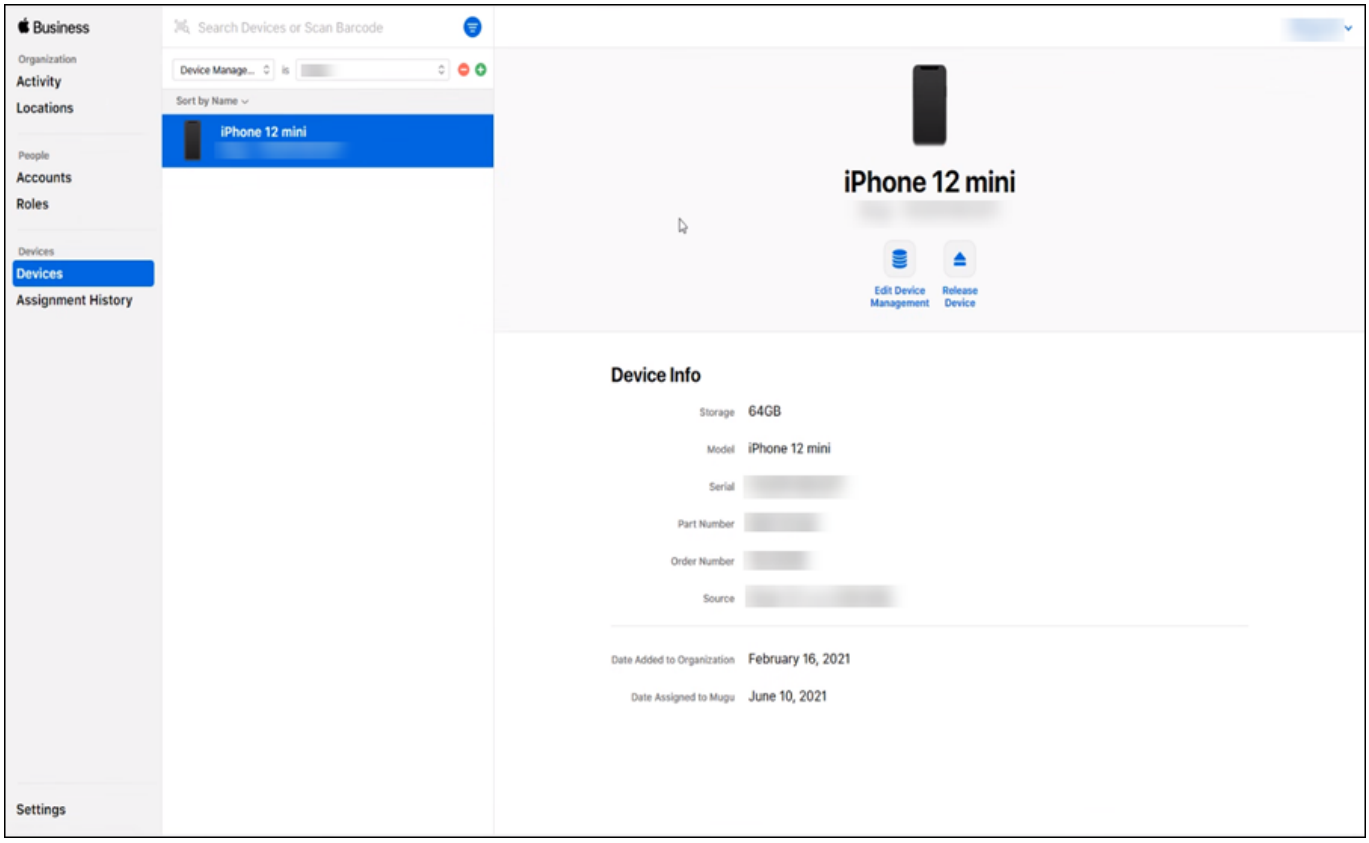


Agregue el dispositivo iOS al ABM de Apple

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.

El intervalo de sincronización de Cloud MDM está establecido en 30 minutos, por lo que tendrá que esperar este tiempo hasta que aparezca el dispositivo de Apple en ESET PROTECT.

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.

Administrar dispositivos móviles

Después de inscribir sus dispositivos móviles Android, puede comenzar a administrarlos.

De la administración de equipos estándar disponible para todos los dispositivos de equipos, la administración de dispositivos móviles ofrece varias características disponibles solo para la administración de dispositivos móviles.

Administración de dispositivos móviles a través de tareas del cliente

Acciones antirrobo (se aplica a dispositivos Android e iOS): estas tareas solo están disponibles para dispositivos móviles administrados, como Buscar, Bloquear y Restablecimiento de fábrica. Estas tareas permiten a los administradores localizar de forma remota el dispositivo móvil, bloquearlo y, si la situación lo requiere, borrar el dispositivo móvil.

Vea todas las tareas del cliente para dispositivos móviles.

> **Desencadenadores de tareas del cliente en dispositivo móvil**
> Solo puede usar estos desencadenadores para las tareas del cliente en dispositivo móvil:
> • Lo antes posible
> • Desencadenador de grupo dinámico unido
> Se producirá un error en las tareas del cliente con desencadenadores distintos de los anteriores, y se mostrará el mensaje **Tipo de desencadenador no admitido**.

Administración de dispositivos Android a través de políticas

Asigne la política **ESET Endpoint Security for Android**, donde puede personalizar cada una de las configuraciones de administración de Android disponibles. Por ejemplo:

- Control de acceso web
- Administración de actualizaciones del sistema operativo
- Instalación remota de aplicaciones: puede forzar de forma remota al dispositivo móvil a instalar las aplicaciones requeridas agregándolas a la lista en la política.

    1.Vaya a la política de **ESET Endpoint Security for Android** aplicada existente (o cree una nueva con esta finalidad).

    2.En **Control de aplicaciones**, active el botón de alternancia **Activar control de la aplicación**.

    3.Haga clic en **Lista de aplicaciones** y agregue las aplicaciones que desee instalar de forma remota en el dispositivo móvil después de aplicar la política.

Cuando inscribe un dispositivo con Android 9 o posteriores mediante Microsoft Intune o VMware Workspace ONE, ESET Endpoint Security para Android versión 3.5 y posteriores ignora los siguientes ajustes de la política:

- Seguridad del dispositivo
- Control de aplicaciones
- Antirrobo

Administración de dispositivos iOS a través de políticas

La administración de dispositivos iOS permite que la funcionalidad CloudMDM también inscriba y administre dispositivos iOS en ESET PROTECT en modo estándar o de inscripción ABM.

Asigne la política **ESET MDM para iOS/iPadOS**, donde puede personalizar cada uno de los ajustes de administración de iOS disponibles. Por ejemplo:

- Configurar la cuenta de Exchange ActiveSync
- Aplicar restricciones a iOS

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. 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.

Crear una directiva para el 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.

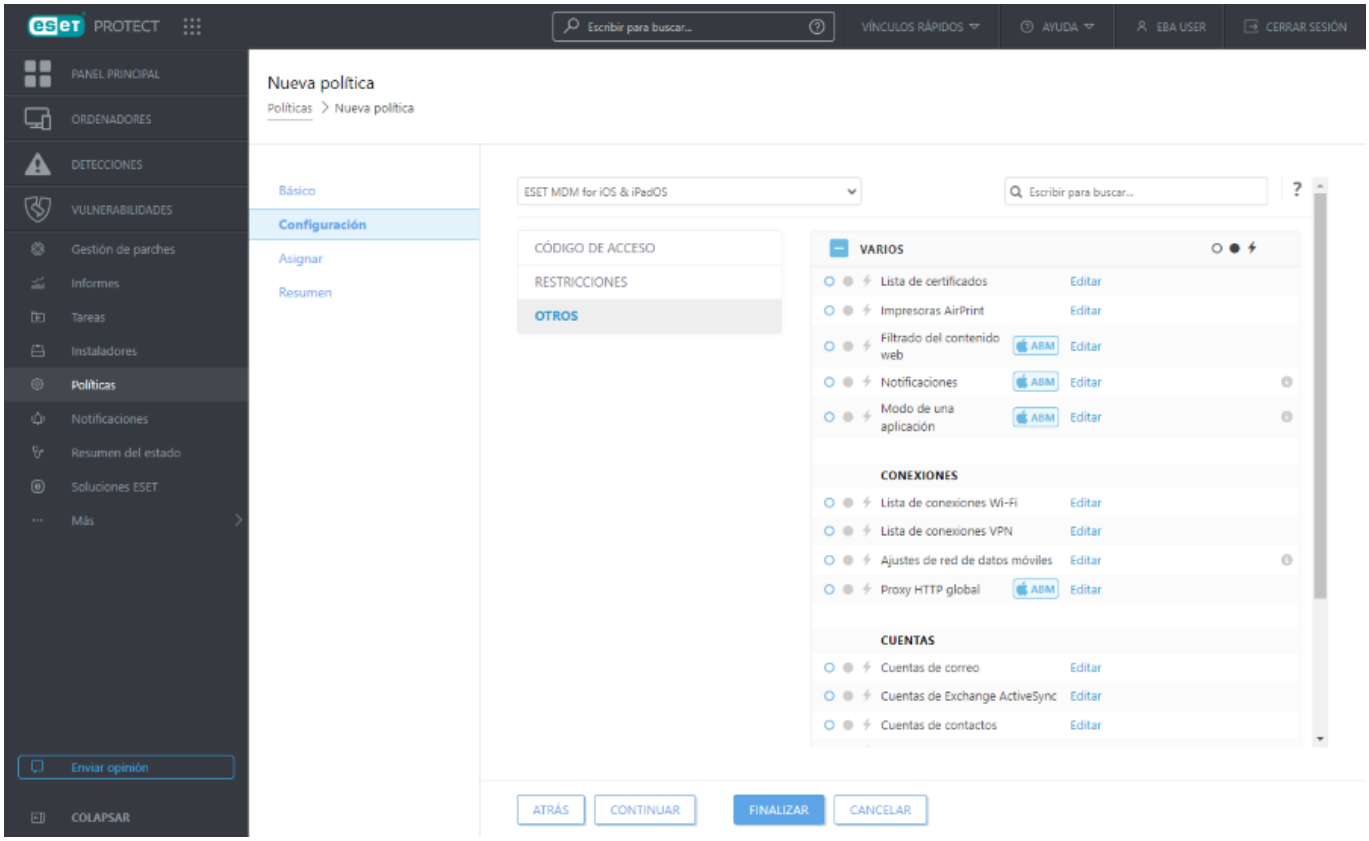
> Antes de comenzar a configurar esta política, asegúrese de haber realizado los pasos descritos en Inscripción de dispositivos móviles.

Básico

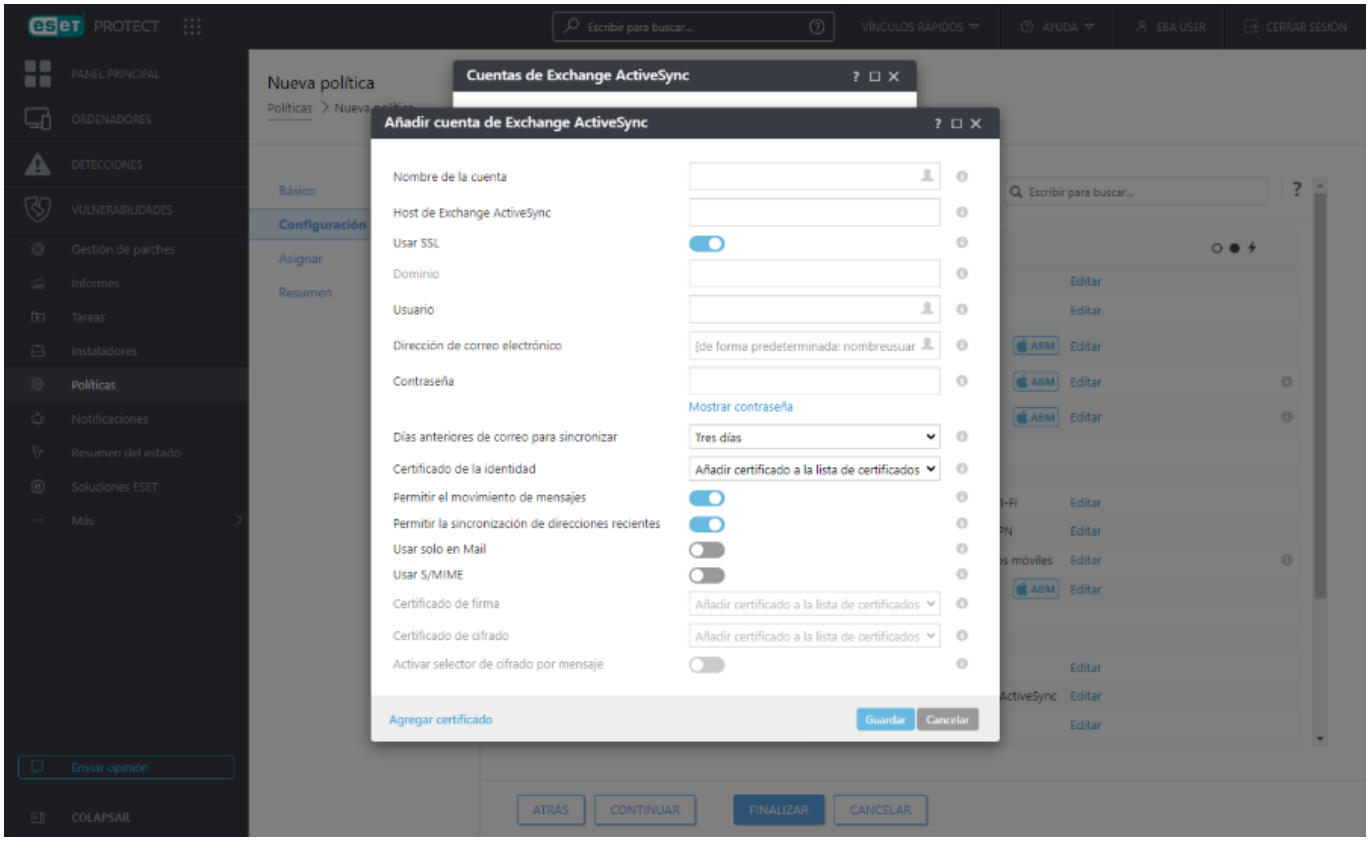
Escriba el **Nombre** de esta directiva. El campo **Descripción** es opcional.

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.

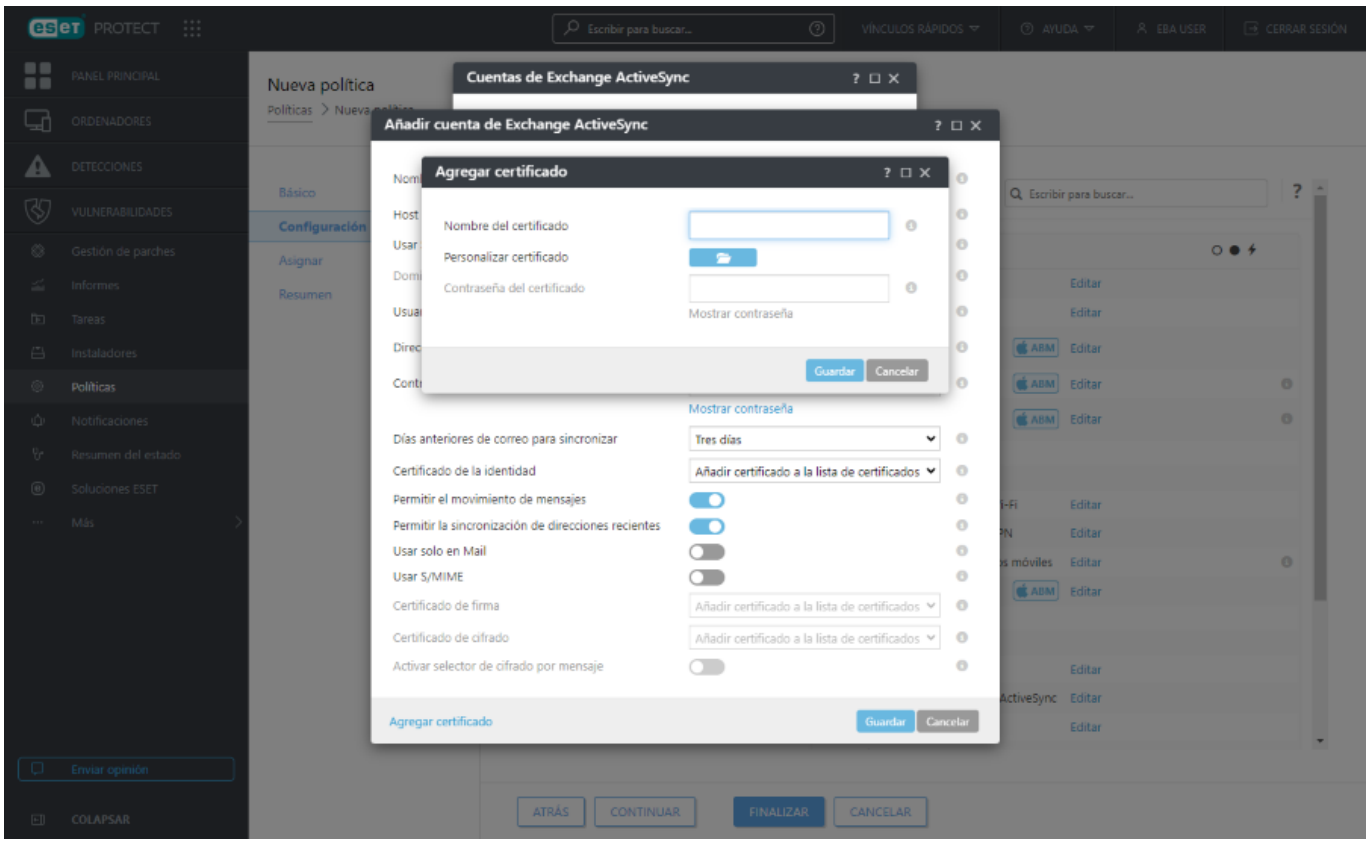
• **Usar S/MIME**: active esta opción para usar el cifrado S/MIME con los mensajes de correo electrónico salientes.

• **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**.

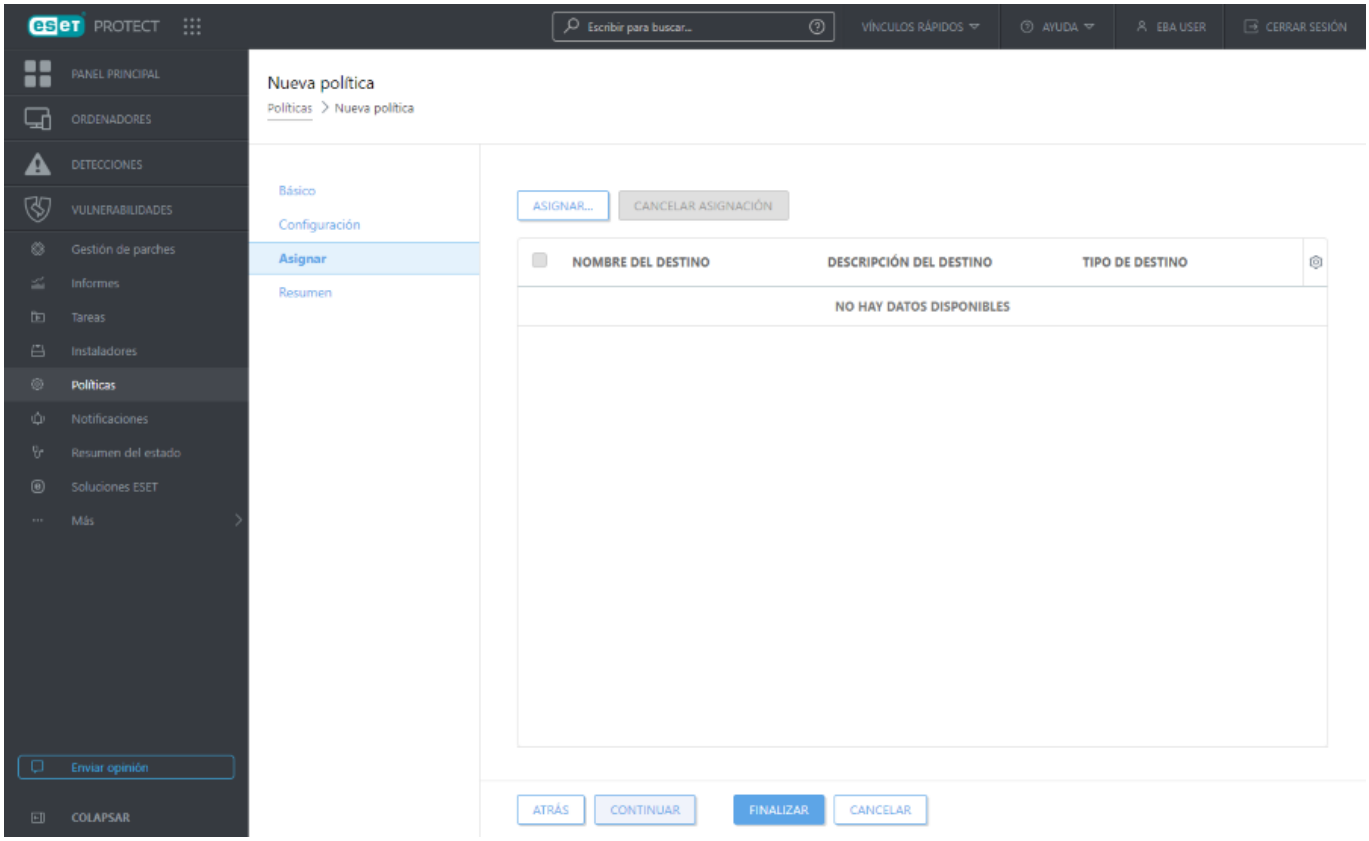


• **Agregar certificado**: puede añadir certificados de Exchange específicos (Identidad del usuario, Firma digital o Certificado de cifrado) en caso de ser necesario.

> 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.

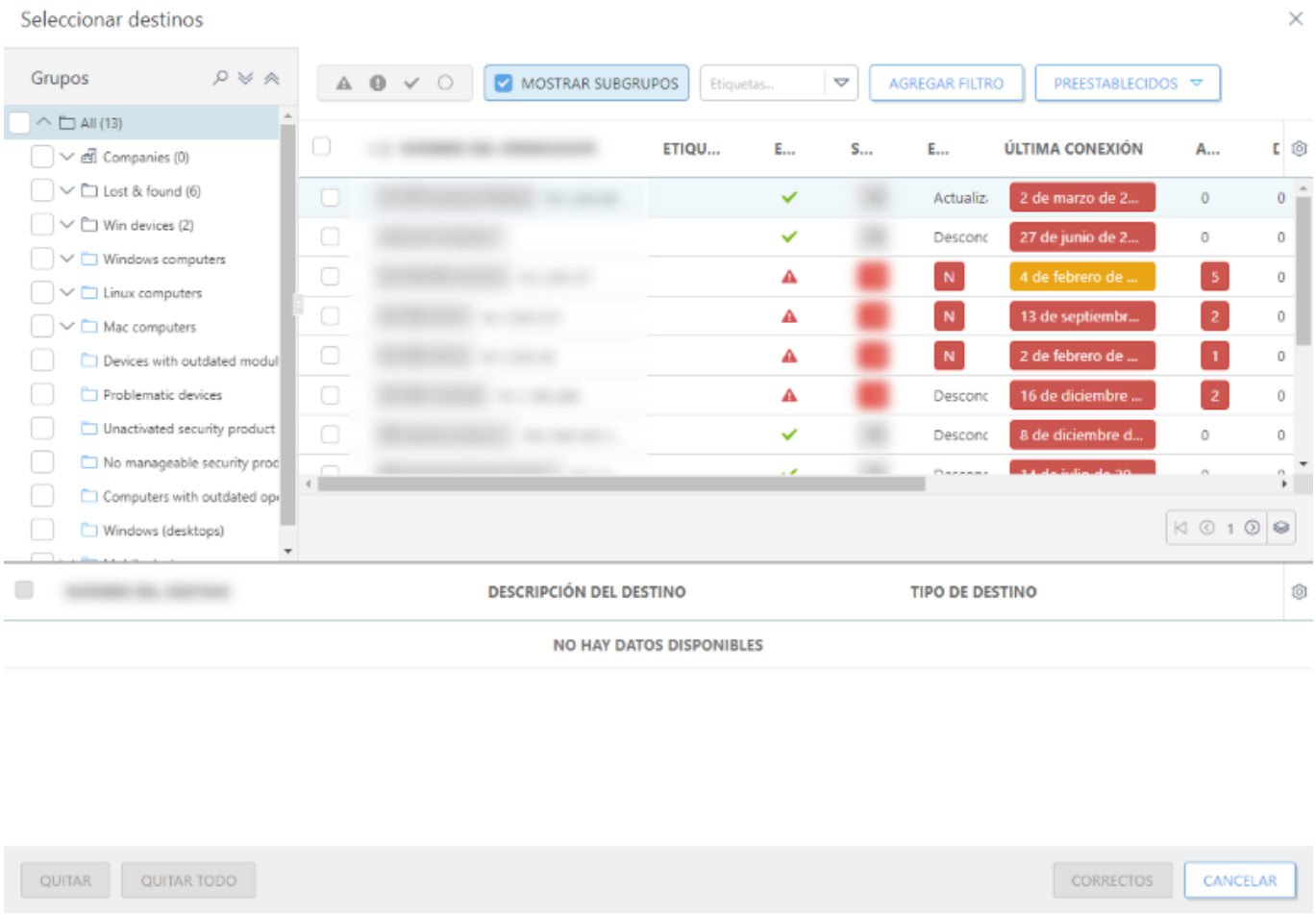
Asignar

Especifique los clientes (ordenadores individuales 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.

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

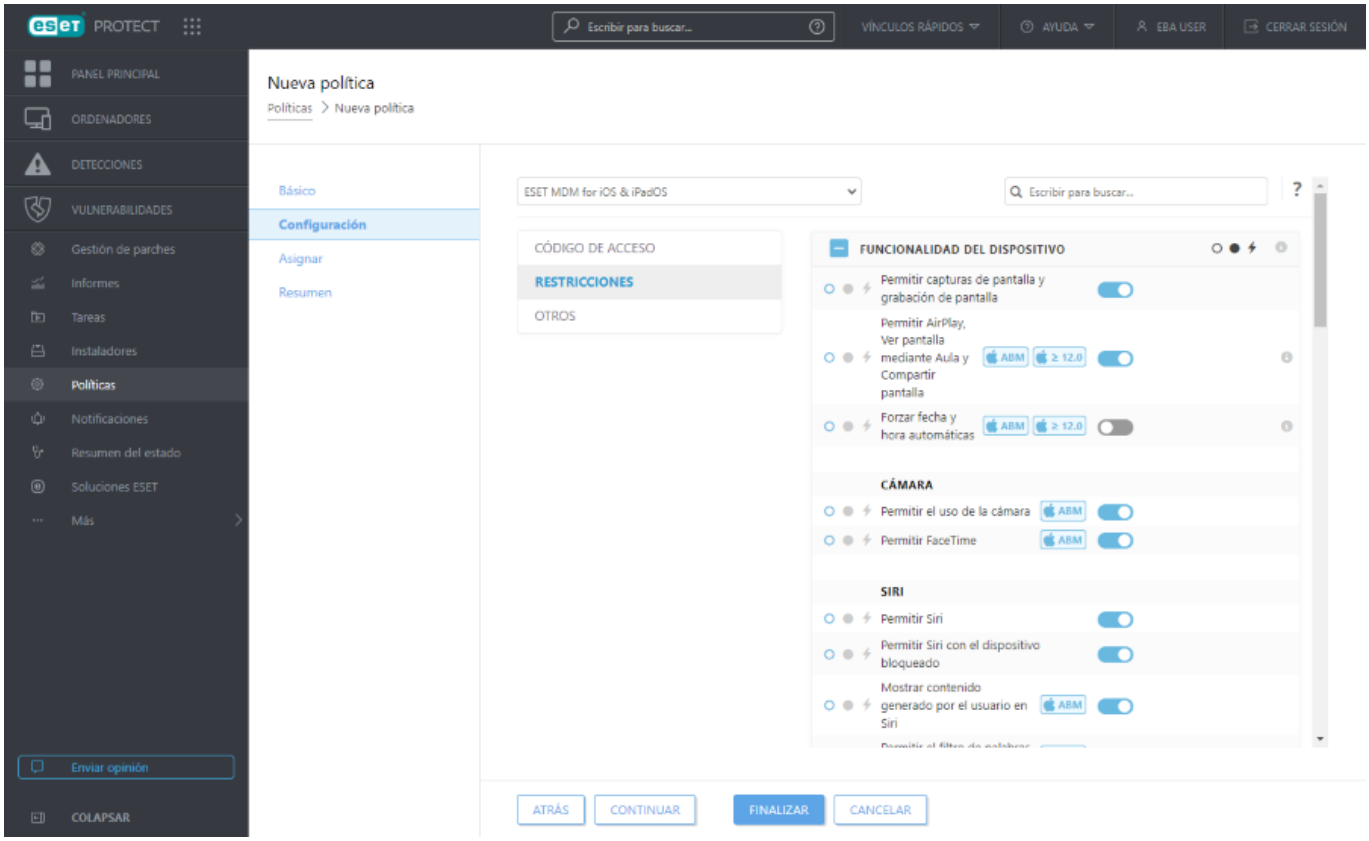
usuario.

Básico

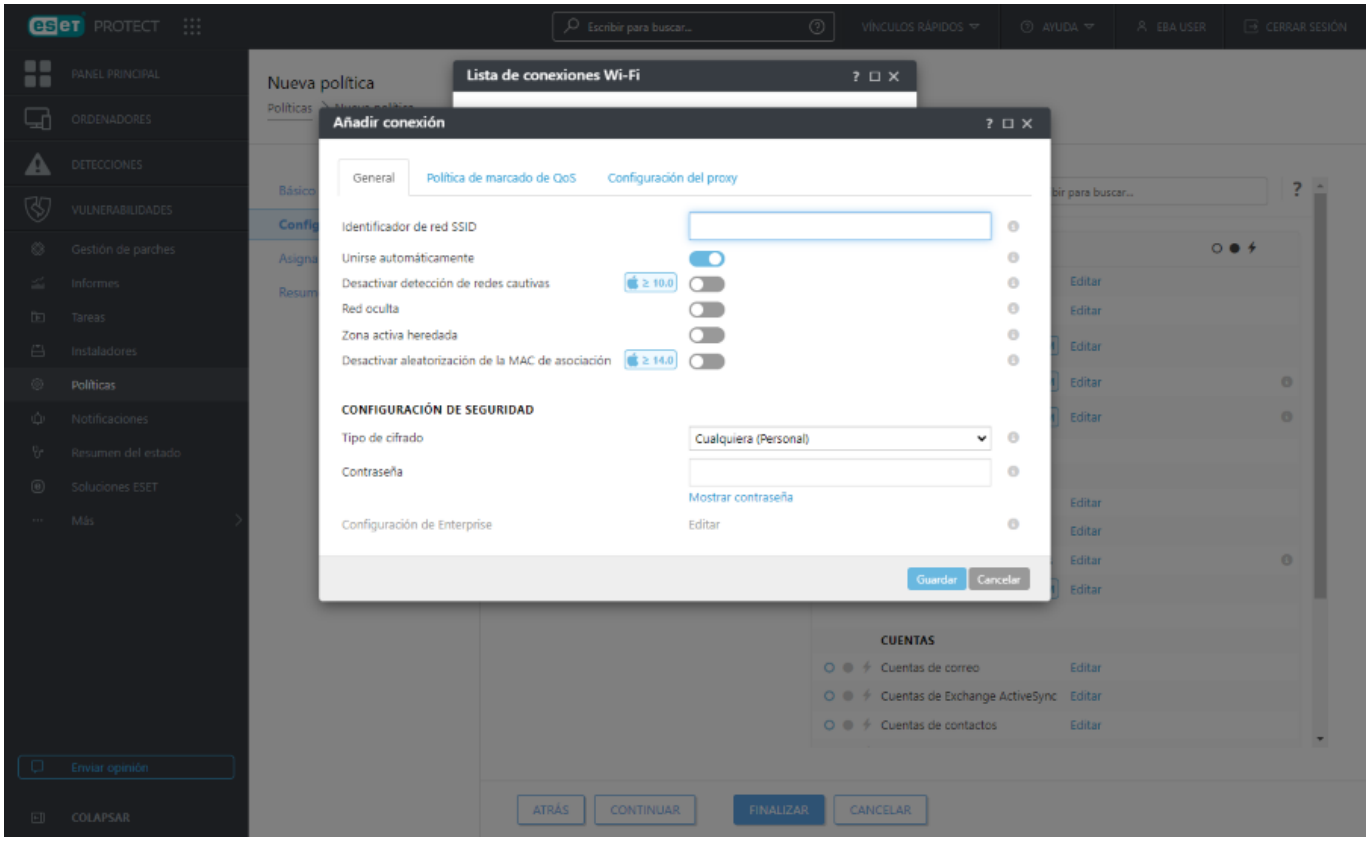
Escriba el **Nombre** de esta directiva. El campo **Descripción** es opcional.

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

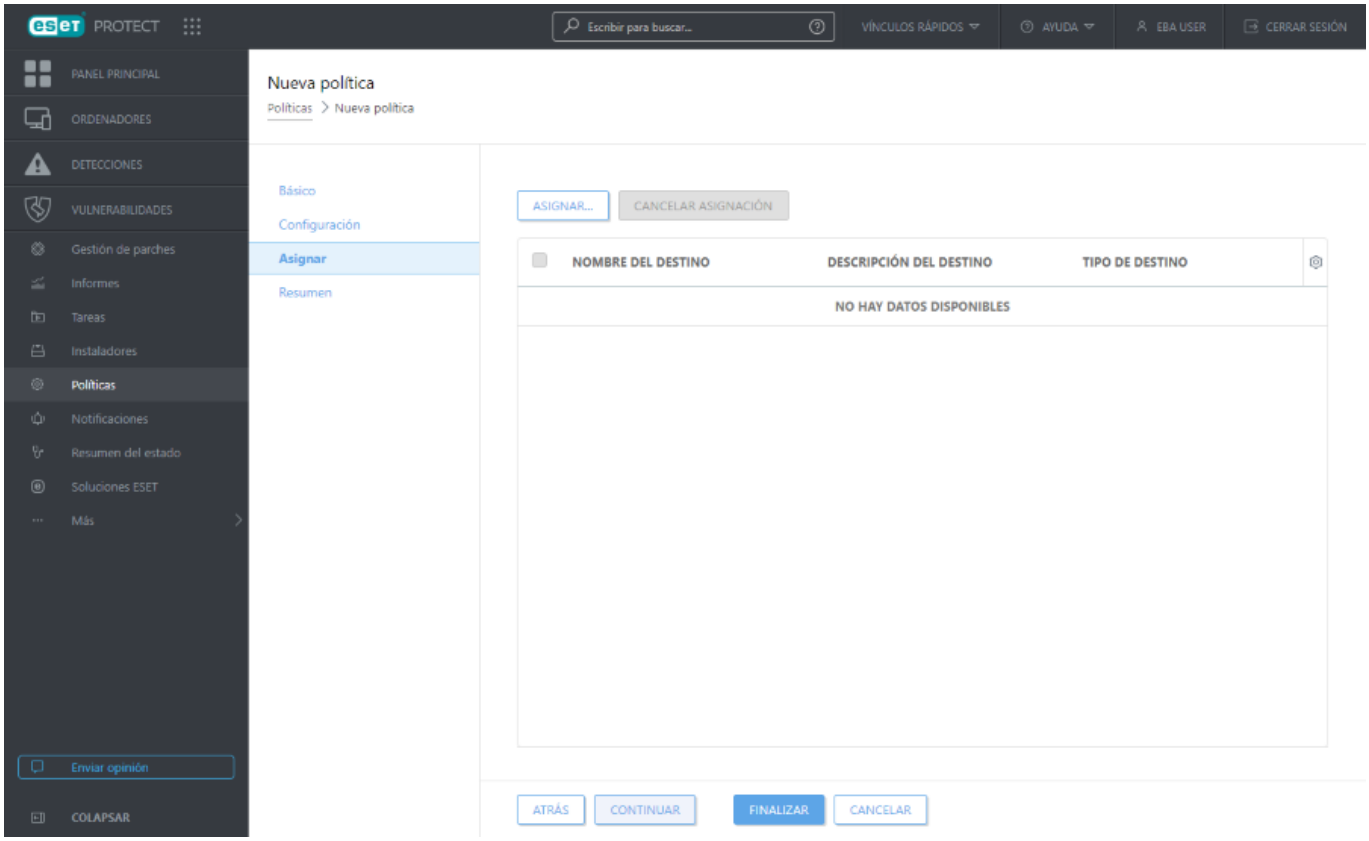
- **Tipo de cifrado**: Seleccione el cifrado adecuado de la lista desplegable, asegúrese de que este valor coincida exactamente con las capacidades de la red wifi.

- **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.

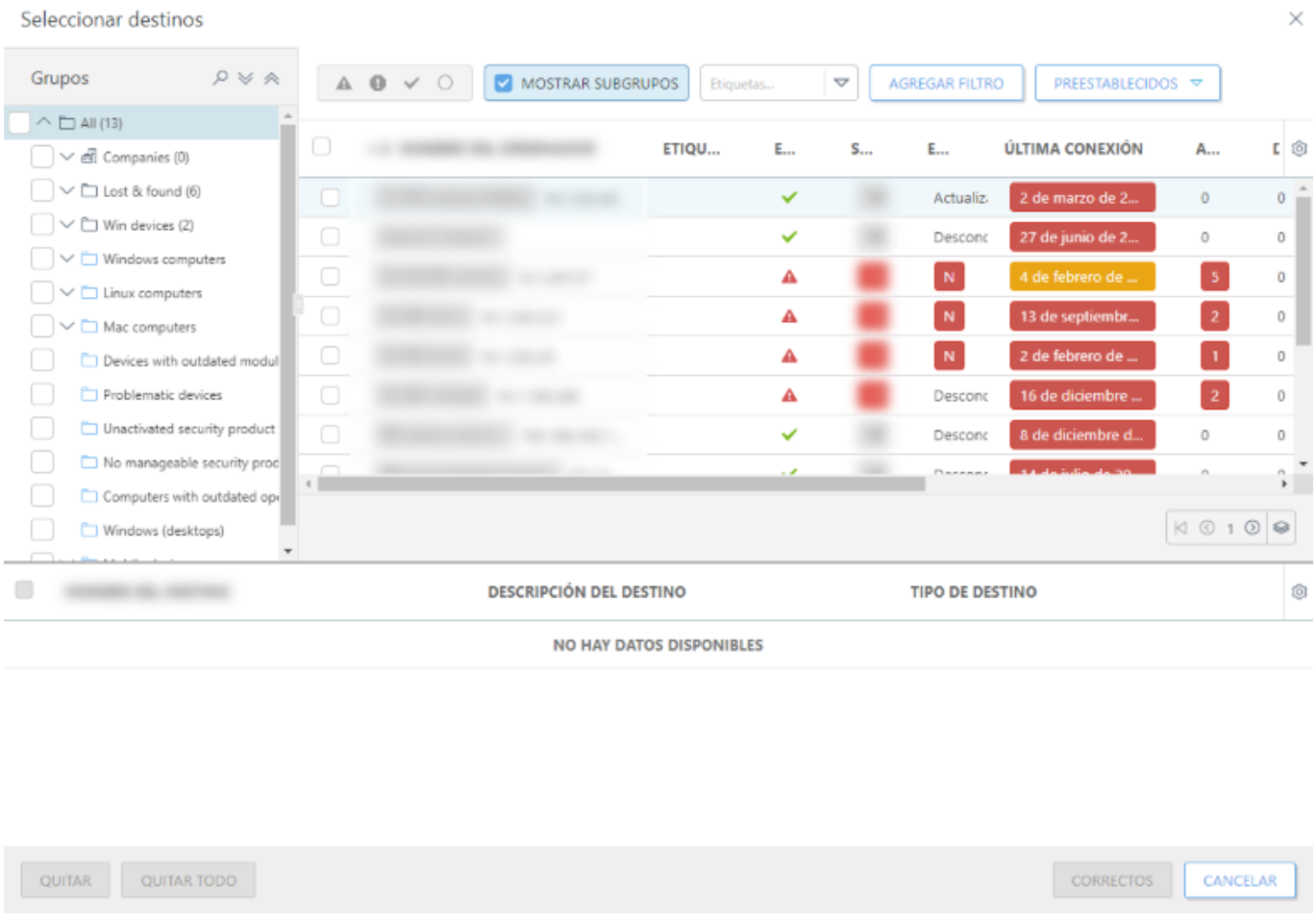
Asignar

Especifique los clientes (ordenadores individuales 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.

Perfiles de configuración del Cloud 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.

Migración a Cloud MDM (desde ESET PROTECT on-prem)

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.

Casos de migración ESET PROTECT

Casos de migración para migrar a ESET PROTECT.

En esta sección analizaremos casos de migración para realizar la transición desde otros productos de ESET a ESET PROTECT. Haga clic en el vínculo que mejor describa su caso entre los que se verá a continuación.

1. Tengo productos de seguridad Endpoint de ESET sin administrar en mi red y quiero empezar a administrarlos con ESET PROTECT.

2. Actualmente administro mi red con ESET PROTECT on-prem y quiero migrar a ESET PROTECT.

3. Actualmente administro mi red con ESET PROTECT y quiero migrar a otro ESET PROTECT.

Si administra dispositivos cifrados con ESET Full Disk Encryption, siga estos pasos para evitar la pérdida de datos de recuperación.
1.Antes de la migración: vaya a **Resumen del estado** > **Cifrado**. Aquí puede **exportar** los **datos de recuperación deESET Full Disk Encryption** actuales.
2.Después de la migración: **importe** los **datos de recuperación de ESET Full Disk Encryption** en la nueva consola de administración.
Si no puede realizar estos pasos, tendrá que descifrar los dispositivos administrados antes de la migración. Tras la migración, puede cifrar los dispositivos administrados desde ESET PROTECT Web Console.

Tengo productos Endpoint de ESET sin administrar en mi red y quiero empezar a administrarlos con ESET PROTECT.

No se pueden actualizar productos de servidor de ESET de la versión 4.5 o anteriores con Live Installer. Debe tener instalados productos de ESET versión 6 o posteriores para actualizarse a ESET PROTECT.

Siga los pasos indicados a continuación para buscar y agregar productos sin administrar en ESET PROTECT:

1. Cree una instancia de ESET PROTECT.

2. Cree un nuevo instalador y seleccione el producto que desee instalar según los productos Endpoint que haya actualmente en su red.

3. Las configuraciones de políticas y grupos de los clientes se pueden definir en el instalador. Si no se selecciona ninguna política como parte del instalador ni se aplica ninguna política a ningún grupo de ESET PROTECT, la configuración actual de sus productos Endpoint no se sobrescribirá y podrá exportarla y convertirla en una política más tarde.

4. Implemente los instaladores en su red. Live Installer instalará ESET Management Agent y actualizará los productos Endpoint existentes.

Live Installer requiere una conexión directa a Internet para descargar los componentes necesarios. Cuando finalice la instalación, podrá cambiar la conexión para que se realice a través del proxy.

5. Cuando la instalación se complete correctamente y los dispositivos se conecten a ESET PROTECT, podrá empezar a administrarlos con ESET PROTECT.

6. Si ninguna política formaba parte del instalador ni se aplicaba a ningún grupo de ESET PROTECT, ya puede exportar la configuración de sus productos Endpoint.

7. Para ello, vaya a **Tareas** y cree una nueva tarea Exportar ajustes de configuración de productos administrados.

8. En la sección **Configuración** seleccione **Producto: todos** y, como **Destino**, seleccione todos los dispositivos desde los que desee exportar la configuración.

9. Espere a que la tarea se ejecute en todos los dispositivos seleccionados.

10. Vaya a **Detalles** > **Configuración** en el dispositivo específico y abra la configuración del producto Endpoint específico.

11. En esta sección puede revisar la configuración exportada y, si todo es correcto, seleccionar **Convertir en política**.

12. Se abrirá el asistente de políticas, en el que puede editar el **nombre** de la revisión de políticas, configurar algunos de los ajustes si es necesario y hacer clic en **Finalizar** para guardar los cambios.

13. Repita este procedimiento para cada producto Endpoint.

14. Cuando todas las configuraciones de productos se hayan convertido, podrá continuar aplicando la política a los respectivos dispositivos cliente para que se bloquee la configuración y el usuario del dispositivo no pueda cambiarla.

Migración parcial de ESET PROTECT on-prem a ESET PROTECT

La migración de ESET PROTECT Server local a ESET PROTECT es parcial, consulte la tabla siguiente:

Se puede migrar:	No se puede migrar:
• Agentes de ESET Management (equipos administrados) • grupos estáticos • políticas • plantillas de grupos dinámicos • plantillas de informe • dispositivos móviles (solo Android)	• toda la base de datos • grupos dinámicos (pero puede migrar plantillas de grupos dinámicos) • detecciones • registros de auditoría • notificaciones • tareas y disparadores • instaladores • informes programados/generados (pero puede migrar plantillas de informes) • etiquetas • iOS dispositivos móviles

ESET PROTECT no es compatible con ESET Inspect On-Prem, pero sí con ESET Inspect. Si migra de ESET PROTECT On-Prem a ESET PROTECT, no podrá administrar ESET Inspect On-Prem desde ESET PROTECT, pero podrá administrar ESET Inspect desde ESET PROTECT.

Siga los pasos que se indican a continuación para migrar de ESET PROTECT Server local a ESET PROTECT:

Si tiene una cuenta MSP, siga los pasos indicados para la migración de MSP a la nube.

I. Cree una nueva instancia de ESET PROTECT.

II. Migrar políticas de ESET PROTECT On-Prem a ESET PROTECT

III. Migrar plantillas de grupos dinámicos de ESET PROTECT On-Prem a ESET PROTECT

IV. Migrar plantillas del informe de ESET PROTECT On-Prem a ESET PROTECT.

V. Migrar ordenadores administrados de ESET PROTECT On-Prem a ESET PROTECT

V.I. Migrar la estructura de grupos estáticos mediante la herramienta de exportación de ordenadores

V.II. Migrar los ordenadores administrados (instancias de ESET Management Agent) mediante la política de migración

VI. Migre los dispositivos móviles

VII. Configure usuarios de ESET PROTECT en ESET Business Account.

VIII. Agregue usuarios de ESET Business Account a ESET PROTECT Web Console.

IX. Retire ESET PROTECT Server local.

Solución de problemas después de la migración

Si administra dispositivos cifrados con ESET Full Disk Encryption, siga estos pasos para evitar la pérdida de datos de recuperación.
1.Antes de la migración: vaya a **Resumen del estado** > **Cifrado**. Aquí puede **exportar** los **datos de recuperación deESET Full Disk Encryption** actuales.
2.Después de la migración: **importe** los **datos de recuperación de ESET Full Disk Encryption** en la nueva consola de administración.
Si no puede realizar estos pasos, tendrá que descifrar los dispositivos administrados antes de la migración. Tras la migración, puede cifrar los dispositivos administrados desde ESET PROTECT Web Console.

No exporte ninguna política del agente ESET Management.
Asegúrese de cancelar por completo la asignación de todas las políticas del agente activas antes de realizar la migración.

I. Cree una nueva instancia de ESET PROTECT.

Requisitos previos

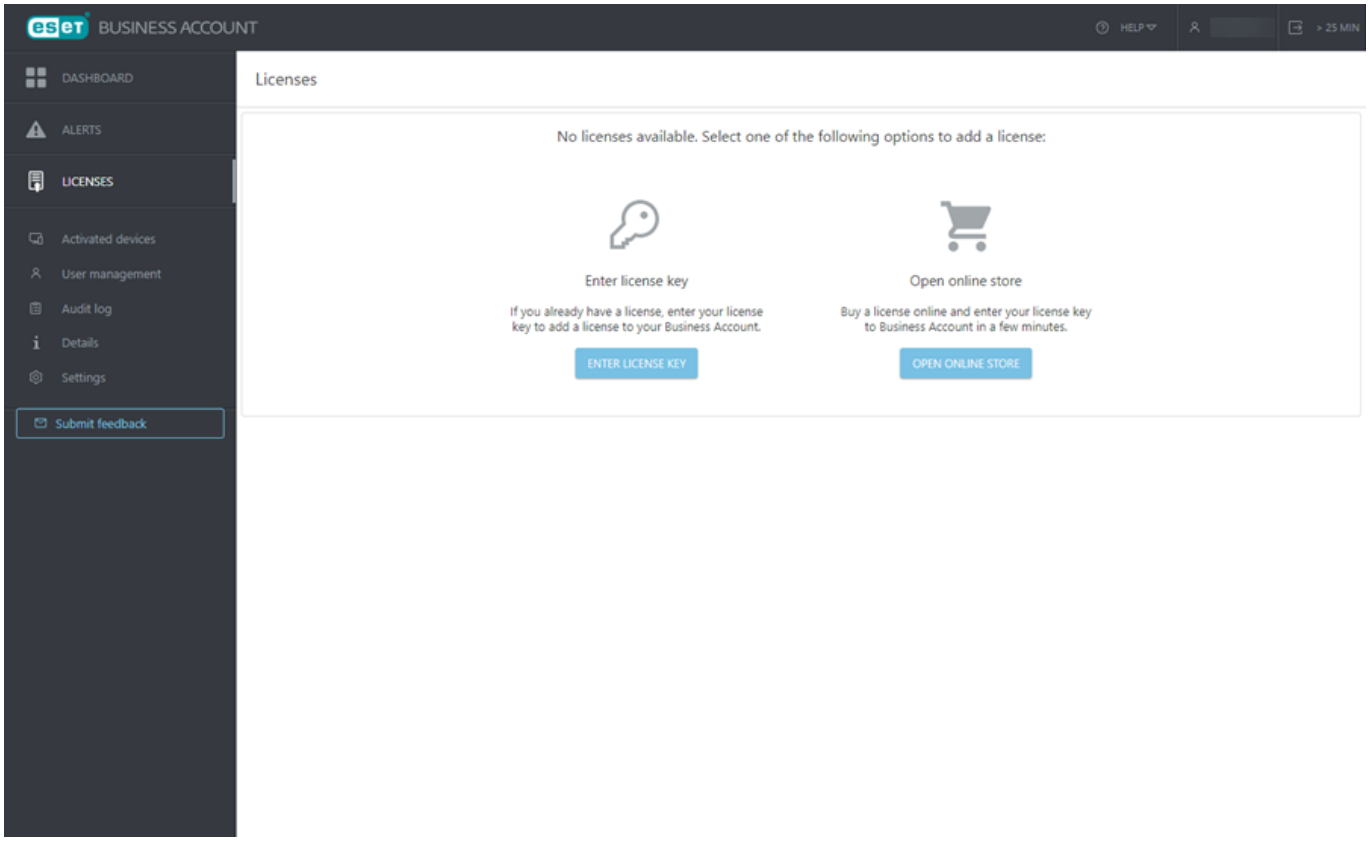
- Una cuenta de superusuario en ESET Business Account.
- Una licencia válida para ESET PROTECT.

Si sus cuentas de EBA y EMA2 se registran con la misma dirección de correo electrónico, ESET PROTECT solo se puede activar desde una cuenta. La cuenta (EBA o EMA2) a partir de la que elige crear la instancia de ESET PROTECT será la única que puede utilizar para activar o eliminar la instancia.

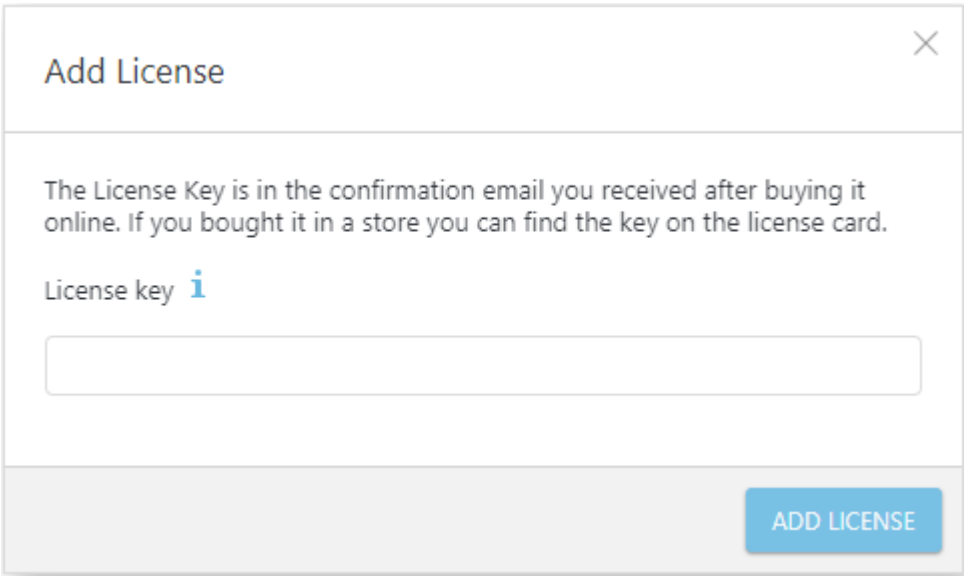
Crear una nueva instancia de ESET PROTECT

1. Abra ESET Business Account e inicie sesión (o cree una nueva cuenta).

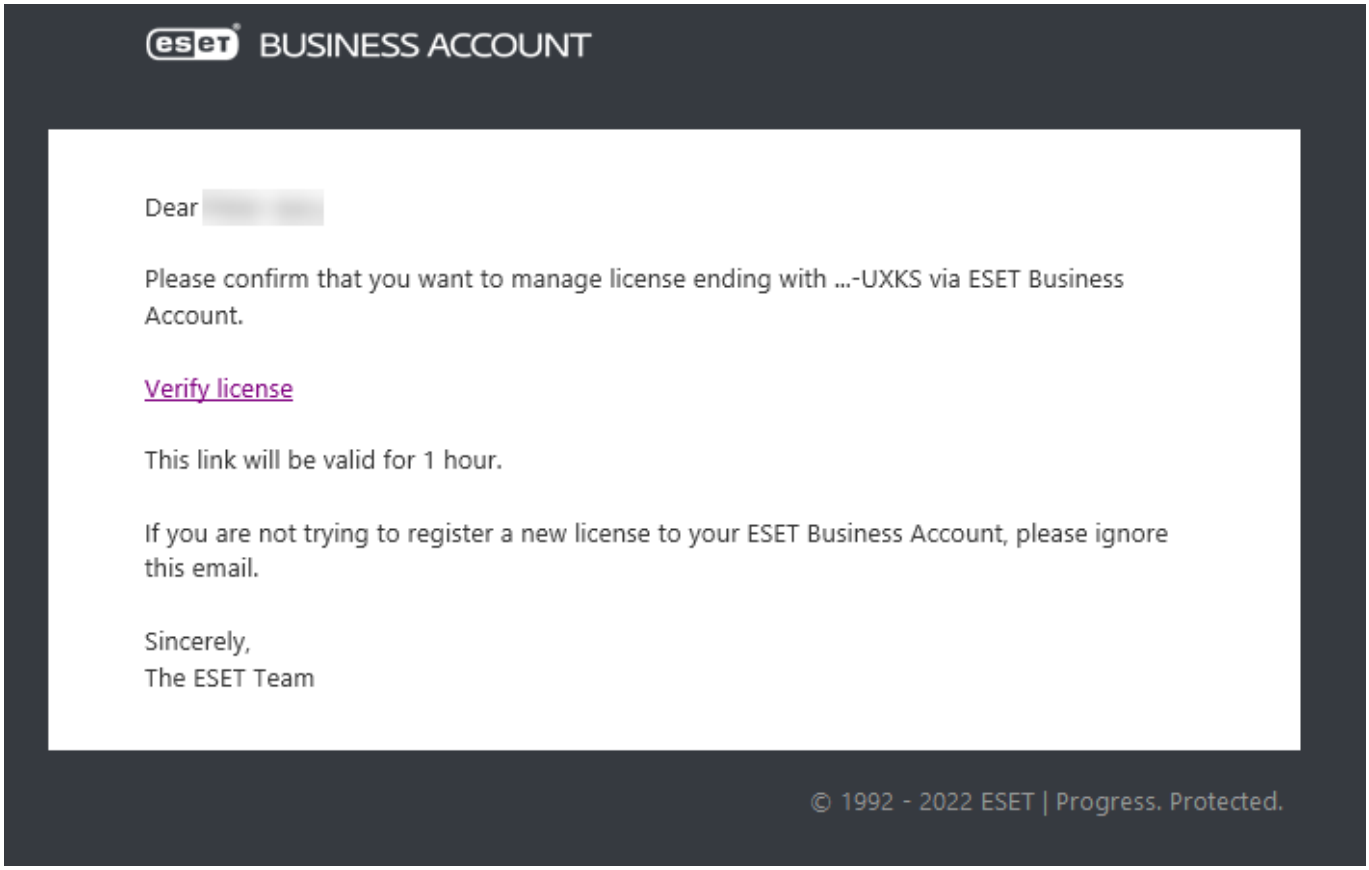
2. Haga clic en **Licencias** > **Introducir clave de licencia**.



3. En la ventana **Agregar licencia**, introduzca su **clave de licencia** de ESET PROTECT y haga clic en **Agregar licencia**.



4. Recibirá un mensaje de correo electrónico de verificación (si no recibe el mensaje de correo electrónico, siga las instrucciones del artículo de la base de conocimiento). Haga clic en **Verificar licencia**.



5. En el **Panel**, haga clic en **Activar** en **ESET PROTECT**.

⚠ Compruebe la configuración de idioma de ESET Business Account. Algunos elementos de las ventanas del programa principal de ESET PROTECT se definen la primera vez que configura el idioma en la configuración de idioma de ESET Business Account y no se pueden cambiar posteriormente.

6. Se abrirá la ventana **Activar ESET PROTECT**. Lea los Términos de uso y marque la casilla de verificación si los acepta.

7. Seleccione la ubicación de centro de datos de su instancia de ESET PROTECT que sea la más cerca a la ubicación de su red administrada y haga clic en **Continuar**.

⚠ Una vez seleccionada, no podrá cambiar la ubicación de centro de datos de su instancia de ESET PROTECT.

8. Se creará su instancia de ESET PROTECT. Puede esperar unos minutos hasta que se cree o puede cerrar sesión y se le notificará por correo electrónico cuando la instancia de ESET PROTECT esté disponible.

9. Haga clic en **Continuar**. También puede hacer clic en **Panel** y en **Abrir** en la ventana dinámica de ESET PROTECT para abrir una nueva pestaña de ESET PROTECT Web Console.

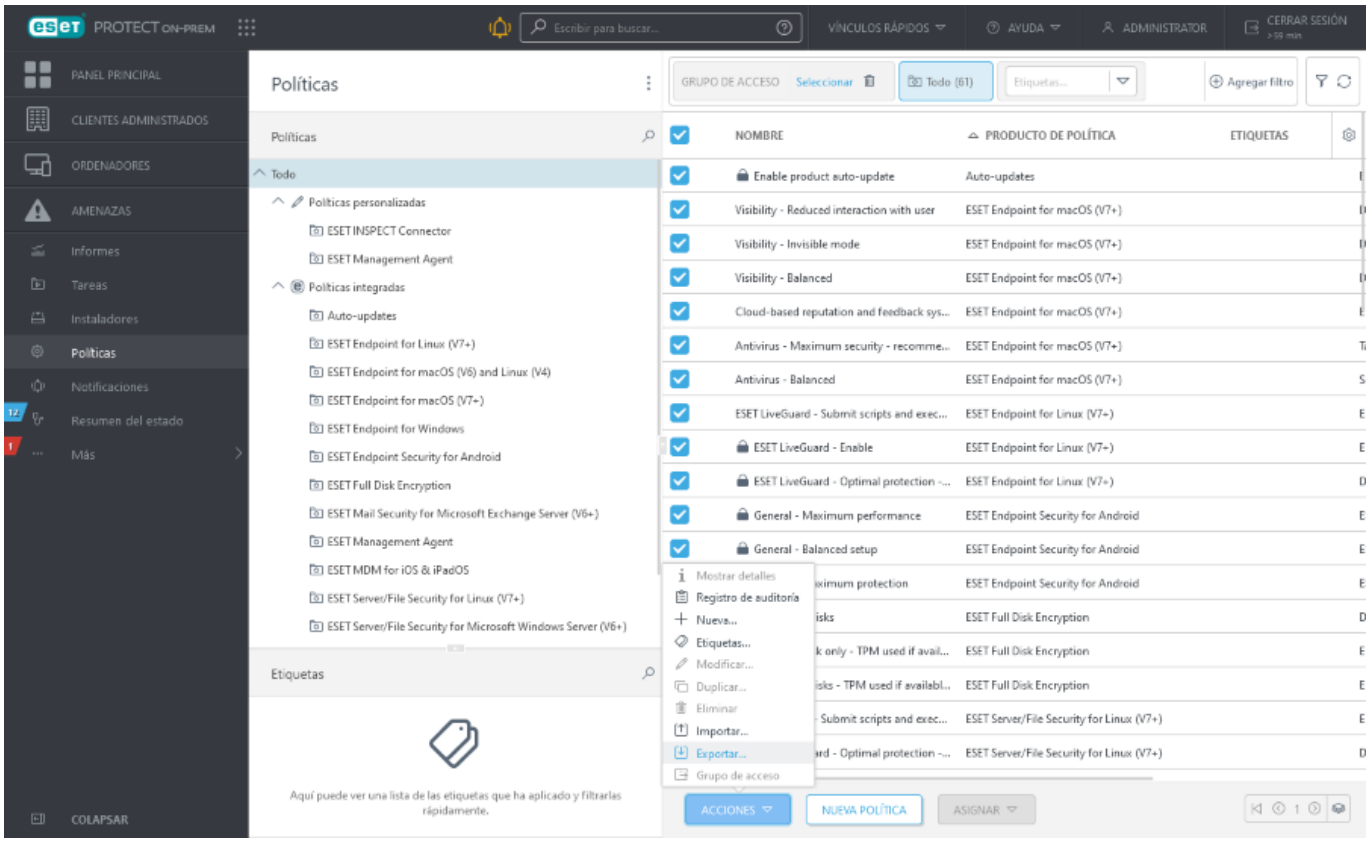
ESET PROTECT sincroniza su estructura de ESET Business Account con el árbol de grupos estáticos de **Ordenadores** en Web Console.

II. Migrar políticas de ESET PROTECT On-Prem a ESET PROTECT

1. Ingrese a su cuenta ESET PROTECT On-Prem.

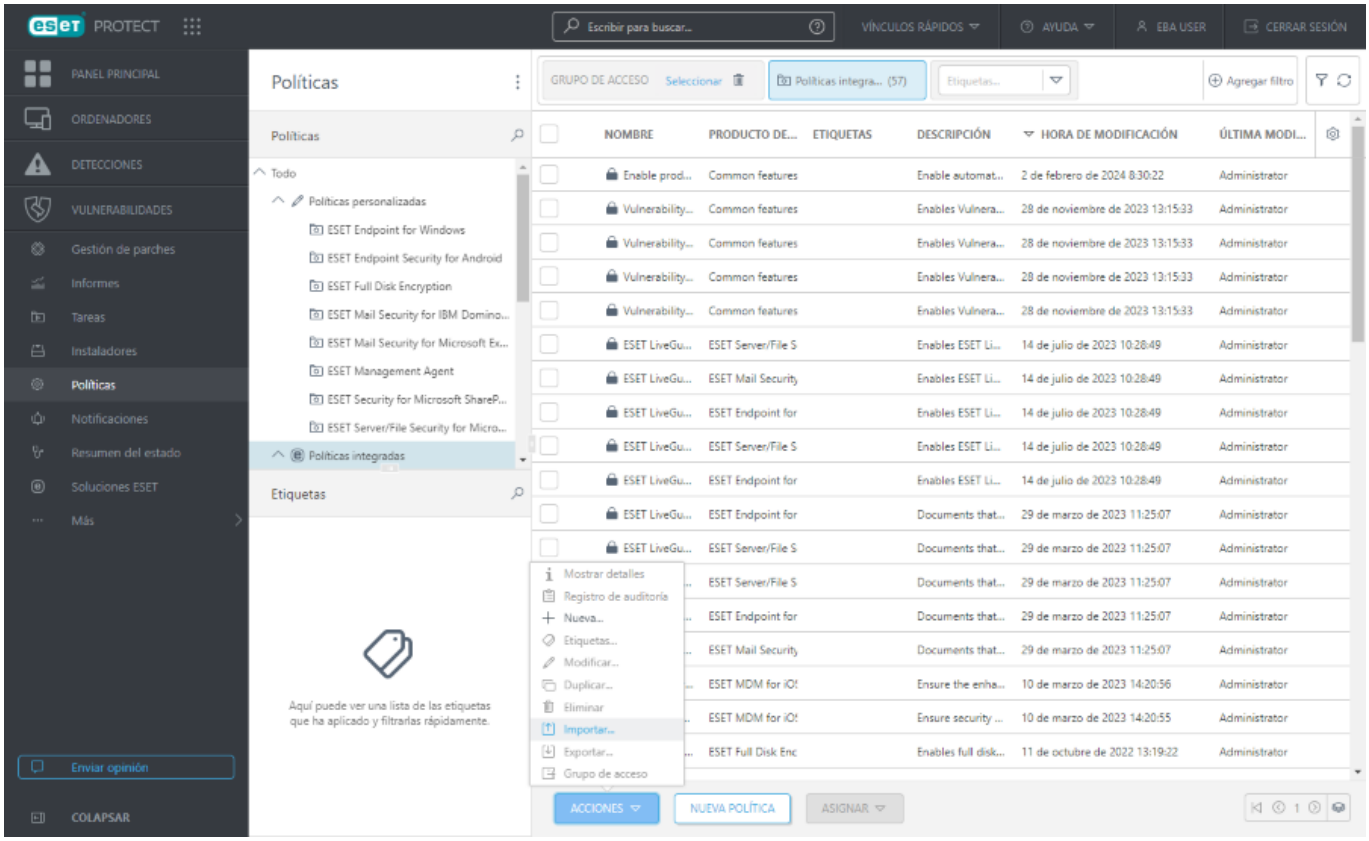
2. En su ESET PROTECT On-Prem, seleccione **Políticas** > **Todas** > seleccione la casilla de verificación ubicada en el encabezado de la tabla (o seleccione las casillas de verificación ubicadas junto a las políticas que desea exportar) y haga clic en **Acciones** > **Exportar**.

> ⚠ No exporte ninguna política del agente ESET Management.
> Asegúrese de cancelar por completo la asignación de todas las políticas del agente activas antes de realizar la migración.



3. Guarde el archivo *.dat* con la lista de políticas.

4. En ESET PROTECT, haga clic en **Políticas** > **Acciones** > **Importar** y seleccione el archivo *.dat* con la lista de políticas exportadas de ESET PROTECT On-Prem en el paso 2 y, a continuación, haga clic en **Importar** para importarlos a ESET PROTECT.



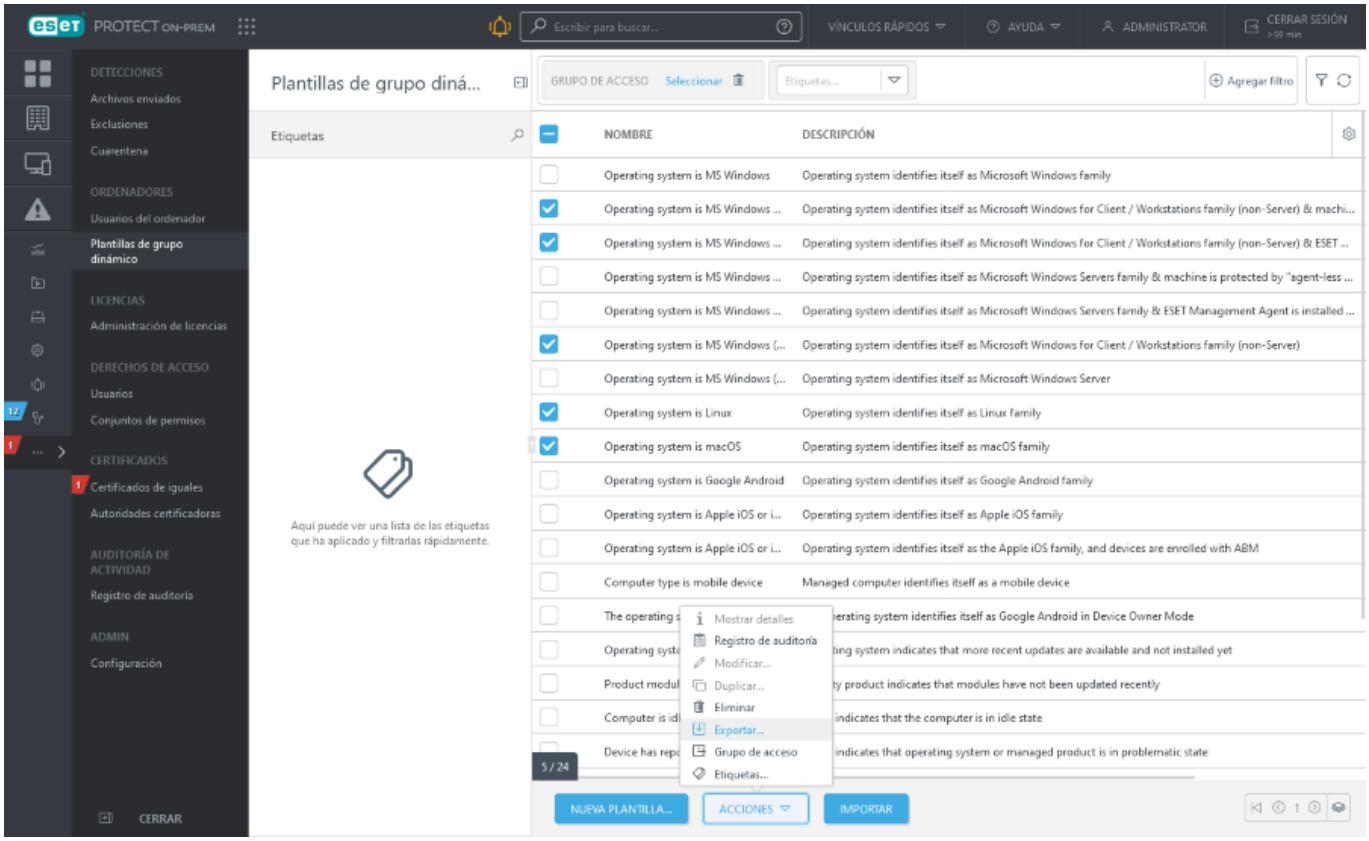
5. Las políticas importadas aparecerán en **Políticas personalizadas**. Tras la migración de equipos de ESET PROTECT On-Prem a ESET PROTECT, las políticas que estaban asignadas a los equipos en ESET PROTECT On-Prem no se conservan. Tras importar las políticas en ESET PROTECT, puede asignarlas a ordenadores importados en ESET PROTECT.

Tenga cuidado a la hora de aplicar políticas a los ordenadores:
a)En su ESET PROTECT On-Prem: haga una lista de las políticas aplicadas y su orden para cada ordenador administrado.
b)Entrante ESET PROTECT: Aplique las políticas a cada equipo en función de la configuración de políticas de ESET PROTECT On-Prem.

III. Migrar plantillas de grupos dinámicos de ESET PROTECT On-Prem a ESET PROTECT

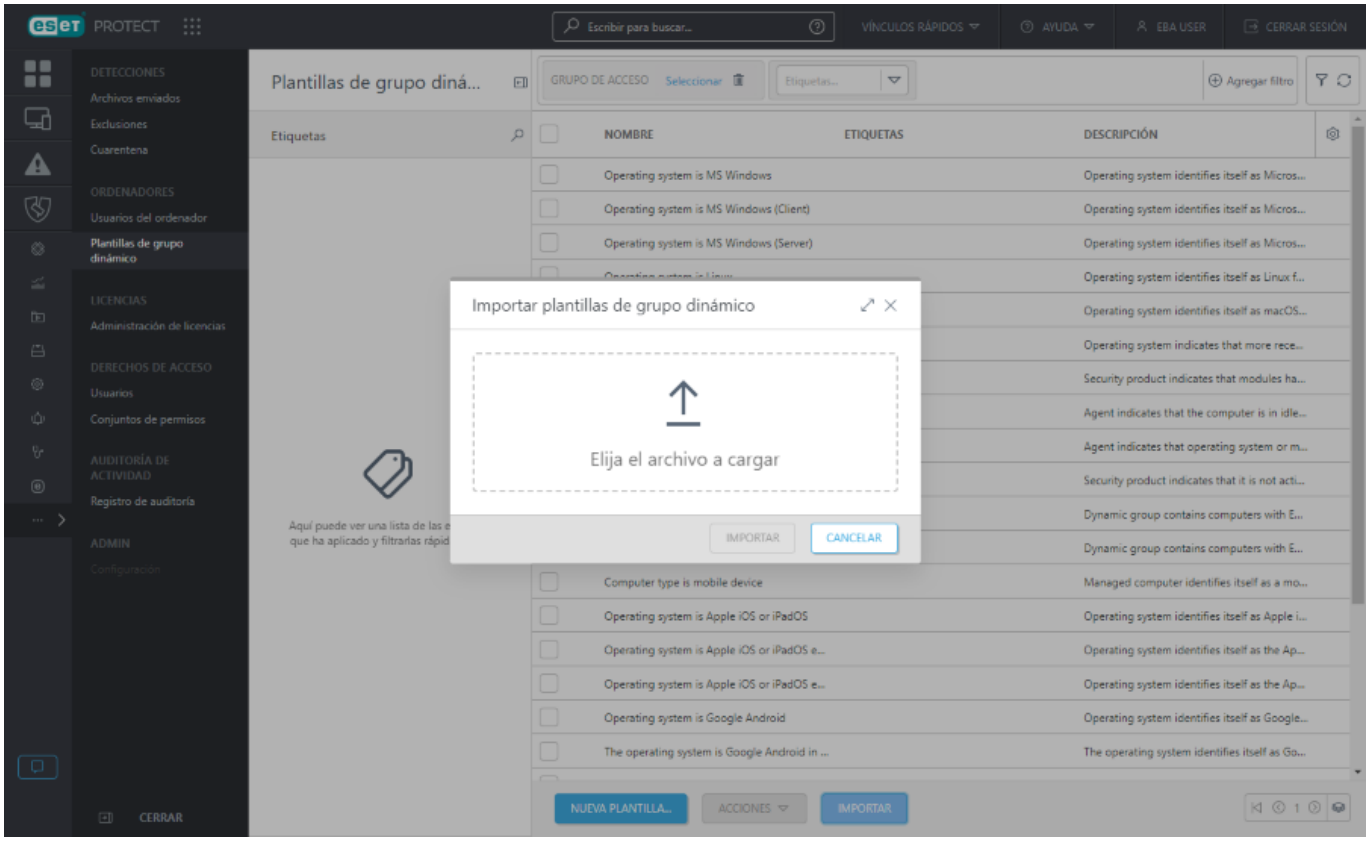
1. En ESET PROTECT, On-Prem seleccione **Más** > **Plantillas de grupos dinámicos**.

2. Seleccione las casillas de verificación situadas junto a las plantillas de grupo dinámico que desea exportar y haga clic en **Acciones** > **Exportar**.



3. Guarde el archivo *.dg* con las plantillas de grupo dinámico exportadas.

4. En ESET PROTECT, haga clic en **Más** > **Plantillas de grupos dinámicos** > **Importar** y seleccione el archivo *.dg* con las plantillas de grupo dinámico exportadas de ESET PROTECTOn-Prem y haga clic en **Importar** para importarlas a ESET PROTECT.



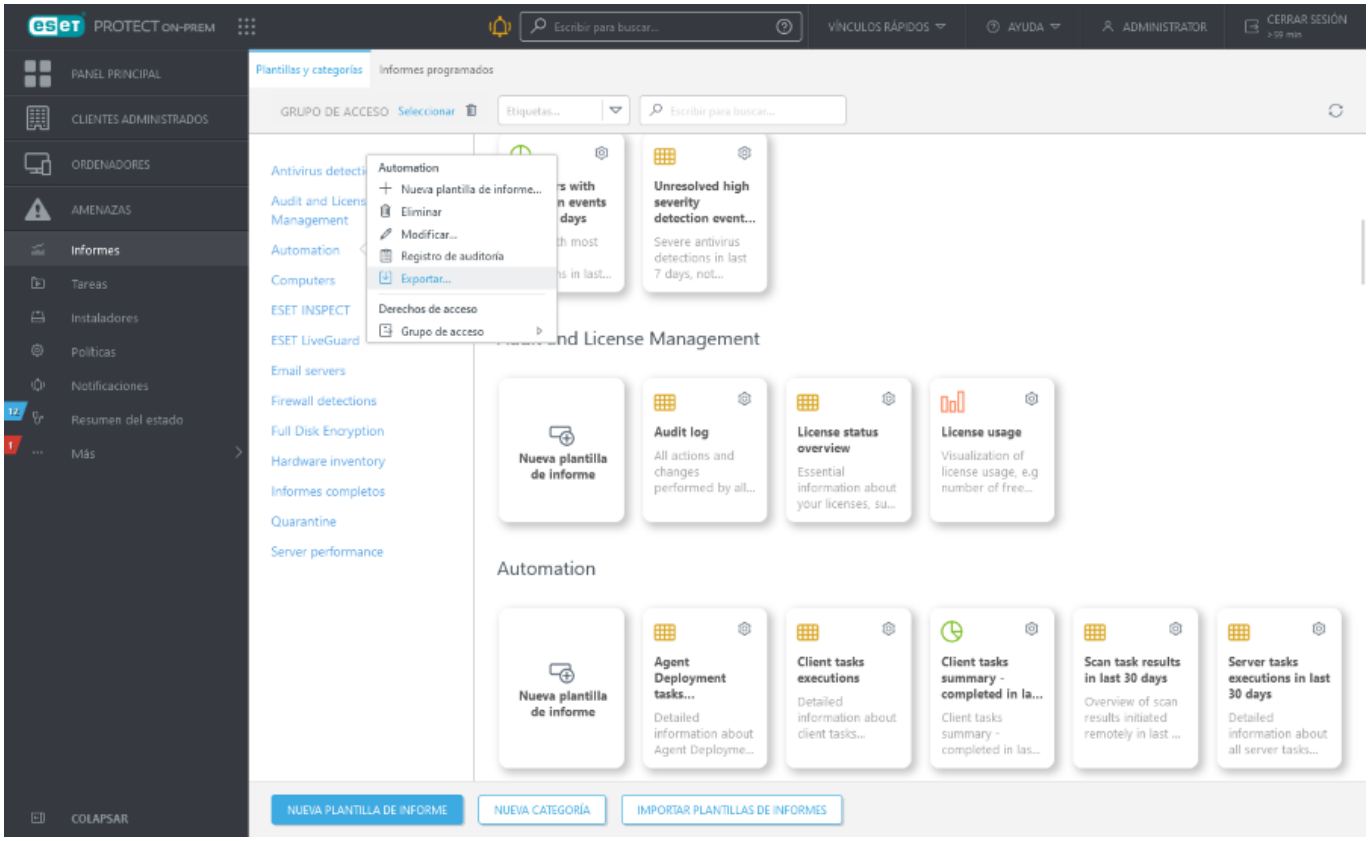
5. Las plantillas de grupo dinámico importadas aparecerán en la lista de todas las plantillas de grupo dinámico

y podrá utilizarlas para crear grupos dinámicos (no se pueden migrar grupos dinámicos).

IV. Migrar plantillas del informe de ESET PROTECT On-Prem a ESET PROTECT.

1. En ESET PROTECT On-Prem, seleccione **Informes**.

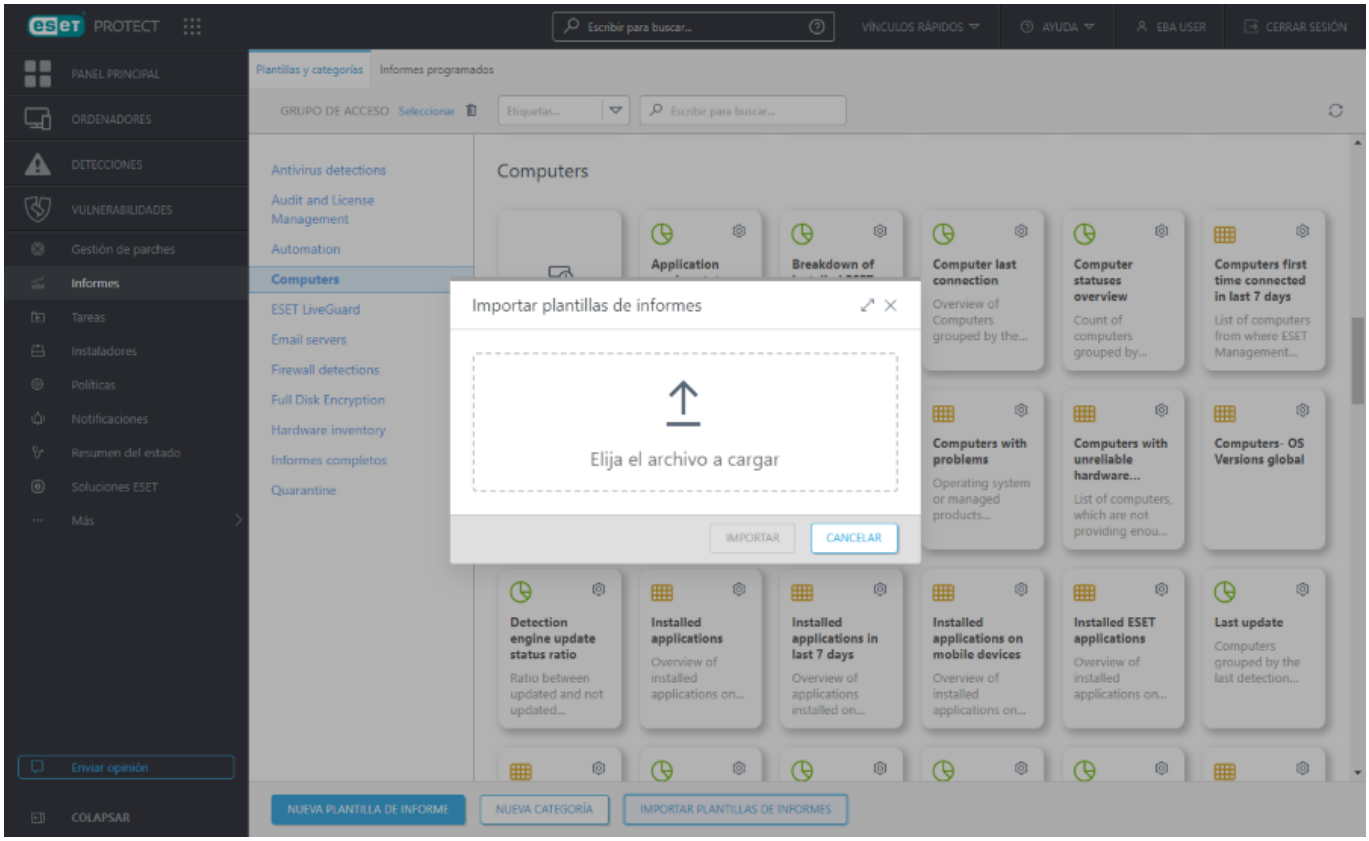
2. Haga clic en el icono de engranaje situado junto a una categoría de informe o una plantilla de informe individual y, a continuación, haga clic en **Exportar**.



3. Guarde el archivo *.dat* con las plantillas de informe exportadas.

4. En ESET PROTECT, haga clic en **Informes** > **Importar plantillas de informe** y seleccione el archivo *.dat* con las plantillas de informe exportadas de ESET PROTECTOn-Prem y haga clic en **Importar** para importarlas a ESET PROTECT.

Repita los pasos anteriores para migrar más plantillas de informe individuales o más categorías de informe.



5. Las plantillas de informe importadas aparecerán en **Informes**. Puede utilizar las plantillas de informe para programar y generar informes.

V. Migrar ordenadores administrados de ESET PROTECT On-Prem a ESET PROTECT

V.I. Migrar la estructura de grupos estáticos mediante la herramienta de exportación de ordenadores

La herramienta de exportación de ordenadores puede exportar la estructura de grupos estáticos (no MSP o MSP) desde ESET PROTECT On-Prem. A continuación, puede importar la estructura de grupos estáticos en ESET PROTECT.

Si decide no utilizar la herramienta de exportación de ordenadores:
- Continúe con la migración usando la política de migración.
- Tras la migración, todos los equipos aparecerán en el grupo estático **Perdidos y encontrados** en ESET PROTECT.

Requisitos previos para ejecutar la herramienta de exportación de ordenadores:

- Windows o Linux de 64 bits

- Python (versión 3.9 y posteriores): puede comprobar si Python está instalado y comprobar su versión ejecutando el siguiente comando:

  - Símbolo del sistema de Windows: `python --version`

- Terminal de Linux: `python3 --version`

Puede descargar Python de https://www.python.org/ e instalarlo. Asegúrese de marcar la casilla **Add python.exe to PATH** durante la instalación en Windows.

- Asegúrese de que se pueda acceder al puerto de Web Console (2223 o un puerto personalizado) en la red.

1. Descargue la herramienta de exportación de ordenadores en el ordenador.

2. Descomprima el archivo *computers_export_tool.zip* descargado.

3. Abra la carpeta *computers_export_tool* en la ventana del símbolo del sistema de Windows o del terminal de Linux.

4. Ejecute el siguiente comando:

- Windows: `python computers_export_tool.py`
- Linux: `python3 computers_export_tool.py`

5. En **Hostname [localhost]**, escriba el nombre de host de ESET PROTECT On-Prem y pulse Enter. Si ejecuta la herramienta de exportación de ordenadores en ESET PROTECT Server, pulse Enter para usar el valor de `localhost` predeterminado.

6. En **Port [2223]**, pulse Enter si ESET PROTECT On-Prem utiliza el puerto de Web Console predeterminado (2223) o escriba el puerto de Web Console personalizado y pulse Enter.

7. En **Username**, escriba el nombre de usuario de Web Console y pulse Enter.

Utilice el usuario de Web Console con privilegios de administrador que tenga acceso a todos los grupos estáticos de ESET PROTECT On-Prem para garantizar la exportación de todos los grupos estáticos.

8. En **Password**, escriba la contraseña del usuario de Web Console (no verá los signos escritos) y pulse Enter.

9. La herramienta genera un archivo *computers.csv* (ubicado en la misma carpeta: *computers_export_tool*). El archivo *computers.csv* contiene la estructura de grupos estáticos de ESET PROTECT On-Prem con nombres de ordenador. Nota: Si vuelve a ejecutar la herramienta, sobrescribe el archivo *computers.csv*.

Un gran número de ordenadores administrados

La importación de un gran número de ordenadores puede llevar mucho tiempo. Si hay más de 30.000 ordenadores administrados en ESET PROTECT On-Prem, siga estos pasos:
1.Con un sencillo editor de texto, divida el archivo *computers.csv* en varios archivos *.csv* con hasta 30.000 líneas en cada archivo.
2.Importe cada archivo *.csv* en ESET PROTECT repitiendo los pasos indicados a continuación.

10. En ESET PROTECT Web Console en la nube, haga clic en **Ordenadores** > haga clic en el icono de engranaje situado junto a **Todos los grupos estáticos** > seleccione **Importar**.

11. Haga clic en **Elegir archivo** > seleccione el archivo *computers.csv* y haga clic en **Abrir**.

12. Haga clic en **Importar**. ESET PROTECT importará la estructura de grupos estáticos de ESET PROTECT On-

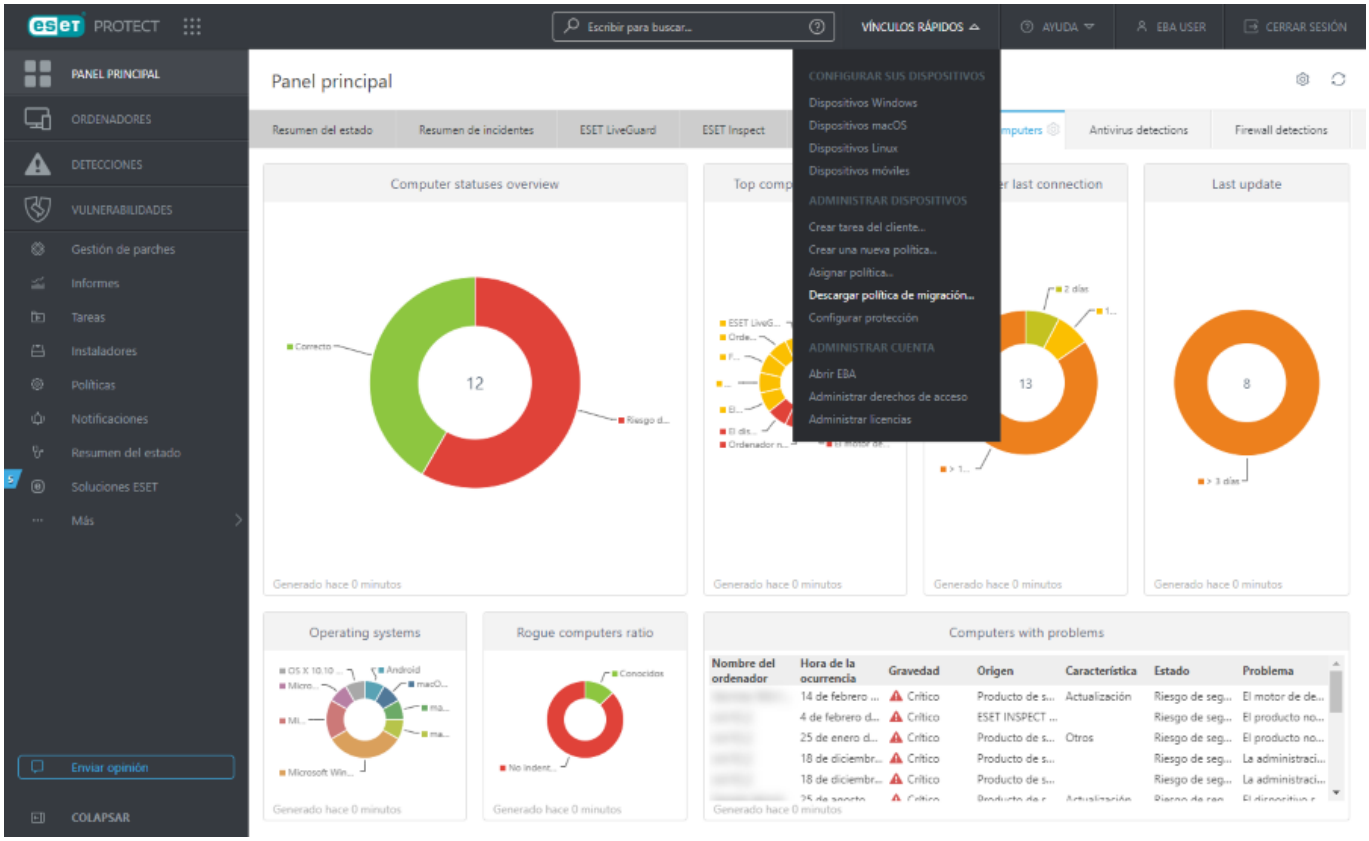
Prem del archivo *computers.csv*. Puede cerrar la ventana de importación y continuar trabajando con ESET PROTECT.

13. Una vez completada la importación, la estructura de grupos estáticos con los nombres de los ordenadores de ESET PROTECT On-Prem aparecerá en **Ordenadores** en ESET PROTECT Web Console en la nube. Continúe con los pasos que se indican a continuación: use la política de migración para migrar los ordenadores administrados (instancias de ESET Management Agent).

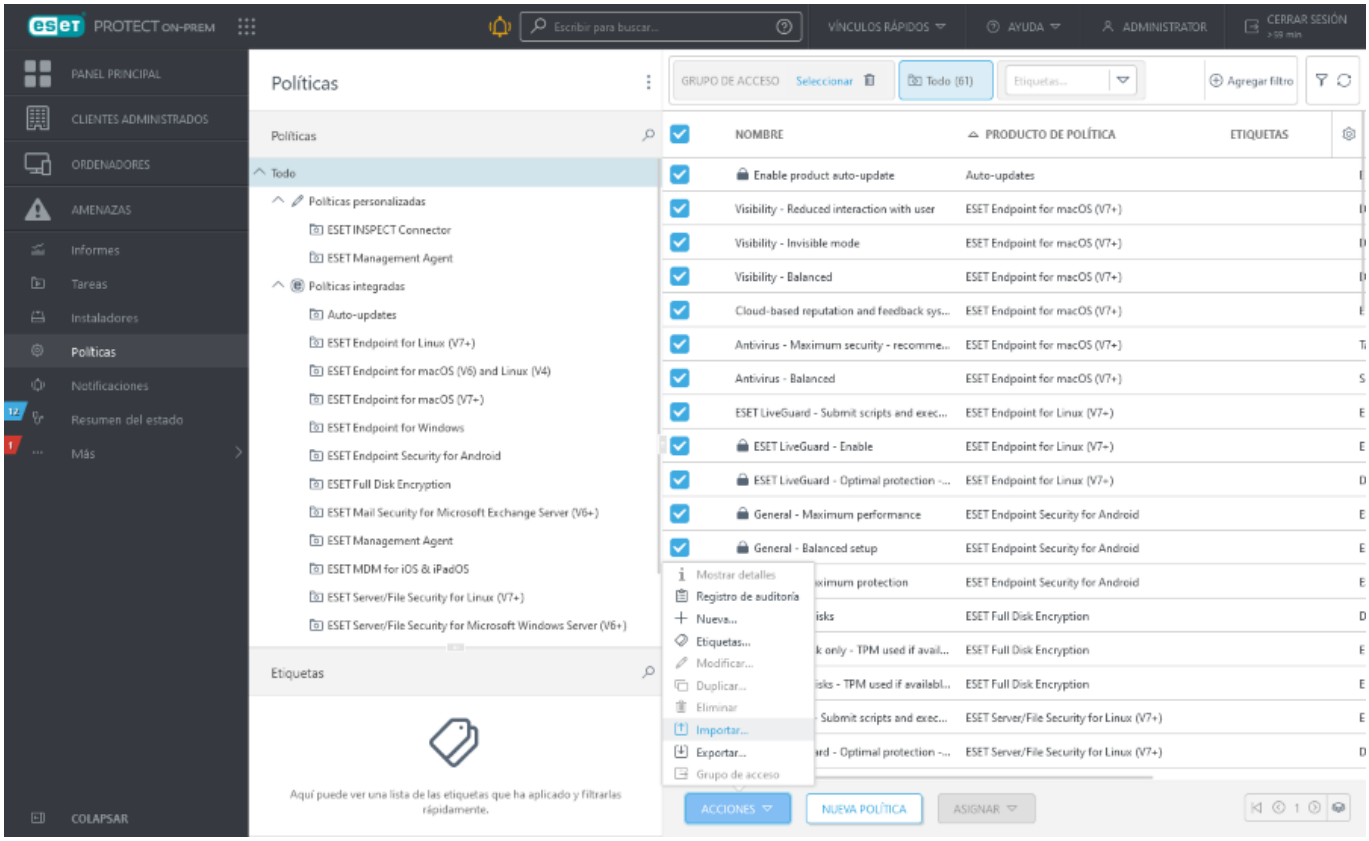
V.II. Migrar los ordenadores administrados (instancias de ESET Management Agent) mediante la política de migración

Antes de la migración de los agentes, asegúrese de que la configuración del cortafuegos cumpla con los requisitos previos de red de ESET PROTECT.

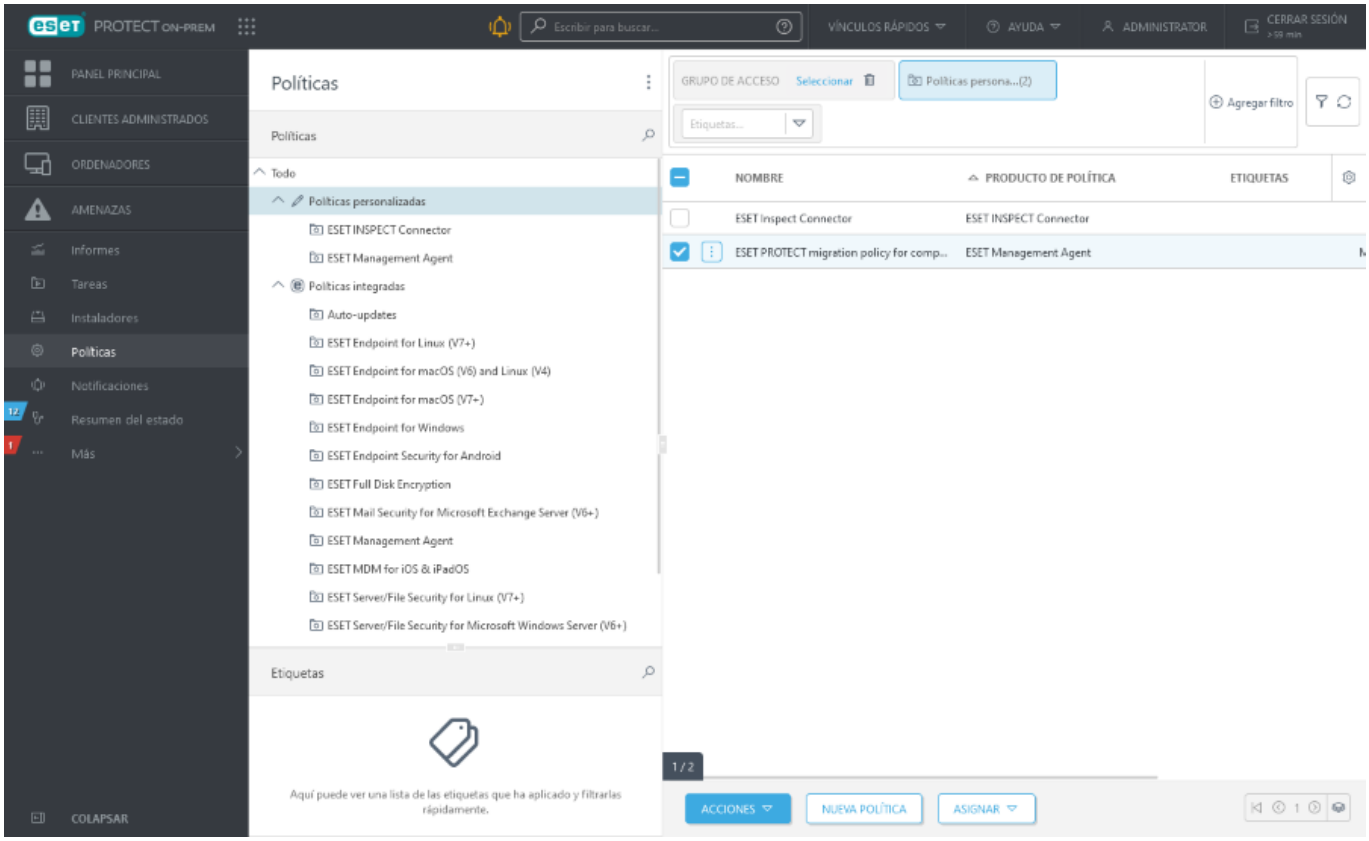
1. En ESET PROTECT Web Console, haga clic en **Vínculos rápidos** > **Descargar política de migración** y guarde el archivo *.dat*.



2. En ESET PROTECT On-Prem, seleccione **Políticas** > **Importar**. Seleccione el archivo *.dat* descargado en el paso anterior y haga clic en **Importar**.



3. Vaya a **Políticas personalizadas** y seleccione la política de migración importada.



4. Haga clic en la política de migración > **Editar**.

5. En **Configuración** > **Conexión**, establezca la marca **Forzar** para **Servidores a los que conectar** y **Certificado**.

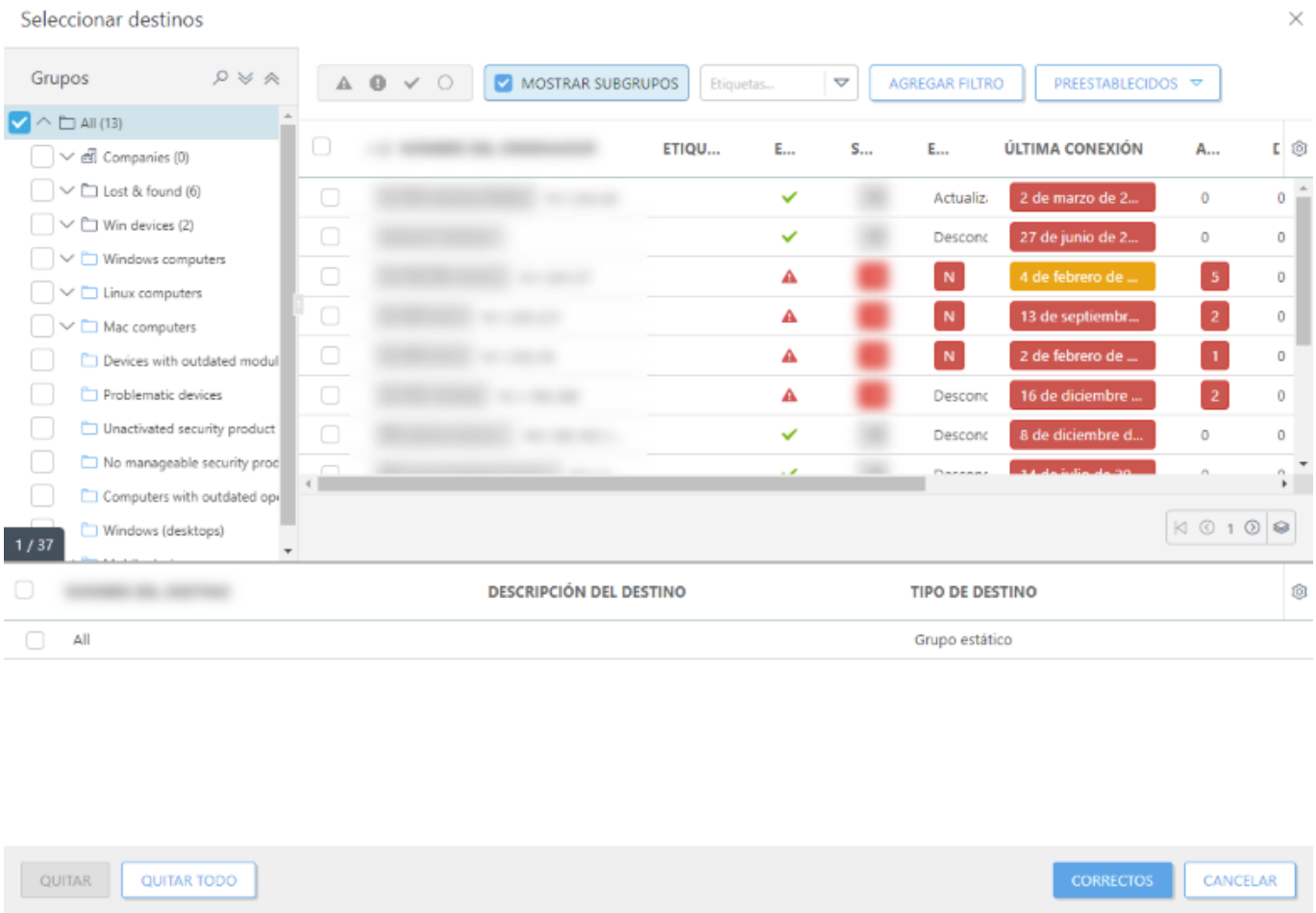
6. Haga clic en **Finalizar**.

> **Probar la migración con varios equipos**
> Se recomienda migrar varios ordenadores a los que se tenga acceso físico. Asegúrese de que puedan conectarse a ESET PROTECT y, a continuación, migre todos los ordenadores.

7. Haga clic en **Asignar** > **Asignar grupos**.

8. Seleccione el grupo estático **Todo** y haga clic en **Aceptar**.

> Aplique la política de migración al grupo estático **Todos** para asegurarse de migrar los equipos administrados.

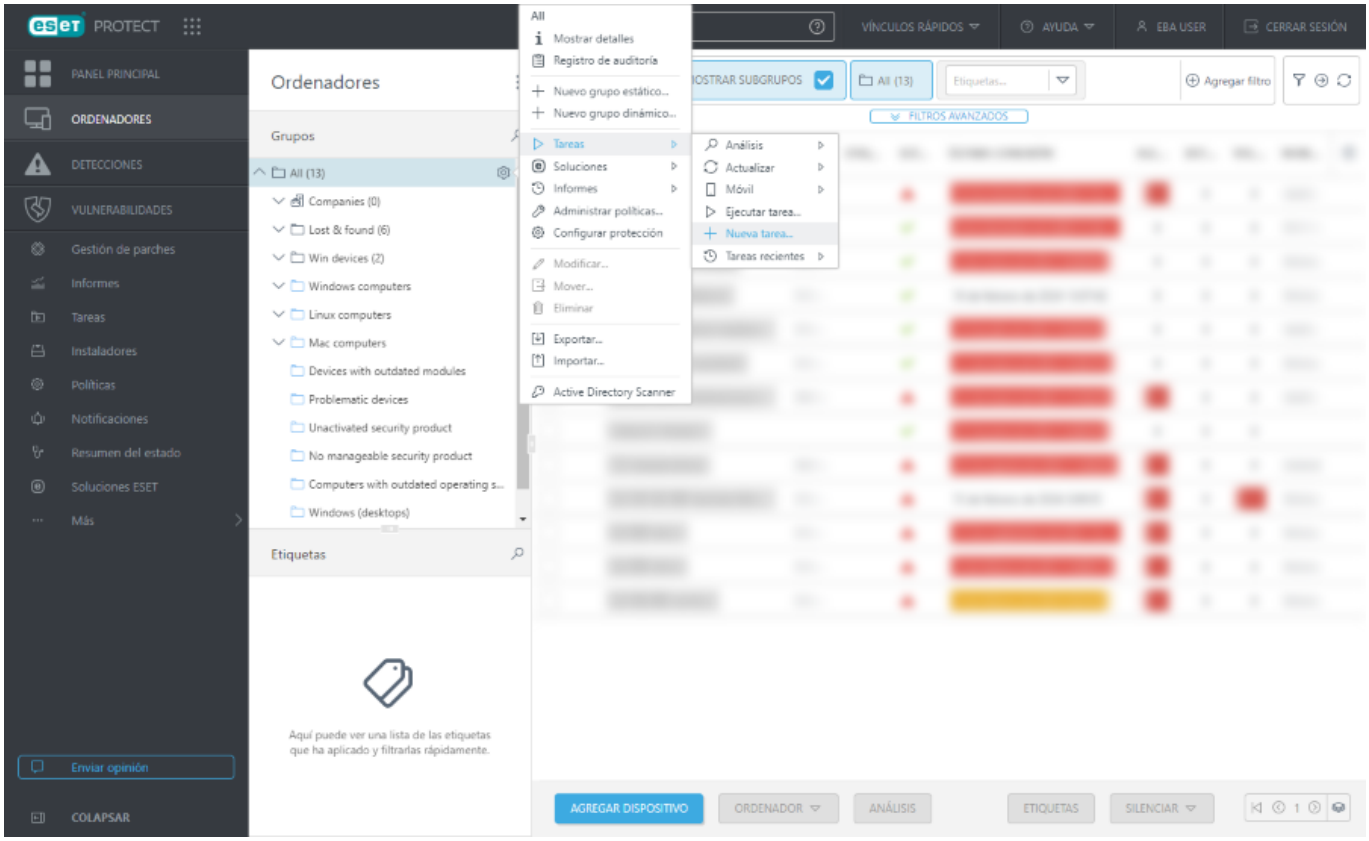


9. Haga clic en **Finalizar** para aplicar la política.

10. Inicie sesión en la Consola Web de ESET PROTECT. En **Equipos**, verá los equipos que se han migrado desde ESET PROTECT On-Prem. Es posible que deba esperar unos minutos hasta que todos los equipos de ESET PROTECT On-Prem empiecen a conectarse a ESET PROTECT.

11. Después de migrar los equipos de ESET PROTECT On-Prem a ESET PROTECT, debe volver a activar los productos de seguridad de ESET en los equipos administrados con licencias en la nube administradas por ESET PROTECT:

a. En la consola web de ESET PROTECT, haga clic en **Equipos** > haga clic en el ícono de engranaje situado junto **Todos** los grupos estáticos > seleccione **Tareas** > **Nueva tarea**.



b.Seleccione **Activación del producto** en el menú desplegable **Tarea**.

c.Seleccione la licencia del producto de seguridad de ESET en **Configuración**, revise los ordenadores de destino en **Destino** y haga clic en **Finalizar**.

Si los ordenadores ejecutan varios productos de seguridad de ESET, debe repetir los pasos de activación y seleccionar la licencia correspondiente para cada categoría de productos de seguridad de ESET.

d.Espere unos minutos hasta que los productos de seguridad de ESET estén activados.

VI. Migre los dispositivos móviles

VII. Configure usuarios de ESET PROTECT en ESET Business Account.

VIII. Agregue usuarios de ESET Business Account a ESET PROTECT Web Console.

IX. Retire ESET PROTECT Server local.

Después de migrar correctamente a ESET PROTECT, retire ESET PROTECT Server.

Si mantiene ESET PROTECT Server local, desactive la tarea Eliminar ordenadores que no se conecten para evitar la posible desactivación de los productos de seguridad de ESET en los ordenadores administrados por ESET PROTECT.

Solución de problemas después de la migración

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

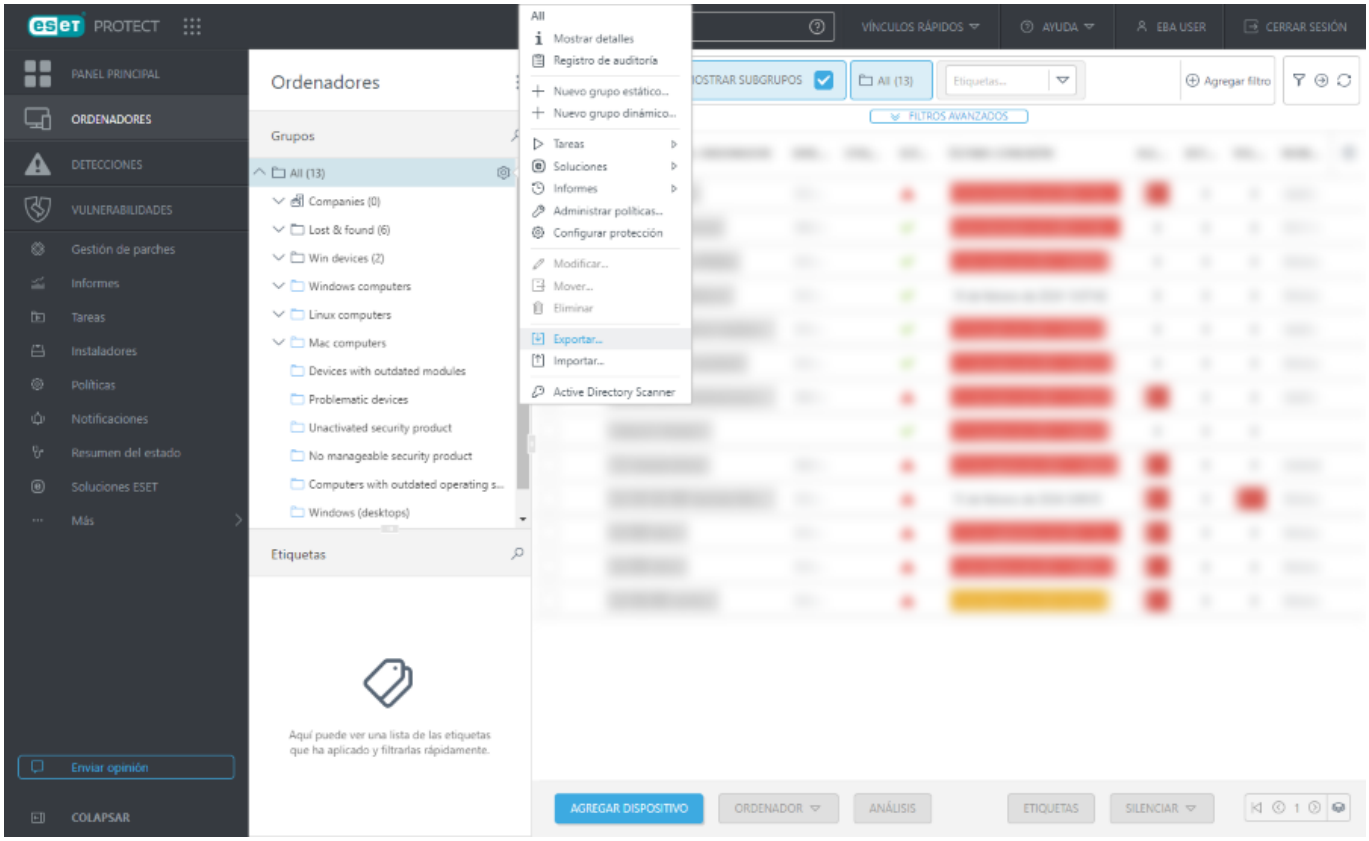
Migración en la nube: de un ESET PROTECT a otro ESET PROTECT

Siga los pasos que se indican a continuación para migrar de un ESET PROTECT (en adelante, **ESET PROTECT 1**) a otro ESET PROTECT (en adelante, **ESET PROTECT 2**) con la política de migración:

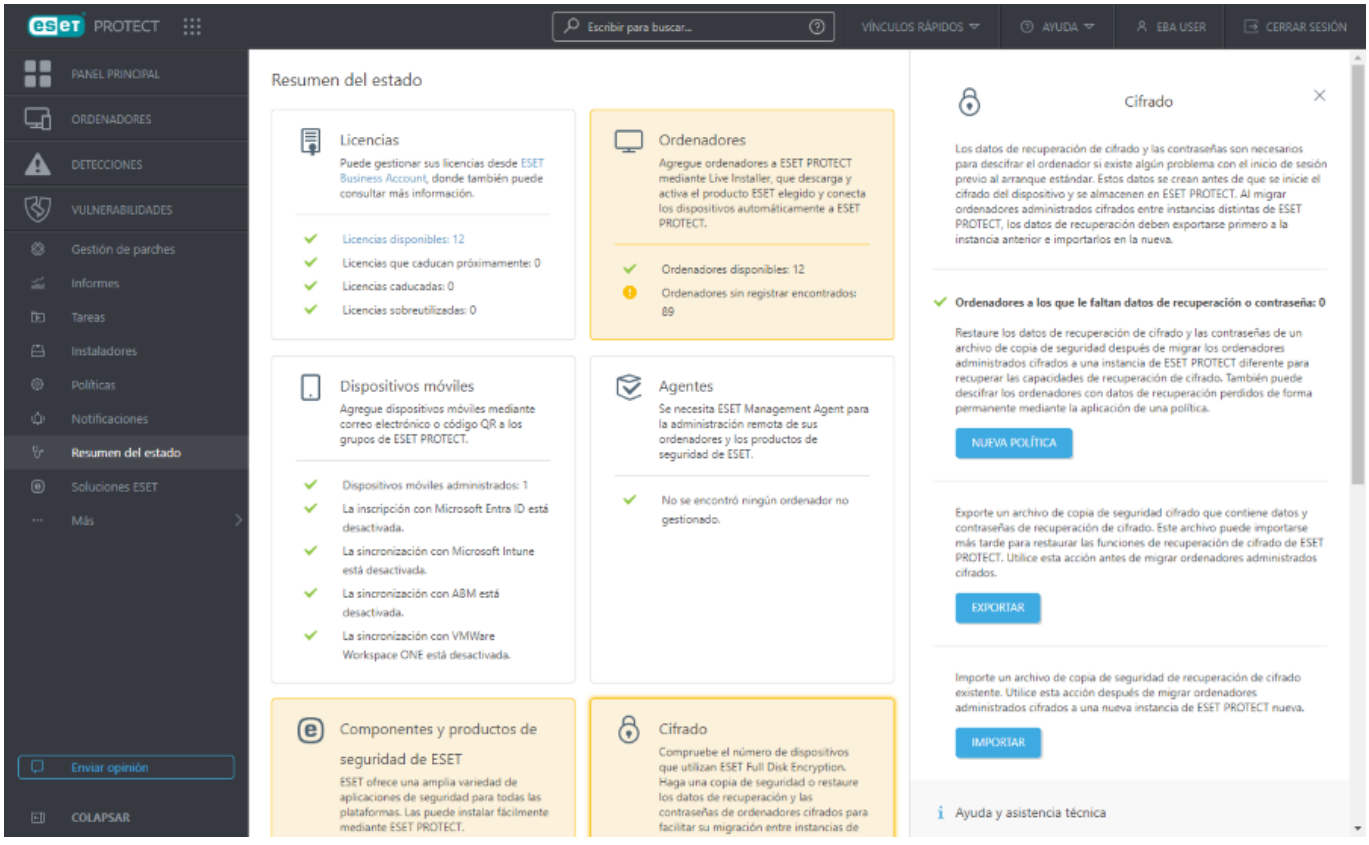
> **ESET PROTECT 1** contiene grupos estáticos personalizados, agentes de conexión de ESET Management, dispositivos administrados con productos de seguridad de ESET instalados y activados y dispositivos cifrados.

Se puede migrar:	No se puede migrar:
• Equipos administrados (agentes de ESET Management y conectores de ESET Inspect) • grupos estáticos • políticas • plantillas de grupos dinámicos • plantillas de informe	• toda la base de datos • grupos dinámicos (pero puede migrar plantillas de grupos dinámicos) • detecciones • registros de auditoría • notificaciones • tareas y disparadores • instaladores • informes programados/generados (pero puede migrar plantillas de informes) • etiquetas • dispositivos móviles (puede volver a inscribirlos)

1. **ESET PROTECT 1**: haga clic en **Equipos** > icono de engranaje situado junto al grupo estático **Todos** > **Exportar** > **Sí** para exportar equipos de subgrupos. A continuación, guarde el archivo *TXT*.

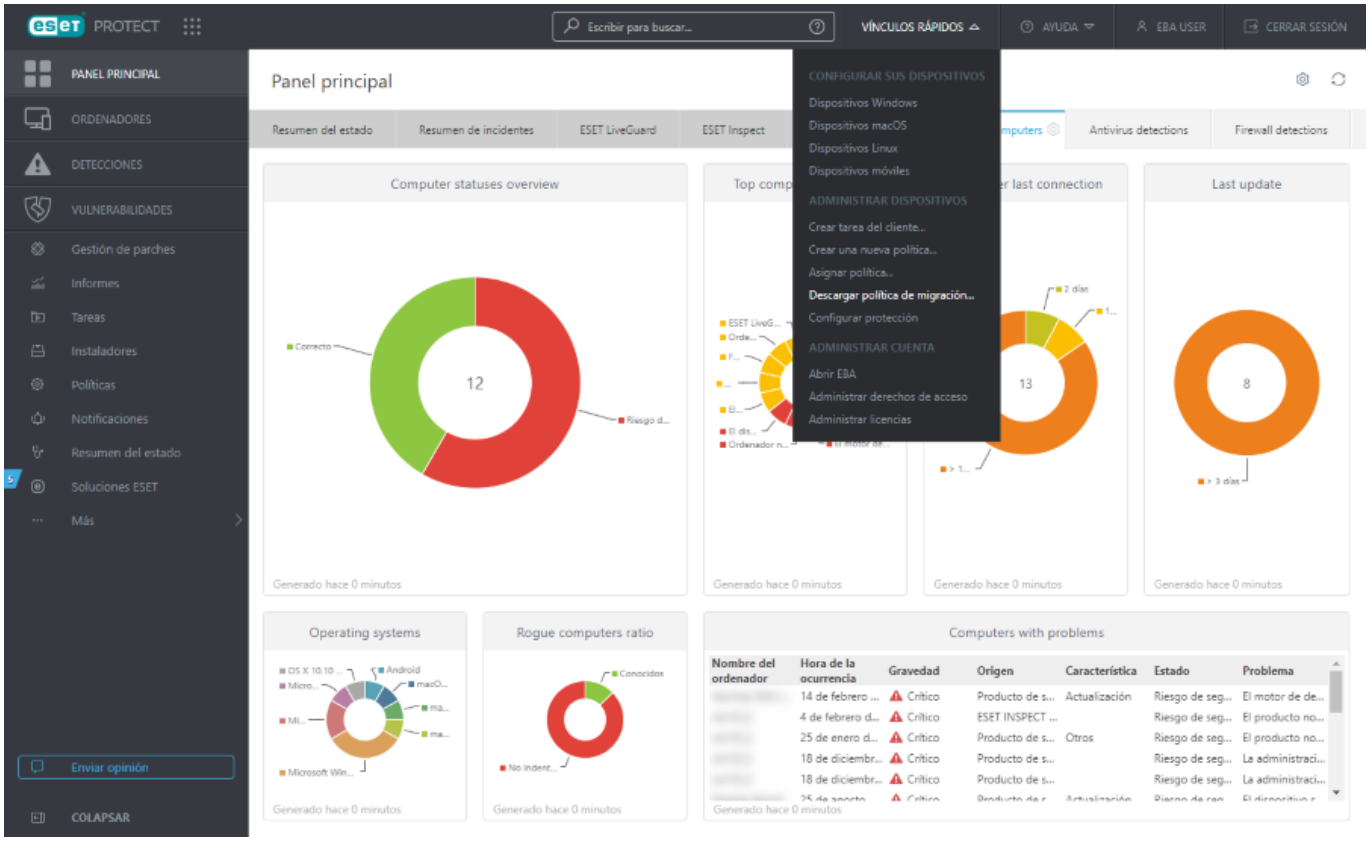


2. **ESET PROTECT 1**: haga clic en **Resumen del estado** > mosaico **Cifrado** > **Exportar** para exportar los datos de cifrado y las contraseñas. A continuación, guarde el archivo **efdeRecoveryExport.dat**.

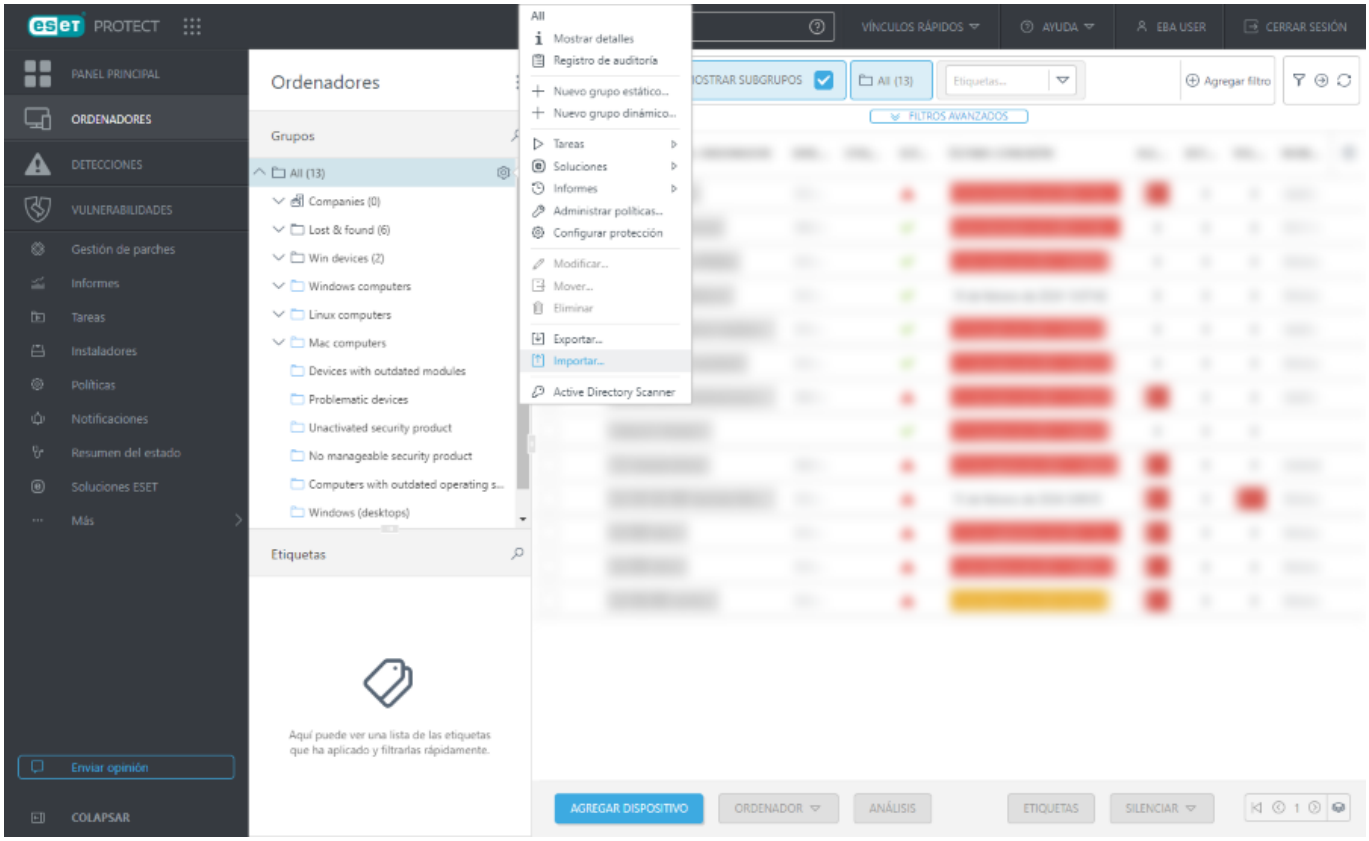


3. Cree un ESET PROTECT nuevo (**ESET PROTECT 2**).

4. **ESET PROTECT 2**: haga clic en **Enlaces rápidos** > **Descargar política de migración**. A continuación, guarde el archivo *CloudMigrationPolicy {timestamp}.dat*.



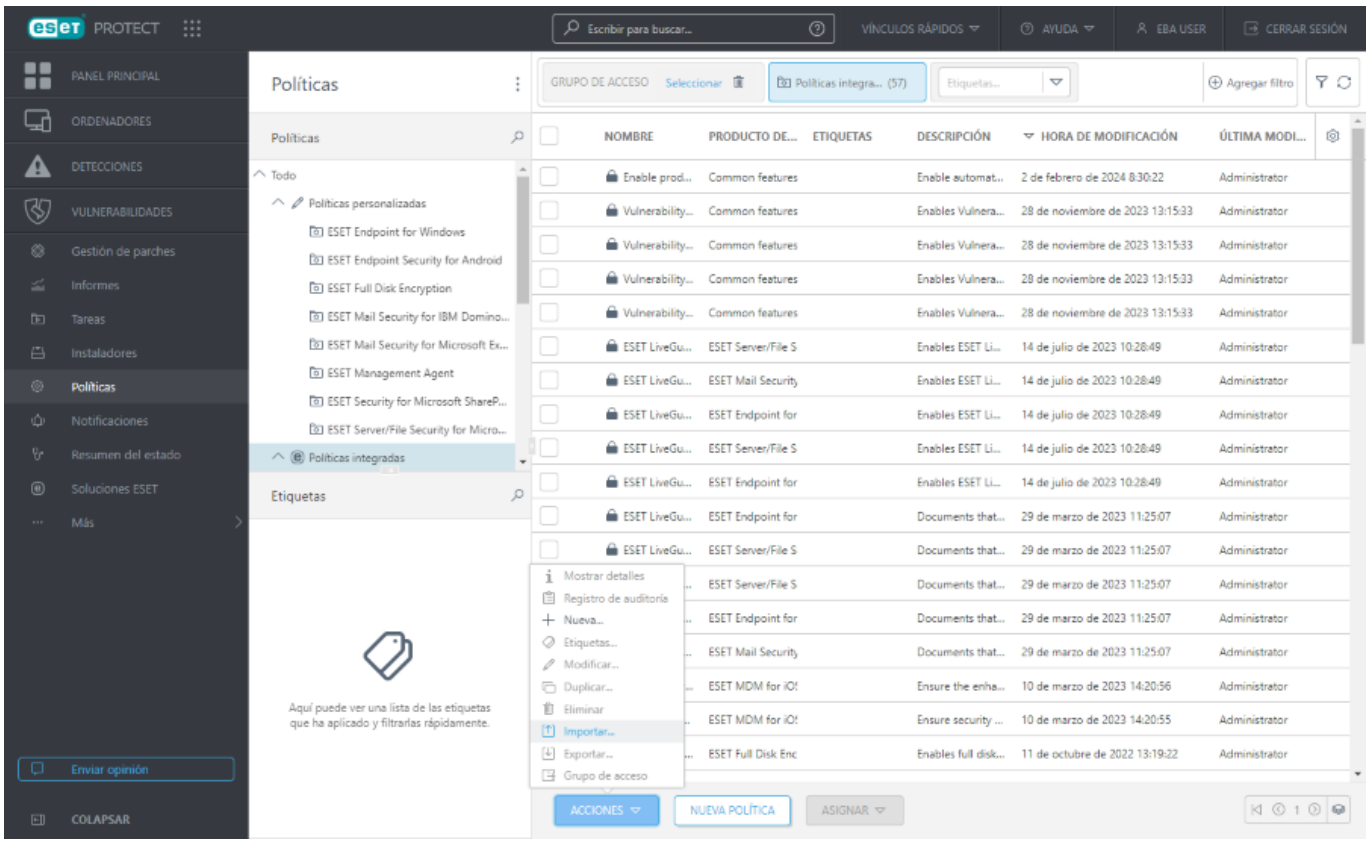
5. **ESET PROTECT 2**: haga clic en **Equipos** > icono de engranaje junto al grupo estático **Todos** > **Importar**. A continuación, importe los grupos estáticos con el archivo *TXT* exportado de **ESET PROTECT 1** en el paso 1 anterior.



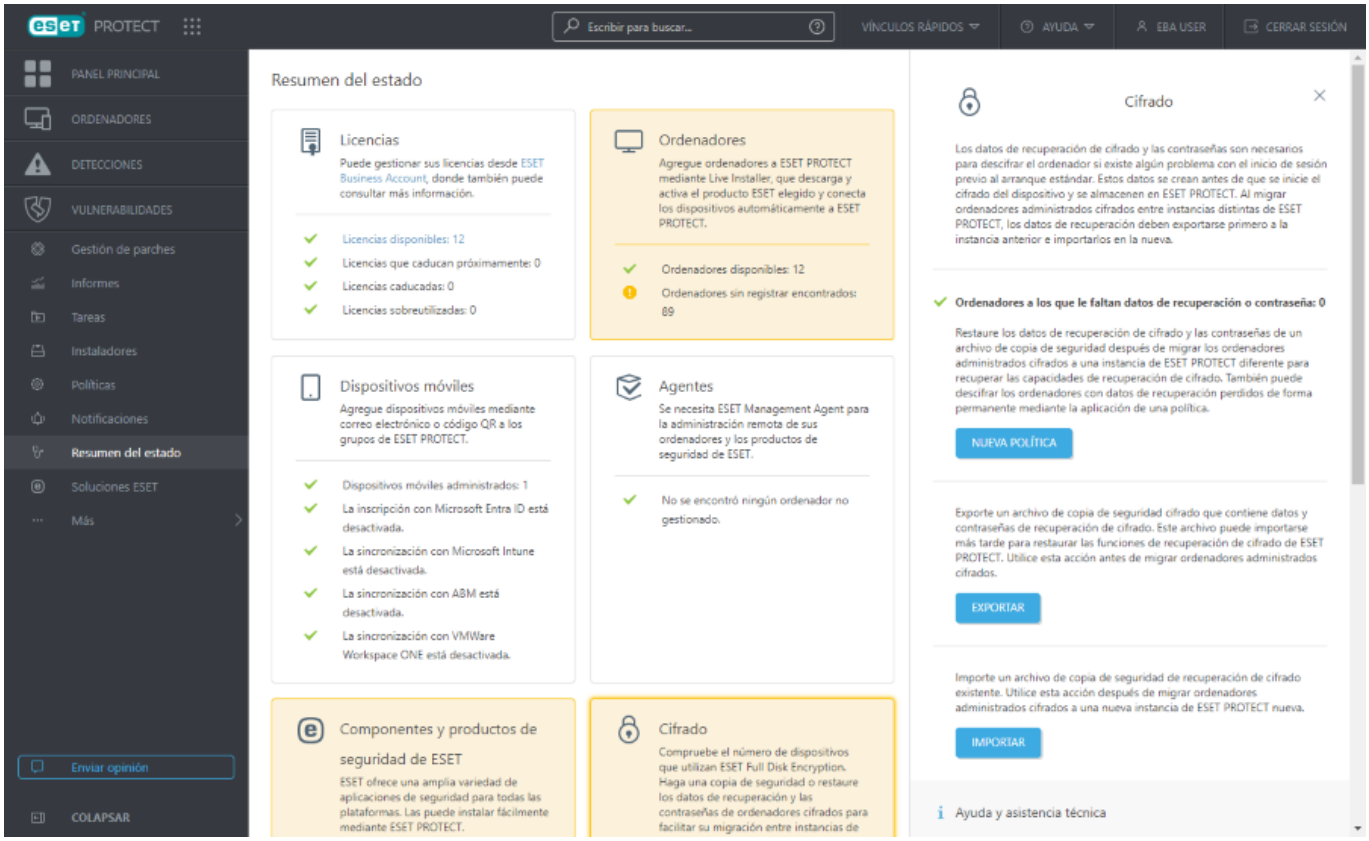
6. **ESET PROTECT 1**: haga clic en **Políticas** > **Acciones** > **Importar**. A continuación, importe el archivo de política de migración *DAT* exportado de **ESET PROTECT 2** en el paso 4 anterior y asigne la política de migración al

grupo estático **Todos**. Los equipos administrados se conectarán a **ESET PROTECT 2**.

> Si utiliza ESET Inspect, los conectores de ESET Inspect en los equipos administrados se conectarán al ESET Inspect nuevo.



7. **ESET PROTECT 2**: haga clic en **Resumen del estado** > mosaico **Cifrado** > **Importar**. A continuación, importe los datos de cifrado y las contraseñas del archivo *DAT* exportado de **ESET PROTECT 1** en el paso 2 anterior.



8. Al igual que en la migración de ESET PROTECT On-Prem a ESET PROTECT, migre de **ESET PROTECT** 1 a **ESET PROTECT 2** para:

   - políticas
   - plantillas de grupos dinámicos
   - plantillas de informe

> **Migración de dispositivos móviles**
> Para migrar los dispositivos móviles administrados, anule la inscripción en **ESET PROTECT 1** e inscríbalos en **ESET PROTECT 2**.

Cómo eliminar ESET PROTECT de la red

Hay dos formas correctas de dejar de administrar su red con ESET PROTECT:

a) Elimine completamente todos los productos de seguridad de ESET y ESET Management Agents y, a continuación, retire la instancia de ESET PROTECT.

b) Continúe utilizando los productos de seguridad de ESET, pero elimine ESET Management Agent y la instancia de ESET PROTECT. (En este caso, vaya a Eliminar ESET Management Agent a continuación).

Eliminar los productos de seguridad de ESET de su red

1. Restablezca los ajustes predeterminados o desbloquee los ajustes del cliente en las políticas.

   a. Elimine todas las **Políticas personalizadas** que se apliquen a los clientes.

b.En todas las **Políticas integradas**, seleccione la política y haga clic en la pestaña **Clientes** para ver si alguna de estas políticas está asignada a los ordenadores de su red.

2. Restablezca el valor predeterminado de la configuración de la contraseña en los clientes.

a.Cree una nueva política y vaya a **Política del producto de seguridad > Interfaz de usuario > Configuración del acceso**.

b.Deje los **Ajustes de contraseña protegida** desactivados y utilice use **Forzar** junto al ajuste **Establecer contraseña**.

c.Asigne esta política a todos los dispositivos de su red. Esto eliminará la protección por contraseña de la configuración avanzada de sus productos de seguridad Endpoint.

3. Descifre todas las estaciones de trabajo cifradas con ESET Full Disk Encryption.

Si alguna estación de trabajo sigue cifrada después de eliminar la instancia de ESET PROTECT, no hay otra forma de descifrar la estación de trabajo (si no ha descargado anteriormente los datos de recuperación de cifrado). Ni siquiera ESET puede ayudar en este caso.

4. Elimine el producto de seguridad de los dispositivos cliente si lo desea. Puede dejar los productos de seguridad instalados, seguirán proporcionando protección aunque no se administren.

Para desinstalar todos los productos de seguridad de su red, utilice la tarea Desinstalación del software.

a.Vaya a **Tareas** > **Nuevo**.

b.En el asistente de creación de tarea, en la sección **Básico**, escriba el Nombre y la Descripción y seleccione **Desinstalación de software** en el menú desplegable **Tarea**.

c.En la sección **Configuración**, seleccione la aplicación que desee desinstalar en el menú desplegable **Desinstalar**. En **Nombre del paquete**, haga clic en **Seleccionar paquete para desinstalar**, seleccione el producto de seguridad que quiera desinstalar y haga clic en **Aceptar**.

d.En **Versión del paquete**, haga clic en **Desinstalar todas las versiones del paquete** para evitar problemas al desinstalar diferentes versiones de productos de seguridad en ordenadores cliente de su red.

e.Marque la casilla situada junto a **Reiniciar automáticamente cuando sea necesario** para asegurarse de que el proceso de desinstalación haya finalizado por completo y, a continuación, haga clic en **Finalizar** para crear la tarea.

f.Haga clic en **Crear desencadenador** para seleccionar un destino para la tarea. Haga clic en **Agregar grupos** y seleccione el grupo **Todos** como destino. Seleccione el desencadenador adecuado y haga clic en **Finalizar** para ejecutar.

Verifique que la tarea se haya ejecutado correctamente en todos los dispositivos y repita el proceso para cada tipo de producto de seguridad de su red.

Eliminar ESET Management Agent de su red.

Para eliminar todos ESET Management Agents de su red de la forma más eficiente, verifique que todos los dispositivos afectados estén encendidos y conectados a ESET PROTECT.

1. Revierta el ajuste de configuración protegida por contraseña (solo Windows).

   a.Cree una nueva política para ESET Management Agent.

   b.Vaya a **Configuración avanzada** y, en **Configuración**, seleccione el indicador **Forzar** junto al ajuste **Configuración de la protección por contraseña**.

   c.Asigne la política al grupo **Todos** y haga clic en **Finalizar** para aplicar.

2. Verifique que la política se haya aplicado. Una vez aplicada correctamente la política en todos los clientes, elimine ESET Management Agent de los ordenadores de su red. Para ello, puede utilizar la tarea Detener administración (desinstalar ESET Management Agent). Asigne la tarea a todos los ordenadores de su red.

3. Espere a que la tarea se ejecute en todos los dispositivos de su red.

4. Quite todos los dispositivos de la sección **Ordenadores** de ESET PROTECT.

Si ninguno de los dispositivos vuelve a aparecer en la consola durante los diez minutos siguientes, ha eliminado correctamente todas las instancias de ESET Management Agent de su red.

Eliminar la instancia de ESET PROTECT

1. Abra su cuenta de ESET Business Account.

2. En la sección del **panel** principal, vaya a la ventana dinámica ESET PROTECT.

3. Haga clic en el icono del engranaje en la ventana dinámica ESET PROTECT y seleccione **Eliminar ESET PROTECT**.

4. Escriba su contraseña y haga clic en **Eliminar**. Su instancia de ESET PROTECT se eliminará.

Caducidad de la última licencia de ESET PROTECT

En este tema se describen los siguientes casos relacionados con las licencias:

- Qué ocurre con una instancia de ESET PROTECT antes y después de que caduque la última licencia válida de ESET PROTECT.
- Qué ocurre después de eliminar de ESET PROTECT la última licencia válida de ESET Business Account.

¿Qué ocurre con una instancia de ESET PROTECT antes y después de que caduque la última licencia válida de ESET PROTECT?

Cuando su licencia esté a punto de caducar, verá una alerta en la interfaz de ESET Business Account.

- Si pasa la fecha de caducidad y no ha renovado su licencia ni ha activado una nueva licencia, verá una alerta de licencia caducada en ESET Business Account.

- Si no hay ninguna licencia válida, se mostrará en ESET Business Account una notificación de que su licencia se suspenderá dentro de catorce días y recibirá un mensaje de correo electrónico en la dirección

especificada en su cuenta de administrador.

Contará con un periodo de gracia de catorce días para renovar la licencia después de que esta haya caducado. Recibirá una notificación en ESET Business Account y por correo electrónico cuando haya transcurrido la mitad del periodo de gracia. Después de catorce días, se suspenderá su uso de ESET PROTECT.

No podrá acceder a la instancia, que tampoco funcionará. La instancia de ESET PROTECT suspendida se almacenará y podrá acceder a ella de nuevo si agrega una nueva licencia válida de ESET PROTECT en ESET Business Account. **Su instancia de ESET PROTECT puede permanecer suspendida hasta 30 días, tras los que la instancia y todos los datos relacionados con ella se eliminarán de forma permanente**.

Si su instancia se suspende, recibirá una notificación en ESET Business Account y por correo electrónico cuando queden catorce días para que se elimine dicha instancia. Debe activar una nueva licencia válida de ESET PROTECT para restaurar el acceso a su instancia de ESET PROTECT.

Qué ocurre después de eliminar de ESET PROTECT la última licencia válida de ESET Business Account.

Si no hay licencias válidas de ESET PROTECT en ESET Business Account, se suspenderá su instancia de ESET PROTECT.

No podrá acceder a la instancia, que tampoco funcionará. La instancia de ESET PROTECT suspendida se almacenará y podrá acceder a ella de nuevo si agrega una nueva licencia válida de ESET PROTECT en ESET Business Account. **Su instancia de ESET PROTECT puede permanecer suspendida hasta 30 días, tras los que la instancia y todos los datos relacionados con ella se eliminarán de forma permanente**.

Si su instancia se suspende, recibirá una notificación en ESET Business Account y por correo electrónico cuando queden catorce días para que se elimine dicha instancia. Debe activar una nueva licencia válida de ESET PROTECT para restaurar el acceso a su instancia de ESET PROTECT.

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

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 ofrece una actualización automática de ESET Management Agent en ordenadores administrados.

Cómo funciona la actualización automática de ESET Management Agent

- La actualización automática del agente está activada de forma predeterminada y no se puede desactivar.
- 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 Actualizar agente.

- 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

ESET PROTECT incluye una función para mantener los productos de seguridad de ESET actualizados a la versión más reciente en sus ordenadores administrados.

Las actualizaciones automáticas del producto se activa automáticamente en una nueva instalación de ESET PROTECT.

- 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

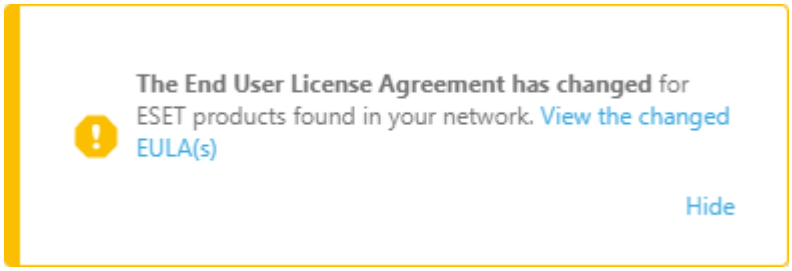
Diferencias entre la tarea del cliente Instalación de software y la función Actualizaciones automáticas:

	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.

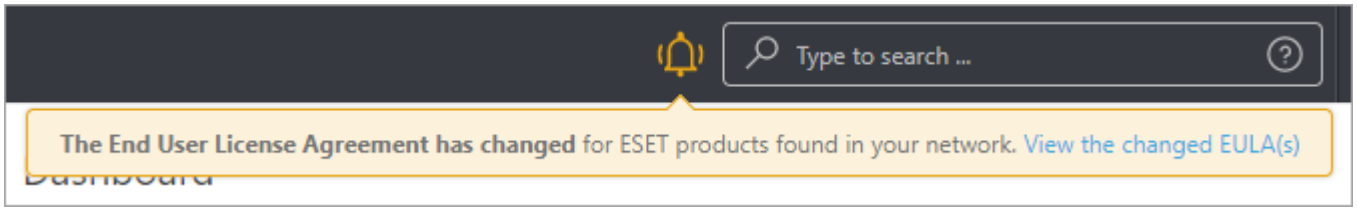
	Proceso de actualización	Reiniciar tras la actualización	Futuras actualizaciones
Actualizaciones automáticas	El proceso de actualización no incluye la reinstalación del producto de seguridad de ESET.	Para actualizar el producto de seguridad de ESET hay que reiniciar el ordenador, pero no inmediatamente (el reinicio no se fuerza). El administrador de ESET PROTECT 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.

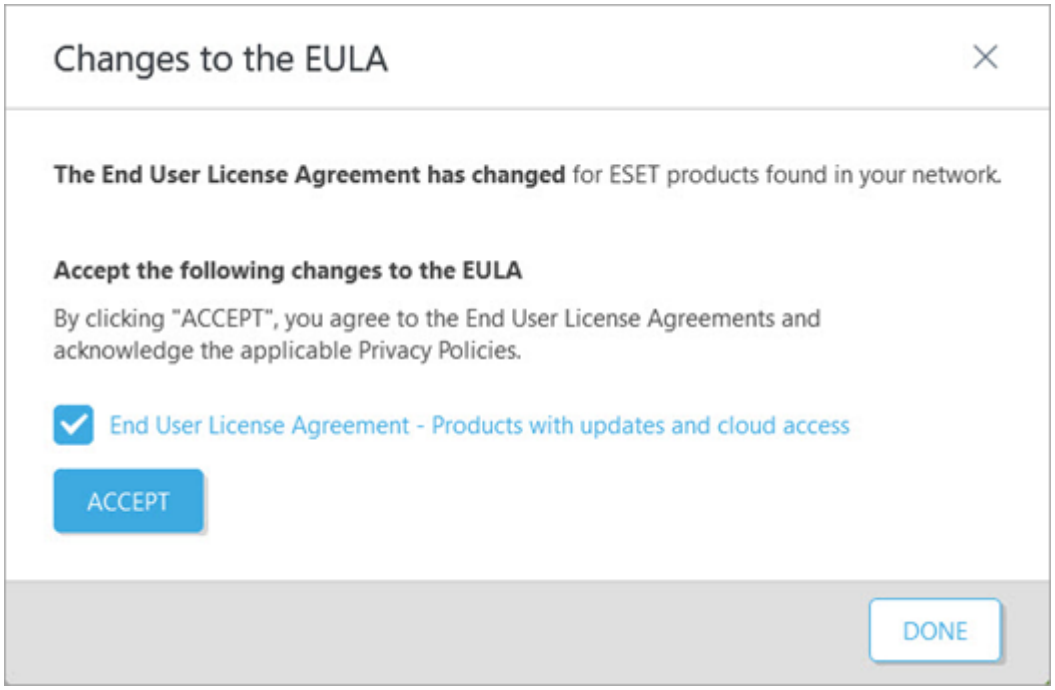


Haga clic en **Ver los EULA modificados** para ver los detalles o en **Ocultar** para mover la notificación situada bajo un icono de campana amarillo en la barra de herramientas superior.

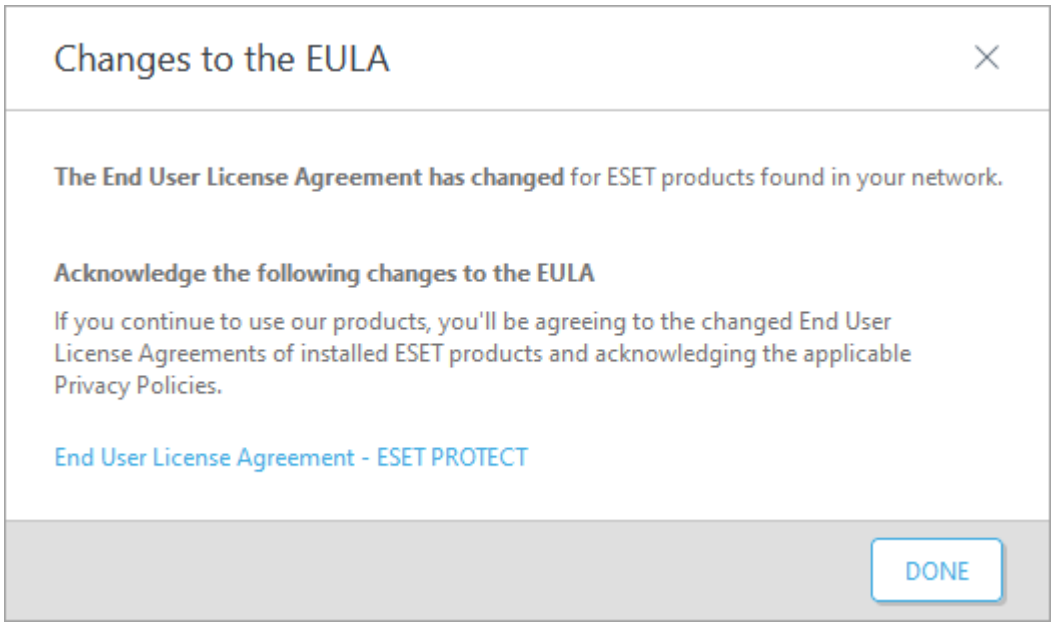


Cuando hace clic en **Ver los EULA modificados**, aparece una nueva ventana con detalles sobre el producto de seguridad de ESET y los cambios de su EULA:

- 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**.

Acerca de ESET PROTECT

Para abrir la ventana **Acerca de**, desplácese hasta **Ayuda** > **Acerca de**. Esta ventana contiene detalles acerca de la versión de ESET PROTECT. En la parte superior de la ventana se muestra información sobre el número de dispositivos cliente conectados y el número de licencias activas.

Cuando se ponga en contacto con el servicio de asistencia técnica de ESET, identifique su instancia de ESET PROTECT con el número UUID de su instancia de ESET PROTECT. Puede consultar el número UUID de su instancia en **Ayuda** > **Acerca de** > **ID**, o en el portal de **ESET Business Account** o **ESET MSP Administrator** en **Ayuda** > **Acerca de** > **ID de ESET PROTECT**.

ESET Connect (API)

ESET Connect es una puerta de enlace de REST API entre un cliente y una colección de servicios backend de ESET. ESET Connect actúa como un proxy inverso para aceptar todas las llamadas a la interfaz de programación de aplicaciones (API), agregar los servicios necesarios para atenderlas y devolver el resultado adecuado.

Las API de ESET y las integraciones de API creadas sobre la puerta de enlace de API permiten la automatización de las actividades de supervisión, seguridad y administración.

ESET Connnect solo está disponible en inglés.
Para obtener más información, consulte la ayuda en línea de ESET Connect.

Preguntas frecuentes sobre Administración de revisiones y vulnerabilidades

A continuación, encontrará las preguntas frecuentes relacionadas con la Gestión de parches y vulnerabilidades (V&PM):

Lista de aplicaciones

¿Con qué frecuencia se actualiza la lista de aplicaciones cubiertas por Vulnerabilidades?	• V&PM puede detectar el software recientemente agregado según la base de datos actualizada varias veces a la semana. • La lista se actualiza diariamente según los datos del proveedor.
¿Se analizan en Vulnerabilidades las aplicaciones que no están incluidas en la lista de aplicaciones compatibles?	No, la lista es definitiva. Las aplicaciones que no estén incluidas en la base de datos no se detectarán.
¿V&PM muestra y aplica revisiones solo a versiones de aplicaciones vulnerables anteriores, o también puede aplicar revisiones a versiones de aplicaciones no vulnerables que se acaban de quedar obsoletas?	V&PM no aplica parches a las aplicaciones que no son de CVE.

Política

¿Las **aplicaciones permitidas** y las **aplicaciones excluidas** en la política de **Funciones comunes** de V&PM se clasifican en función de las aplicaciones a las que se pueden aplicar revisiones automáticamente?	Se añaden a una lista de aplicaciones seguras o de aplicaciones denegadas para la administración de revisiones automáticas según la configuración de **Estrategia de aplicación automática de parches**.

Planificador de administración de revisiones y vulnerabilidades

¿Cómo se activa exactamente el análisis de V&PM?	El planificador de V&PM activa el análisis de V&PM una vez al día en función de la configuración que realiza el administrador en la política.
¿Qué sucede durante el periodo de tiempo seleccionado?	El análisis se realiza una vez al día en ese intervalo de tiempo especificado. El análisis se inicia cuando se enciende un ordenador dentro de este intervalo de tiempo.
¿Están interconectadas una tarea de análisis y una tarea de revisión? A las 15:50, configuraré el planificador para que se inicie de 16:00 a 19:00. ¿Activará solo una tarea de análisis o también una tarea de revisión? Si solo se activa una tarea de análisis a las 16:00, ¿cuándo se activará la siguiente tarea de revisión?	El análisis y la revisión no están interconectados. Si son las 15:50 y aplica la política, el análisis se ejecutará a las 16:00 y la revisión se ejecutará a una hora aleatoria entre las 16:30 y las 18:30. Pero si está fuera del periodo de mantenimiento, la revisión automática se ejecutará a la siguiente vez. Administración de revisiones no aplica revisiones fuera de ese horario.
Si un ordenador se enciende a las 19:00, ¿se activará inmediatamente la tarea de análisis/revisión o esperará hasta las 9:00? ¿Está configurado en la tarea del planificador que si se salta la hora programada, la revisión se inicie inmediatamente después?	Si según la configuración de la política esas tareas deben ejecutarse entre las 17:00 y las 9:00, y abre el ordenador a las 19:00, el análisis se ejecutará lo antes posible, y también se ejecutará una revisión solo si la hora seleccionada aleatoriamente cuando se creó esa tarea es anterior a las 19:00; si no, esperará a la hora seleccionada.
Si no se establece un planificador en una política, ¿cuándo se activarán el análisis y la aplicación de revisiones? La política preestablecida es de 17:00 a 09:00. ¿Significa que el análisis/revisión se activará a las 17:00 + 30 minutos o a las 9:00 - 30 minutos si no hay una política establecida?	Sí, el intervalo de tiempo programado es el mismo que el de la política preestablecida de 17:00 a 9:00.
¿Cómo y cuándo se activa exactamente una actualización de aplicaciones (cuando la disponibilidad en el planificador está configurada para todos los días y todo el ciclo de 24 horas)?	La revisión automática es una tarea que ejecuta el planificador, pero el tiempo de ejecución es un valor aleatorio entre la **hora de inicio** + 30 minutos y la **hora de finalización** - 30 minutos. Ejemplo: el administrador establece la hora de inicio del lunes del planificador para la 1:00 a.m. y la hora de finalización para las 11:00 a.m. Cuando la política se aplica en un punto de acceso, tenemos un algoritmo que crea la tarea de revisión automática para el planificador seleccionando un valor aleatorio entre la 1:30 a.m. y las 10:30 a.m. Por ejemplo, si se selecciona 4:21 a.m., significa que la revisión automática se ejecutará todos los lunes a las 4:21 a.m. También se utiliza el mismo flujo cuando se seleccionan todos los días y la hora de inicio es entre 0:00 a.m. y 12:00 p.m. (24h). Se selecciona un valor entre esas horas. Por ejemplo, si se selecciona 1:23 p.m., todos los días la revisión automática se ejecutará a la 1:23 p.m.

¿El momento del análisis depende de la configuración del planificador de V&PM (por ejemplo, se puede forzar el análisis manualmente editando la configuración del planificador), o solo el planificador determina el momento en que se aplica la revisión?	El análisis no se puede forzar manualmente. Lo ejecuta solo el planificador.
¿Hay un tiempo establecido para el análisis, o el intervalo de tiempo es aleatorio?	La tarea de análisis se ejecuta en los días de la semana seleccionados y se utiliza el valor de la hora de inicio. Por ejemplo, si se selecciona lunes y viernes con **hora de inicio** 1:00 a.m. y **hora de finalización** 11:00 a.m., el análisis se ejecutará el lunes a la 1:00 a.m. y el viernes a la 1:00 a.m.

Proceso

¿En la página Vulnerabilidades aparecen las vulnerabilidades del sistema operativo?	V&PM puede detectar tanto las vulnerabilidades de las aplicaciones como las vulnerabilidades del sistema operativo.
¿Cómo se realiza el análisis?	No se realizan comprobaciones activas de explotabilidad. Las versiones del software instalado se comparan con las que figuran en la base de datos como vulnerables.
Cuando la tarea de aplicación de revisiones indica que ha finalizado, ¿qué significa? ¿Que se ha aplicado correctamente la revisión al equipo o que se ha enviado correctamente la solicitud de aplicación de revisiones? ¿Por qué aparece que las tareas de actualización se han aplicado correctamente si en realidad no se ha aplicado ninguna revisión?	El producto de punto de acceso inicia el comando en el sistema operativo. No hay otra forma de rastrear los resultados de la operación msiexec, por lo que si el comando se transmite correctamente, la tarea indica que ha finalizado correctamente.
¿ELC y registros de diagnóstico?	Para recopilar registros avanzados de V&PM: 1.Presione F5 > haga clic en Herramientas > Diagnóstico > Activar registro avanzado de Administración de revisiones y vulnerabilidades para activar el registro de diagnóstico de V&PM. 2.Reproduzca el problema. 3.Deshabilite el registro avanzado (de lo contrario, los datos recopilados no se escribirán en el registro). 4.Recopile registros de ELC + SysInspector con ELC 4.9.0 y versiones posteriores.
¿Dónde puedo encontrar un informe de revisiones aplicadas y fallidas?	Puede crear un informe con la lista de ordenadores con pares CVE/revisión, pero actualmente no puede crear un informe de tareas con errores, ni siquiera para ver los resultados de las tareas en las que se realiza la aplicación de revisiones en un sistema operativo y también los registra el sistema operativo.
¿Cuánto tiempo tarda en aplicarse en el punto de acceso un comando de actualización manual para aplicar una revisión a una aplicación?	La revisión manual se realizará en cuanto el agente se conecte. El comando Actualizar creará una tarea Aplicar revisión de aplicación que se activa inmediatamente.

Si el reinicio se produce cuando aún no se han aplicado todas las revisiones, ¿continuará el proceso después del reinicio?	Solo tenemos una tarea de parches que itera a través de todas las aplicaciones y parches uno por uno. Si uno de ellos requiere un reinicio, el mensaje de reinicio se muestra una vez finalizada la iteración. El reinicio no se produce sin notificaciones ni durante la iteración a lo largo de la lista de aplicaciones a las que se deben aplicar revisiones. Aunque algunas aplicaciones se reiniciarán directamente después de aplicarse las revisiones sin informarnos de que es necesario un reinicio, y ya tenemos un ticket abierto, esto no debería suceder. Pero si se reinicia, la aplicación de revisiones no continuará desde donde se quedó, incluso si estamos en el intervalo de tiempo correcto. Se ejecutará la siguiente vez.
¿Hay alguna forma de instalar una versión específica de las aplicaciones? ¿No solo la versión más reciente?	No se pueden aplicar revisiones al software compatible solo a la versión más reciente.
¿Cómo será la descarga de los paquetes de instalación de revisiones? ¿Los alojará ESET o se almacenarán en caché?	Descarga directa solo desde el equipo de punto de acceso.
¿El reinicio del ordenador tiene algún efecto en la actualización de la aplicación/administración de revisiones?	No, el reinicio solo es necesario si la aplicación de revisiones al final de la revisión requiere un reinicio y, en este caso, notificaremos al usuario que es necesario reiniciar.

Seguridad para ESET PROTECT

Introducción

La finalidad de este documento es resumir los controles y prácticas de seguridad que se aplican en ESET PROTECT Cloud. Los controles y prácticas de seguridad están diseñados para proteger la confidencialidad, integridad y disponibilidad de la información del cliente. Tenga en cuenta que los controles y prácticas de seguridad pueden cambiar.

Alcance

En este documento se resumen los controles y prácticas de seguridad para la infraestructura, organización, personal y procesos operativos de ESET MSP Administrator (en adelante, "EMA"), ESET Business Account (en adelante, "EBA"), y la infraestructura de ESET PROTECT Cloud. Entre los controles y prácticas de seguridad se incluyen los siguientes:

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información
3. Seguridad de recursos humanos
4. Administración de activos
5. Control de acceso
6. Cifrado
7. Seguridad física y ambiental
8. Seguridad de las operaciones
9. Seguridad de la comunicación
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Relación con proveedores

12. Gestión de incidentes de seguridad de la información
13. Aspectos de seguridad de la información de la gestión de la continuidad de la actividad
14. Cumplimiento

Concepto de seguridad

La empresa ESET s.r.o. cuenta con la certificación ISO 27001:2013, con un alcance del sistema de administración integrado que abarca explícitamente los servicios de ESET PROTECT Cloud, EBA y EMA.

Por lo tanto, el concepto de seguridad de la información utiliza el marco de ISO 27001 para implementar una estrategia de seguridad por capas al aplicar controles de seguridad en las capas de red, sistemas operativos, bases de datos, aplicaciones, personal y procesos operativos. El objetivo de los controles y las prácticas de seguridad aplicables es superponerse y complementarse entre sí.

Controles y prácticas de seguridad

1. Políticas de seguridad de la información

ESET utiliza políticas de seguridad de la información para cumplir todos los aspectos de la norma ISO 27001, incluidos los controles y prácticas de seguridad, así como la gobernanza de la seguridad de la información. Las políticas se revisan anualmente y se actualizan tras cambios importantes para garantizar su conveniencia, adecuación y eficacia continuas.

ESET efectúa revisiones anuales de esta política y comprobaciones de seguridad interna para garantizar la coherencia con esta. El incumplimiento de las políticas de seguridad de la información puede acarrear medidas disciplinarias para los empleados de ESET y sanciones contractuales, incluida la rescisión del contrato, en el caso de los proveedores.

2. Organización de la seguridad de la información

La organización de la seguridad de la información de ESET PROTECT Cloud se compone de varios equipos y personas implicados en la seguridad de la información y la TI, entre otros los siguientes:

- Administración ejecutiva de ESET
- Equipos de seguridad interna de ESET
- Equipos de TI de aplicaciones empresariales
- Otros equipos de apoyo

Las responsabilidades de seguridad de la información se asignan de acuerdo con las políticas de seguridad de la información establecidas. Los procesos internos se identifican y evalúan para determinar si hay riesgo de uso indebido o modificación no autorizada o involuntaria de los activos de ESET. Las actividades riesgosas o delicadas de los procesos internos adoptan el principio de segregación de controles para mitigar el riesgo.

El equipo jurídico de ESET es responsable de la comunicación con las autoridades gubernamentales, incluidas las entidades reguladoras eslovacas dedicadas a la seguridad informática y la protección de datos personales. El equipo de seguridad interna de ESET es responsable de la comunicación con grupos de interés especiales, como ISACA. El equipo del laboratorio de investigación de ESET es responsable de la comunicación con otras empresas de seguridad y la comunidad de seguridad informática en general.

La seguridad de la información se integra en la gestión de proyectos mediante el marco de gestión de proyectos aplicado desde la concepción hasta la finalización del proyecto.

El teletrabajo se asegura mediante una política implementada en los dispositivos móviles que incluye protección de datos mediante cifrado seguro al atravesar redes que no son de confianza. Los controles de seguridad de los dispositivos móviles están diseñados para funcionar independientemente de los sistemas internos y las redes internas de ESET.

3. Seguridad de recursos humanos

ESET utiliza prácticas estándar de recursos humanas, como políticas diseñadas para proteger la seguridad de la información. Estas prácticas abarcan todo el ciclo de vida de los empleados y se aplican a todos los equipos que acceden al entorno de ESET PROTECT Cloud.

4. Administración de activos

La infraestructura de ESET PROTECT Cloud está incluida en los inventarios de activos de ESET con estrictos controles de propiedad y reglas que se aplican según el tipo y la sensibilidad del activo. ESET tiene un esquema de clasificación interno definido. Todos los datos y configuraciones de ESET PROTECT Cloud se clasifican como confidenciales.

5. Control de acceso

El acceso a ESET PROTECT Cloud se rige por la política de control de acceso de ESET. El control de acceso se establece en la infraestructura, los servicios de red, el sistema operativo, la base de datos y el nivel de la aplicación. La administración del acceso total de los usuarios a nivel de la aplicación es autónoma. El inicio de sesión único de ESET PROTECT Cloud y ESET Business Account se rige por un proveedor de identidad central, que garantiza que un usuario solo pueda acceder al inquilino autorizado. La aplicación utiliza permisos de ESET PROTECT Cloud estándar para aplicar control de acceso basado en roles para el inquilino.

El acceso al backend de ESET está estrictamente limitado a las personas y roles autorizados. Los procesos estándar de ESET para el (des)registro, (des)aprovisionamiento, administración de privilegios y revisión de derechos de acceso de los usuarios se utilizan para administrar el acceso de los empleados de ESET a la infraestructura y las redes de ESET PROTECT Cloud.

Existe una autenticación segura para proteger el acceso a todos los datos de ESET PROTECT Cloud.

6. Cifrado

Con el fin de proteger los datos de ESET PROTECT Cloud, se utiliza un cifrado seguro para cifrar los datos en reposo y en tránsito. Por lo general, la autoridad certificadora de confianza se utiliza para emitir certificados para servicios públicos. La infraestructura de clave pública de ESET interna se utiliza para administrar las claves de la infraestructura de ESET PROTECT Cloud. Los datos almacenados en la base de datos están protegidos por claves de cifrado generadas en la nube. Todos los datos de copia de seguridad están protegidos por claves administradas de ESET.

7. Seguridad física y ambiental

Dado que ESET PROTECT Cloud y ESET Business Account están basados en la nube, utilizamos Microsoft Azure para la seguridad física y ambiental. Microsoft Azure utiliza centros de datos certificados con estrictas medidas de seguridad física. La ubicación física del centro de datos depende de la región seleccionada por el cliente. Se utiliza un cifrado seguro para proteger los datos del cliente durante el transporte fuera del sitio desde el entorno de la nube (por ejemplo, en tránsito hacia un almacén físico de datos de copia de seguridad).

8. Seguridad de las operaciones

El servicio de ESET PROTECT Cloud se presta por medios automatizados basados en estrictos procedimientos operativos y plantillas de configuración. Todos los cambios, como los cambios de configuración y la implementación de nuevos paquetes, se aprueban y prueban en un entorno de pruebas específico antes de la implementación en producción. Los entornos de desarrollo, pruebas y producción se separan entre sí. Los datos de ESET PROTECT Cloud se ubican solo en el entorno de producción.

El entorno de ESET PROTECT Cloud se somete a supervisión operativa para identificar rápidamente los problemas y proporcionar suficiente capacidad a todos los servicios de la red y los niveles de host.

Todos los datos de configuración se almacenan en nuestros repositorios con copia de seguridad periódica para garantizar la recuperación automática de la configuración de un entorno. Las copias de seguridad de los datos de ESET PROTECT Cloud se almacenan tanto en el sitio como fuera del sitio.

Las copias de seguridad se cifran y se someten a pruebas periódicas de recuperabilidad como parte de las pruebas de continuidad de la actividad.

La auditoría de los sistemas se lleva a cabo de conformidad con las normas y directrices internas. Se recopilan de forma continuada los registros y eventos de la infraestructura, el sistema operativo, la base de datos, los servidores de aplicaciones y los controles de seguridad. Los equipos de TI y seguridad interna procesan los registros para identificar anomalías operativas y de seguridad, e incidentes de seguridad de la información.

ESET utiliza un proceso general de administración de vulnerabilidades técnicas para gestionar la aparición de vulnerabilidades en la infraestructura de ESET, incluida la de ESET PROTECT Cloud y otros productos de ESET. Este proceso incluye un análisis proactivo de vulnerabilidades y pruebas reiteradas de penetración de la infraestructura, los productos y las aplicaciones.

ESET establece directrices internas para la seguridad de la infraestructura interna, las redes, los sistemas operativos, las bases de datos, los servidores de aplicaciones y las aplicaciones. Estas directrices se verifican mediante la supervisión del cumplimiento técnico y nuestro programa interno de auditoría de seguridad de la información.

9. Seguridad de la comunicación

El entorno de ESET PROTECT Cloud se somete a segmentación nativa de la nube, con acceso a la red limitado solo a los servicios necesarios entre los segmentos de red. La disponibilidad de los servicios de red se consigue mediante controles nativos de la nube, como zonas de disponibilidad, equilibrio de carga y redundancia. Se implementan componentes específicos de equilibrio de carga a fin de proporcionar equipos concretos para el enrutamiento de instancias de ESET PROTECT Cloud que exijan la autorización del tráfico y el equilibrio de carga. El tráfico de red se supervisa continuamente para detectar anomalías operativas y de seguridad. Los posibles ataques se pueden resolver mediante controles nativos de la nube o soluciones de seguridad implementadas. Todas las comunicaciones de red se cifran mediante técnicas generalmente disponibles, como IPsec y TLS.

10. Adquisición, desarrollo y mantenimiento de sistemas

El desarrollo de los sistemas de ESET PROTECT Cloud se realiza de conformidad con la política de desarrollo de software seguro de ESET. Los equipos de seguridad interna se incluyen en el proyecto de desarrollo de ESET PROTECT Cloud desde la fase inicial y supervisan todas las actividades de desarrollo y mantenimiento. El equipo de seguridad interna define y verifica el cumplimiento de los requisitos de seguridad en diferentes etapas del desarrollo de software. Todos los servicios, incluidos los que se han desarrollado recientemente, se someten a pruebas de seguridad continuas tras su lanzamiento.

11. Relación con proveedores

Las relaciones con proveedores relevantes se desarrollan de conformidad con las directrices válidas de ESET, que abarcan la gestión de toda la relación y los requisitos contractuales desde la perspectiva de la privacidad y la seguridad de la información. La calidad y seguridad de los servicios prestados por el proveedor de servicios críticos se evalúan periódicamente.

Además, ESET utiliza el principio de portabilidad para ESET PROTECT Cloud a fin de evitar el bloqueo de proveedores.

12. Administración de seguridad de la información

La gestión de incidentes de seguridad de la información en ESET PROTECT Cloud es similar a la de otras infraestructuras de ESET y se basa en procedimientos de respuesta a incidentes definidos. En la respuesta a incidentes, se definen y asignan funciones en múltiples equipos, como el jurídico, así como los de TI, seguridad, recursos humanos, relaciones públicas y administración ejecutiva. El equipo de respuesta a incidentes se establece función de la clasificación del incidente determinada por el equipo de seguridad interna. Este equipo estará a cargo de la coordinación del resto de equipos que gestionen el incidente. El equipo de seguridad interna también es responsable de la recopilación de pruebas y las lecciones aprendidas. Se notifica a las partes afectadas cuando ocurre el incidente y cuando se resuelve. El equipo jurídico de ESET es responsable de notificar a los organismos normativos en caso necesario de acuerdo con el Regulación General de Protección de Datos (RGPD) y la Ley de seguridad informática, por la que se transpone la Directiva de seguridad de las redes y la información (NIS).

13. Aspectos de seguridad de la información de la gestión de la continuidad de la actividad

La continuidad de la actividad del servicio de ESET PROTECT Cloud está codificada en la sólida arquitectura utilizada para maximizar la disponibilidad de los servicios proporcionados. Es posible restaurar totalmente componentes de ESET PROTECT Cloud o el servicio de ESET PROTECT Cloud a partir de datos de configuración y copia de seguridad fuera del sitio en caso de fallo catastrófico de todos los nodos redundantes. El proceso de restauración se prueba periódicamente.

14. Cumplimiento

El cumplimiento de los requisitos normativos y contractuales de ESET PROTECT Cloud se evalúa y revisa con regularidad, al igual que otros procesos e infraestructuras de ESET, y se toman las medidas necesarias para garantizar dicho cumplimiento en todo momento. ESET está registrado como proveedor de servicios digitales de informática en la nube y presta múltiples servicios, entre otros, ESET PROTECT Cloud. Tenga en cuenta que las actividades de cumplimiento de ESET no están destinadas a satisfacer los requisitos generales de cumplimiento de los clientes.

Términos de uso

Fecha de entrada en vigor: 29 de septiembre de 2023 | Consulte una versión anterior de los Términos de uso | Comparar cambios

Estos Términos de uso ("Términos") constituyen un acuerdo especial entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, número de registro: 31333532 ("ESET" o "Proveedor"), y usted, una persona física o jurídica ("Usted" o "Usuario") que accede a una cuenta de administración y a ESET PROTECT Cloud y que utiliza servicios en línea que ESET posee y presta ("Cuenta"), especificados en la documentación correspondiente, a la que se puede acceder desde la Ayuda en línea de ESET ("documentación").

Si utiliza la Cuenta en nombre de una organización, acepta estos Términos en nombre de dicha organización y garantiza que tiene autoridad para someter a la organización a estos Términos. Es ese caso, "Usted" y el "Usuario" se referirán a esa organización. Lea estos Términos atentamente. Se refieren también a los servicios prestados por ESET a través de la Cuenta o en relación con ella. Las condiciones específicas de uso de servicios concretos no incluidas en estos Términos se indican con cada servicio, y su aceptación forma parte del proceso de activación del servicio.

Seguridad y protección de datos

La Cuenta permite acceder a los servicios prestados por ESET. El nombre completo del usuario, el nombre de la empresa, la dirección de correo electrónico válida, el número de teléfono, los datos de licencias y las estadísticas son necesarios para el registro y el uso de la Cuenta y a efectos de la prestación y el mantenimiento de los servicios a los que se accede a través de la Cuenta. Acepta la recopilación de los datos y su transferencia a los servidores del Proveedor o de sus socios: los únicos fines de lo anterior son garantizar la funcionalidad y la autorización de uso del Software y la protección de los derechos del Proveedor. Cuando estos Términos dejen de estar en vigor, el Proveedor y sus socios podrán transferir, procesar y almacenar datos esenciales que lo identifiquen para fines relacionados con la asistencia y el cumplimiento de estos Términos. Solo está autorizado para utilizar la Cuenta con los fines y la forma que se mencionan en estos Términos, en los términos de servicio correspondientes y en la documentación.

Usted es el responsable de la seguridad de su Cuenta y las credenciales necesarias para iniciar sesión. ESET no es responsable de pérdidas o daños derivados del incumplimiento de esta obligación de garantizar la seguridad. El Usuario también es responsable de todas las actividades relacionadas con el uso de la Cuenta, autorizadas o no. Si la seguridad de la Cuenta se ve comprometida, debe informar al Proveedor inmediatamente.

Para proporcionar el servicio de administración de la Cuenta, es necesaria la recopilación de los datos relativos a los datos administrados junto con la información de administración (en lo sucesivo "Datos"). Usted proporciona los Datos con el único fin de recibir el servicio de administración de la Cuenta. Los Datos se proporcionarán y almacenarán de conformidad con las políticas y prácticas de seguridad de ESET, además de con la Política de privacidad.

Los datos, así como otros registros relacionados con la Cuenta, se almacenarán de acuerdo con la Política de retención de registros.

Puede obtener información detallada sobre la privacidad, la protección de los datos personales y sus derechos como persona interesada en la Política de privacidad.

Seguridad de datos de la API

Al utilizar la Interfaz de programación de aplicaciones (la "API"), Usted reconoce y acepta que cualquier dato o información transmitido a la API o recibido de ella puede salir de la infraestructura segura de ESET o entrar en ella. Esto incluye, por ejemplo, instrucciones, solicitudes, comandos o directivas recibidos de sistemas o redes de terceros. Usted comprende que ESET no puede garantizar la seguridad ni la confidencialidad de los datos o información transmitidos a la API o recibidos por ella, y que ESET no es responsable de accesos no autorizados, divulgaciones, pérdidas, daños o usos indebidos de dichos datos o información.

Usted declara y garantiza que ha implementado medidas de seguridad adecuadas para proteger tanto los datos y la información transmitidos a la API como las instrucciones recibidas de terceros mediante la API. Usted acepta que tiene responsabilidad exclusiva sobre la seguridad y la confidencialidad de los datos y la información una vez que salen de la infraestructura de ESET o entran en ella, y también sobre la interpretación y la ejecución de las instrucciones recibidas mediante la API. Usted reconoce que asume todos los riesgos asociados a la interacción de la API con sistemas o redes de terceros, lo que incluye, por ejemplo, el riesgo de interferencia malintencionada.

Directiva de uso correcto

El usuario está obligado a cumplir las limitaciones técnicas estipuladas en la documentación. Acepta que solo utilizará la Cuenta y sus funciones de manera que no se limiten las posibilidades de otros Usuarios de acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance de los servicios prestados a Usuarios concretos a fin de permitir que la máxima cantidad posible de Usuarios pueda utilizar los servicios. Limitar el alcance de los servicios significa también poner fin por completo a la posibilidad de utilizar cualquiera de las funciones de la Cuenta y eliminar datos e información.

El Proveedor también se reserva el derecho de limitar el número de dispositivos administrados en la Cuenta. Puede agregar y administrar hasta 50000 dispositivos terminales.

Limitación de uso

El uso de la Cuenta se limita a la gestión del producto activado con licencias aptas para la nube. ESET Full Disk Encryption solo se utilizará en los equipos con productos de seguridad instalados y activados mediante licencias aptas para la nube, o bien por separado sin exceder el número total de puestos de licencias aptas para la nube obtenidos. El Proveedor también se reserva el derecho de limitar el número de productos administrados en la Cuenta en caso de que Usted no respete esta limitación.

Ubicación

El Proveedor puede permitirle elegir una de las ubicaciones host disponibles para la Cuenta, incluida la ubicación recomendada elegida por el Proveedor. Reconoce que, si elige una ubicación distinta de la recomendada, su experiencia de Usuario puede verse afectada. En función de la ubicación elegida, podrían ser de aplicación el Acuerdo de protección de datos incluido en el Anexo n.º 2 de este Acuerdo y las Cláusulas contractuales tipo incluidas en el Anexo n.º 3 de este Acuerdo. ESET se reserva el derecho a cambiar la ubicación específica en cualquier momento sin previo aviso para mejorar los servicios prestados por ESET de acuerdo con sus preferencias de ubicación (p. ej., Unión Europea).

Software

ESET o sus proveedores tienen los derechos de autor o pueden ejercerlos en lo que respecta a todo el software disponible en los sitios web de la Cuenta (en adelante, el "Software"). El Software solo puede utilizarse de conformidad con el Acuerdo de licencia para el usuario final (en adelante, el "EULA"). El EULA se distribuye junto con el Software o forma parte de él. El Software distribuido con el EULA no puede instalarse si el Usuario no acepta el EULA. Encontrará más información sobre licencias, derechos de autor, documentación y marcas comerciales en la Información legal.

Restricciones

No puede copiar ni distribuir la Cuenta, ni extraer componentes o crear obras derivadas de ella. El uso de la Cuenta software está sujeto a las siguientes restricciones:

(a) No puede utilizar, modificar, traducir ni reproducir la Cuenta ni transferir los derechos de uso de la Cuenta o sus componentes de ninguna forma que no se haya establecido expresamente en estos Términos.

(b) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar la Cuenta, ni utilizarla para prestar servicios comerciales.

(c) No puede aplicar la ingeniería inversa, descompilar ni desmontar la Cuenta, ni intentar obtener de otra manera

su código fuente, salvo que la ley prohíba expresamente esta restricción.

(d) Acepta que el uso de la Cuenta 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.

Descargo de responsabilidad

COMO USUARIO, RECONOCE POR LA PRESENTE QUE LA CUENTA Y LOS SERVICIOS SE OFRECEN "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, HASTA DONDE LO PERMITA LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, NI SUS LICENCIADORES O FILIALES NI LOS TITULARES DE LOS DERECHOS DE AUTOR DECLARAN NI GARANTIZAN NADA, NI EXPLÍCITA NI IMPLÍCITAMENTE, LO QUE INCLUYE, ENTRE OTRAS COSAS, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN A UN PROPÓSITO ESPECÍFICO O QUE LA CUENTA O LOS SERVICIOS RESPETEN LAS PATENTES, LOS DERECHOS DE AUTOR, LAS MARCAS U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LA CUENTA O LOS SERVICIOS CUMPLAN SUS REQUISITOS NI QUE EN EL FUNCIONAMIENTO DE LA CUENTA O LOS SERVICIOS NO HAYA INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN Y EL USO DE LA CUENTA Y LOS SERVICIOS PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LOS RESULTADOS OBTENIDOS.

Estos Términos no crean más obligaciones al Proveedor ni a sus licenciadores que las expuestas específicamente en este documento.

Limitación de responsabilidad

HASTA DONDE LO PERMITA LA LEGISLACIÓN APLICABLE, NI EL PROVEEDOR, NI SUS EMPLEADOS NI SUS CONTRATISTAS SERÁN RESPONSABLES EN NINGÚN CASO DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE GASTOS POR ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, DAÑOS MATERIALES, DAÑOS PERSONALES, INTERRUPCIÓN COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, INCIDENTALES, ECONÓMICOS, DE COBERTURA, PUNITIVOS O CONSECUENTES, SEA CUAL SEA SU CAUSA Y TANTO SI SE DERIVAN DE UN CONTRATO, UN ACUERDO EXTRACONTRACTUAL, UNA NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD, PROVOCADOS POR EL USO DE LA CUENTA O LA INCAPACIDAD DE UTILIZARLA, AUNQUE EL PROVEEDOR O SUS CONTRATISTAS O FILIALES CONOZCAN 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, SUS CONTRATISTAS O SUS AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR EL SERVICIO O LA CUENTA EN CUESTIÓN.

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 de estos Términos 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 de estos Términos 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 la sección (a) de esta cláusula de Cumplimiento de las normas de control comercial, 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 de estos Términos podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

(c) Ninguna disposición de estos Términos 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.

Legislación aplicable e idioma

Estos Términos se regirán e interpretarán de conformidad con la legislación eslovaca. El Usuario final y el Proveedor acuerdan que no se aplicarán las disposiciones relativas a conflictos de leyes de la legislación aplicable y la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Si es un consumidor con domicilio habitual en la UE, también se le concede protección adicional mediante disposiciones legales obligatorias aplicables en su país de residencia.

Acepta explícitamente que la jurisdicción exclusiva en caso de reclamaciones o disputas con el Proveedor, relacionadas de cualquier forma con su uso del Software, la Cuenta o los Servicios o derivadas de estos Términos o Términos especiales (en su caso), corresponde al tribunal de distrito de Bratislava I (Eslovaquia); además, acepta y consiente explícitamente el ejercicio de la jurisdicción personal en el tribunal de distrito de Bratislava I en relación con dichas reclamaciones o disputas. Si es consumidor y tiene un domicilio habitual en la UE, también puede presentar una reclamación para exigir que se cumplan sus derechos de consumidor en el lugar de la jurisdicción exclusiva o en el país de la UE en el que vive. También puede utilizar una plataforma de resolución de disputas en línea, a la que se puede acceder aquí: https://ec.europa.eu/consumers/odr/. No obstante, puede ponerse en contacto con nosotros en primer lugar antes de realizar cualquier reclamación de forma oficial.

Si existen discrepancias entre las versiones en diferentes idiomas de estos Términos, siempre prevalecerá la versión en inglés, disponible aquí.

Disposiciones generales

ESET se reserva el derecho de revisar estos Términos y esta documentación o cualquier parte de ellos en cualquier momento; se limitará a actualizar el documento correspondiente para reflejar cambios de la legislación o cambios de la Cuenta. Se le notificará cualquier revisión de estos Términos mediante la Cuenta. Si no acepta los cambios de estos Términos, puede cancelar su Cuenta. A menos que cancele su Cuenta tras recibir la notificación de los

cambios, las modificaciones y las revisiones de estos Términos serán vinculantes para Usted. Le recomendamos que visite esta página periódicamente para consultar los Términos aplicables a su uso de la Cuenta.

Avisos

Todos los avisos deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Anexo n.º 1

EULA de ESET Management Agent

Anexo n.º 2

Acuerdo de procesamiento de datos

Anexo n.º 3

Cláusulas contractuales tipo

Acuerdo de licencia para el usuario final de ESET Management Agent

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

Comunicación y datos de administración. A la comunicación y los datos de administración se les aplican las siguientes disposiciones adicionales:

El Software contiene una función que permite transferir información entre el Ordenador 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 lo determinará la configuración del software instalado en el Ordenador. El contenido de las instrucciones del software de administración lo determinará la configuración del software de administración remota.

EULAID: EULA-PRODUCT-AGENT; 3537.0

Acuerdo de procesamiento de datos

De acuerdo con los requisitos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, "RGPD"), el Proveedor (en adelante, "Encargado del tratamiento") y Usted (en adelante, "Responsable del tratamiento") establecen una relación contractual sobre tratamiento de datos para definir los términos y condiciones del tratamiento de datos personales, la forma de proteger esos datos y otros derechos y obligaciones de ambas partes respecto al tratamiento de datos personales de los interesados en nombre del Responsable del tratamiento con respecto al objeto de estos Términos como contrato principal.

1. **Tratamiento de datos personales.** Entre los servicios prestados de acuerdo con estos Términos, se puede incluir el tratamiento de información relativa a una persona física identificada o identificable indicada en la Política de privacidad (en adelante, "Datos personales").

2. **Autorización.** El Responsable del tratamiento autoriza al Encargado del tratamiento a tratar los Datos personales, incluidas las siguientes instrucciones:

(i) "Finalidad del tratamiento" es la prestación de servicios de acuerdo con estos Términos. El Encargado del tratamiento solo puede procesar los Datos personales en nombre del Responsable del tratamiento en relación con la prestación de servicios solicitada por este. Toda la información recopilada con fines adicionales se procesa fuera de la relación contractual Controlador-Encargado del tratamiento.

(ii) Período de tratamiento es el período comprendido entre el inicio de la cooperación mutua de acuerdo con estos Términos y la finalización de los servicios.

(iii) Alcance y categorías de los datos personales. Los Servicios están diseñados únicamente para el tratamiento de datos personales generales. Sin embargo, el Responsable del tratamiento es el único responsable de la determinación del alcance de los datos personales.

(iv) "Interesado" es la persona física en tanto usuario autorizado de los dispositivos del Responsable del tratamiento.

(v) Operaciones de tratamiento son todas las operaciones necesarias para el tratamiento.

(vi) "Instrucciones documentadas" son las instrucciones descritas en estos Términos, sus Anexos, la Política de privacidad y la documentación del servicio. El Responsable del tratamiento se encargará de la legalización del tratamiento de los Datos personales por parte del Encargado del tratamiento en relación con las correspondientes disposiciones aplicables de la ley de protección de datos.

3. **Obligaciones del Encargado del tratamiento**. El Encargado del tratamiento está obligado a:

(i) Procesar los Datos personales solo de acuerdo con las instrucciones documentadas y con el fin definido en los Términos, sus Anexos, la Política de privacidad y la documentación de servicio.

(ii) Dar instrucciones a las personas autorizadas para tratar los Datos personales (en adelante, las "Personas autorizadas") sobre sus derechos y obligaciones en virtud del RGPD, sobre su responsabilidad en caso de infracción, y a garantizar que las Personas autorizadas se han comprometido a mantener la confidencialidad y seguir las instrucciones Documentadas.

(iii) Implementar y seguir las medidas descritas en los Términos, sus Anexos, la Política de privacidad y la documentación de servicio.

(iv) Ayudar al Responsable del tratamiento a responder a las solicitudes de los Interesados relacionadas con sus derechos. El Encargado del tratamiento no corregirá, eliminará ni restringirá el tratamiento de los Datos personales sin las instrucciones del Responsable del tratamiento. Todas las solicitudes del Interesado relacionadas con los Datos personales procesados en nombre del Responsable del tratamiento se remitirán al Responsable del tratamiento sin demora.

(v) Ayudar al Responsable del tratamiento en la notificación de una infracción de los Datos personales a la autoridad supervisora y al Interesado. El Encargado del tratamiento debe informar al Responsable del tratamiento de cualquier infracción del tratamiento de los Datos personales o de la seguridad de los datos personales inmediatamente después de tener constancia de dicha infracción. El Encargado del tratamiento deberá colaborar, en la medida de lo posible, en la investigación y corrección de dicha infracción, y adoptará medidas razonables para limitar otras implicaciones negativas.

(vi) Según decida el Responsable del tratamiento, eliminar o devolver todos los Datos personales al Responsable del tratamiento una vez que finalice el Periodo de tratamiento. El Responsable del tratamiento se compromete a informar al Encargado del tratamiento de su decisión en el plazo de diez (10) días después de la finalización del Periodo de tratamiento. Esta disposición no afectará al derecho del Encargado del tratamiento de mantener los Datos personales en la medida necesaria con fines de archivado por interés público, fines de investigación, con fines estadísticos o con fines de divulgación, ejercicio o defensa de procedimientos legales.

(vii) Mantener un registro actualizado de todas las categorías de actividades de tratamiento realizadas en nombre del Responsable del tratamiento.

(viii) Poner toda la información necesaria para demostrar el cumplimiento de los Términos, sus Anexos, la Política de privacidad y la documentación del servicio a disposición del Responsable del tratamiento. En caso de auditoría o control del tratamiento de los Datos personales por parte del Responsable del tratamiento, el Responsable del tratamiento está obligado a informar al Encargado del tratamiento por escrito con una antelación mínima de treinta (30) días antes de la auditoría o el control planificados.

4. **Participación de otro Encargado del tratamiento.** El Encargado del tratamiento tiene derecho a solicitar la participación de otro Encargado del tratamiento para realizar actividades de tratamiento específicas, como proporcionar infraestructura y almacenamiento en la nube para el servicio de acuerdo con estos Términos, sus Anexos, la Política de privacidad y la documentación del servicio. Microsoft ofrece actualmente almacenamiento en la nube e infraestructura como parte de Azure Cloud Service. Incluso en este caso, el Encargado del tratamiento seguirá siendo el único punto de contacto y la parte responsable del cumplimiento de la normativa. Por la presente, el Encargado del tratamiento se compromete a informar al Responsable del tratamiento de posibles adiciones o sustituciones de otro encargado del tratamiento, por si decidiera oponerse a dicho cambio.

5. **Territorio del tratamiento.** El Encargado del tratamiento garantiza que el tratamiento tiene lugar en el Espacio Económico Europeo o en un país considerado seguro por la Comisión Europea de acuerdo con la decisión del

Responsable del tratamiento. En caso de transferencias y tratamiento que tengan lugar fuera del Espacio Económico Europeo o de un país considerado seguro por la Comisión Europea a petición del Responsable del tratamiento, se aplican las cláusulas contractuales tipo.

6. **Seguridad.** El Encargado del tratamiento cuenta con la certificación ISO 27001:2013 y usa el marco de referencia ISO 27001 para implementar una estrategia de seguridad por capas al aplicar controles de seguridad en las capas de red, sistemas operativos, bases de datos, aplicaciones, personal y procesos operativos. El cumplimiento de los requisitos normativos y contractuales se evalúa y revisa con regularidad, de forma similar a lo que sucede con otras operaciones e infraestructuras del Encargado del tratamiento, y se dan los pasos necesarios para garantizar dicho cumplimiento en todo momento. El Encargado del tratamiento ha organizado la seguridad de los datos mediante ISMS según la norma ISO 27001. La documentación de seguridad incluye principalmente documentos de políticas sobre seguridad de la información, seguridad física y seguridad del equipo, gestión de incidentes, gestión de filtraciones de datos e incidentes de seguridad, etc.

7. **Medidas técnicas y organizativas**. El Encargado del tratamiento protegerá los Datos personales contra daños y destrucción, pérdidas, cambios, acceso y revelación no autorizadas de los Datos personales. A tal fin, el Encargado del tratamiento deberá adoptar las medidas técnicas y organizativas adecuadas correspondientes al modo de tratamiento y al riesgo que presenta el tratamiento para los derechos de los Interesados, de acuerdo con los requisitos que marca el RGPD. En la Política de seguridad se expone una descripción detallada de las medidas técnicas y organizativas.

8. **Datos de contacto del Encargado del tratamiento.** Todas las notificaciones, solicitudes, demandas y demás comunicaciones relativas a la protección de Datos personales deben dirigirse a ESET, spol. s.r.o., attention of: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Cláusulas contractuales tipo

SECCIÓN I

Cláusula 1 Finalidad y ámbito de aplicación

a) La finalidad de estas cláusulas contractuales tipo es garantizar que se cumplan los requisitos que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos(1) (Reglamento general de protección de datos), exige para la transferencia de datos personales a un tercer país.

b) Las Partes:

i) la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, «entidad» o «entidades») que va(n) a transferir los datos personales, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «exportador de datos»), y

ii) la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «importador de datos»),

han pactado las presentes cláusulas contractuales tipo (en lo sucesivo, «pliego de cláusulas»).

c) El presente pliego de cláusulas se aplica a la transferencia de datos personales especificada en el anexo I.B.

d) El apéndice del presente pliego de cláusulas, que contiene los anexos que se citan en estas, forman parte del

pliego.

Cláusula 2 Efecto e invariabilidad de las cláusulas

a) El presente pliego de cláusulas establece garantías adecuadas, incluidos derechos exigibles de los interesados y acciones judiciales eficaces, de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679 y, en relación con las transferencias de datos de responsables a encargados o de encargados a otros encargados, de conformidad con las cláusulas contractuales tipo a que se refiere el artículo 28, apartado 7, del Reglamento (UE) 2016/679 siempre que no se modifiquen, salvo para seleccionar el módulo o módulos adecuados o para añadir o actualizar información del apéndice. Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, al presente pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

b) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el exportador de datos en virtud del Reglamento (UE) 2016/679.

Cláusula 3 Tercero beneficiario

a) Los interesados podrán invocar, como terceros beneficiarios, el presente pliego de cláusulas contra el exportador y/o el importador de datos y exigirles su cumplimiento, con las excepciones siguientes.

Cláusulas 1, 2, 3, 6 y 7.

ii) Cláusula 8: [módulo uno] cláusula 8.5, letra e), y cláusula 8.9, letra b); [módulo dos] cláusula 8.1, letra b), y cláusula 8.9, letras a), c), d) y e); [módulo tres] cláusula 8.1, letras a), c) y d), y cláusula 8.9, letras a), c), d), e), f) y g); [módulo cuatro] cláusula 8.1, letra b), y cláusula 8.3, letra b).

iii) Cláusula 9: [módulo dos] cláusula 9, letras a), c), d) y e); [módulo tres] cláusula 9, letras a), c), d) y e).

iv) Cláusula 12: [módulo uno] cláusula 12, letras a) y d); [módulos dos y tres] cláusula 12, letras a), d) y f).

v) Cláusula 13

vi) Cláusula 15.1, letras c), d) y e).

vii) Cláusula 16, letra e).

viii) Cláusula 18: [módulos uno, dos y tres] cláusula 18, letras a) y b); [módulo cuatro] cláusula 18.

b) Lo dispuesto en la letra a) se entiende sin perjuicio de los derechos que el Reglamento (UE) 2016/679 otorga a los interesados.

Cláusula 4 Interpretación

a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en dicho Reglamento.

b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.

c) El presente pliego de cláusulas no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679.

Cláusula 5 Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 6 Descripción de la transferencia o transferencias

Los datos de la transferencia o transferencias y, en particular, las categorías de datos personales que se transfieren y los fines para los que se transfieren se especifican en el anexo I.B.

Cláusula 7 (opcional) Cláusula de incorporación

a) Cualquier entidad que no sea parte en el presente pliego de cláusulas podrá, previo consentimiento de todas las partes, adherirse al presente pliego de cláusulas en cualquier momento, ya sea como exportador de datos o como importador de datos, cumplimentando el apéndice y firmando el anexo I.A.

b) Una vez haya cumplimentado el apéndice y firmado el anexo I.A, la entidad que se adhiera se considerará parte en el presente pliego de cláusulas y tendrá los derechos y obligaciones de un exportador de datos o un importador de datos, según la categoría en la que se haya inscrito en el anexo I.A.

c) La entidad que se adhiera no adquirirá derechos y obligaciones del presente pliego de cláusulas derivados del período anterior a la adhesión.

SECCIÓN II: OBLIGACIONES DE LAS PARTES

Cláusula 8 Garantías en materia de protección de datos

El exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el importador de datos puede, aplicando medidas técnicas y organizativas adecuadas, cumplir las obligaciones que le atribuye el presente pliego de cláusulas.

MÓDULO UNO: transferencia de responsable a responsable

8.1. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B. Solo podrá tratar los datos personales con otros fines:

i) cuando haya recabado el consentimiento previo del interesado;

ii) cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos;

iii) cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

8.2. Transparencia

a) A fin de que los interesados puedan ejercer de forma eficaz los derechos que les otorga la cláusula 10, el importador de datos les informará, directamente o a través del exportador de datos:

i) de su identidad y datos de contacto;

ii) de las categorías de datos personales tratados;

iii) del derecho a solicitar una copia del presente pliego de cláusulas;

iv) cuando tenga la intención de realizar transferencias ulteriores de los datos personales a terceros, del destinatario o de las categorías de destinatarios (según proceda con el fin de proporcionar información significativa), la finalidad de dicha transferencia ulterior y el motivo de la misma con arreglo a la cláusula 8.7.

b) Lo dispuesto en la letra a) no será de aplicación cuando el interesado ya disponga de la información (por ejemplo, si el exportador de datos ya ha proporcionado dicha información) o cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado para el importador de datos. En este último caso, el importador de datos hará pública la información en la medida de lo posible.

c) Previa solicitud, las partes pondrán gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, las partes podrán expurgar el texto del apéndice antes de compartir una copia, pero deberán aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada.

d) Lo dispuesto en las letras a) a c) se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.3. Exactitud y minimización de datos

a) Cada parte se asegurará de que los datos personales sean exactos y, cuando proceda, estén actualizados. El importador de datos adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

b) Si una de las partes tiene conocimiento de que los datos personales que ha transferido o recibido son inexactos o han quedado obsoletos, informará de ello a la otra parte sin dilación indebida.

c) El importador de datos se asegurará de que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento.

8.4. Limitación del plazo de conservación

El importador de datos no conservará los datos personales más tiempo del necesario para los fines para los que se traten. Establecerá las medidas técnicas u organizativas adecuadas para garantizar el cumplimiento de esta obligación, como la supresión o anonimización (2) de los datos y de todas las copias de seguridad al finalizar el período de conservación.

8.5. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para el interesado. Las partes deberán considerar, en

particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento.

b) Las partes han pactado las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

c) El importador de datos garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

d) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los posibles efectos negativos.

e) En caso de violación de la seguridad de los datos personales que sea probable que entrañe un riesgo para los derechos y libertades de las personas físicas, el importador de datos lo notificará sin dilación indebida tanto al exportador de datos como a la autoridad de control competente con arreglo a la cláusula 13. Dicha notificación contendrá i) una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), ii) las consecuencias probables, iii) las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad y iv) los datos de un punto de contacto en el que pueda obtenerse más información. En la medida en que el importador de datos no pueda proporcionar toda la información al mismo tiempo, podrá hacerlo por fases sin más dilaciones indebidas.

f) En caso de violación de la seguridad de los datos personales que sea probable que entrañe un riesgo elevado para los derechos y libertades de las personas físicas, el importador de datos también notificará sin dilación indebida a los interesados la violación de la seguridad de los datos personales y su naturaleza —en caso necesario con la colaboración del exportador de datos— junto con la información a que se refiere la letra e), incisos ii) a iv), a menos que dicha notificación suponga un esfuerzo desproporcionado o que el importador de datos haya aplicado medidas para reducir significativamente el riesgo para los derechos o libertades de las personas físicas. En este último caso, el importador de datos realizará una comunicación pública o adoptará una medida semejante para informar al público de la violación de la seguridad de los datos personales.

g) El importador de datos documentará todos los hechos pertinentes relacionados con la violación de la seguridad de los datos personales, como sus efectos y las medidas correctivas adoptadas, y llevará un registro de las mismas.

8.6. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas o infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará restricciones específicas y/o garantías adicionales adaptadas a la naturaleza específica de los datos y el riesgo de que se trate. Una de estas puede ser, por ejemplo, la reducción del personal autorizado a acceder a los datos personales, medidas de seguridad adicionales (como la seudonimización) y/o restricciones adicionales con respecto a la comunicación ulterior.

8.7. Transferencias ulteriores

El importador de datos no comunicará los datos personales a terceros situados fuera de la Unión Europea (3) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») a menos

que el tercero esté vinculado por el presente pliego de cláusulas o consienta a someterse a este, con elección del módulo correspondiente. De no ser así, el importador de datos solo podrá efectuar una transferencia ulterior si:

i) esta va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;

iii) el tercero suscribe un instrumento vinculante con el importador de datos que garantice el mismo nivel de protección de datos que el del presente pliego de cláusulas, y el importador de datos entrega una copia de estas garantías al exportador de datos;

iv) si es necesario para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos;

v) si es necesario para proteger intereses vitales del interesado o de otra persona física; o

vi) de no concurrir las demás condiciones, el importador de datos ha recabado el consentimiento expreso del interesado para una transferencia ulterior en una situación específica, tras haberle informado de su finalidad, de la identidad del destinatario y de los posibles riesgos de dicha transferencia para el interesado debido a la falta de garantías adecuadas en materia de protección de datos. En este caso, el importador de datos informará al exportador de datos y, a petición de este, le remitirá una copia de la información proporcionada al interesado.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.8. Tratamiento bajo la autoridad del importador de datos

El importador de datos se asegurará de que las personas que actúen bajo su autoridad, especialmente el encargado, solo trate los datos siguiendo instrucciones del importador de datos.

8.9. Documentación y cumplimiento

a) Las partes deberán poder demostrar el cumplimiento de las obligaciones derivadas del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen bajo su responsabilidad.

b) El importador de datos pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud.

MÓDULO DOS: transferencia de responsable a encargado

8.1. Instrucciones

a) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del exportador de datos. El exportador de datos podrá dar dichas instrucciones durante todo el período de vigencia del contrato.

b) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones.

8.2. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia

indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del exportador de datos.

8.3. Transparencia

Previa solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como las medidas descritas en el anexo II y datos personales, el exportador de datos podrá expurgar el texto del apéndice del presente pliego de cláusulas antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada. La presente cláusula se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.4. Exactitud

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5. Duración del tratamiento y supresión o devolución de los datos

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del exportador de datos y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la cláusula 14, letra a).

8.6. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

b) El importador de datos solo concederá acceso a los datos personales a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato.

Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también lo notificará al exportador de datos sin dilación indebida una vez tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente, en su caso, medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

d) El importador de datos deberá colaborar con el exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8. Transferencias ulteriores

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del exportador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea (4) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

i) la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;

iii) si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o

iv) si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9. Documentación y cumplimiento

a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del exportador de datos.

c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y, a instancia del exportador de datos, permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.

d) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.

e) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

MÓDULO TRES: transferencia de encargado a encargado

8.1. Instrucciones

a) El exportador de datos ha informado al importador de datos de que actúa como encargado del tratamiento siguiendo las instrucciones de su responsable o responsables, que el exportador de datos deberá poner a disposición del importador de datos antes del tratamiento.

b) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del responsable del tratamiento, comunicadas al importador por el exportador de datos, así como instrucciones documentadas adicionales del exportador de datos. Dichas instrucciones adicionales no podrán estar en conflicto con las instrucciones del responsable. El responsable o el exportador de datos podrán dar instrucciones documentadas adicionales sobre el tratamiento de datos durante todo el período de vigencia del contrato.

c) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones. Si el importador de datos no puede seguir las instrucciones del responsable, el exportador de datos lo notificará inmediatamente al responsable.

d) El exportador de datos asegura que ha impuesto al importador de datos las obligaciones en materia de protección de datos establecidas en el contrato u otro acto jurídico con arreglo al Derecho de la Unión o del Estado miembro entre el responsable y el exportador de datos (5).

8.2. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del responsable, comunicadas al importador de datos por el exportador de datos, o del exportador de datos.

8.3. Transparencia

Previa solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el exportador de

datos podrá expurgar el texto del apéndice antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada.

8.4. Exactitud

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5. Duración del tratamiento y supresión o devolución de los datos

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del responsable y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la cláusula 14, letra a).

8.6. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para el interesado. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos o del responsable. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

b) El importador de datos solo concederá acceso a los datos a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también notificará sin dilación indebida al exportador de datos y, cuando proceda y sea viable, al responsable cuando tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las

categorías y el número aproximado de interesados y registros de datos personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

d) El importador de datos deberá colaborar con el exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación al responsable para que este luego lo notifique a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8. Transferencias ulteriores

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del responsable, tal y como las haya comunicado el exportador de datos al importador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea (6) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

i) la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679;

iii) si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o

iv) si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9. Documentación y cumplimiento

a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos o del responsable relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del responsable.

c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente pliego de cláusulas; el exportador de

datos luego la proporcionará al responsable.

d) El importador de datos permitirá y contribuirá a las auditorías que realice el exportador de datos sobre las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Lo mismo se aplicará cuando el exportador de datos solicite una auditoría siguiendo instrucciones del responsable. Al decidir si se realiza una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.

e) Cuando la auditoría se realice siguiendo instrucciones del responsable del tratamiento, el exportador de datos pondrá los resultados a disposición del responsable.

f) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.

g) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

MÓDULO CUATRO: transferencia de encargado a responsable

8.1. Instrucciones

a) El exportador de datos solo tratará los datos personales siguiendo instrucciones documentadas del importador de datos que actúe como su responsable.

b) El exportador de datos informará inmediatamente al importador de datos si no puede seguir dichas instrucciones, especialmente si dichas instrucciones infringen el Reglamento (UE) 2016/679 u otro instrumento normativo del Derecho de la Unión o del Estado miembro en materia de protección de datos.

c) El importador de datos no obrará de forma que pueda impedir al exportador de datos cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679 y, en particular, en el marco del subtratamiento o de la cooperación con las autoridades de control competentes.

d) Una vez se hayan prestado los servicios de tratamiento, el exportador de datos suprimirá, a petición del importador de datos, todos los datos personales tratados por cuenta del importador de datos y acreditará al importador de datos que lo ha hecho, o devolverá al importador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes.

8.2. Seguridad del tratamiento

a) Las partes aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, especialmente durante la transferencia; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza de los datos personales (7), la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados, y considerarán, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento.

b) El exportador de datos ayudará al importador de datos a garantizar una seguridad adecuada de los datos de conformidad con la letra a). En caso de violación de la seguridad de los datos personales tratados por el exportador de datos en virtud del presente pliego de cláusulas, el exportador de datos lo notificará sin dilación

indebida al importador de datos, una vez que tenga conocimiento de ello, y le ayudará a poner remedio a la violación de la seguridad.

c) El exportador de datos garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

8.3. Documentación y cumplimiento

Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas.

b) El exportador de datos pondrá a disposición del importador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones que le atribuye el presente pliego de cláusulas y permitirá y contribuirá a las auditorías.

Cláusula 9 Recurso a subencargados

MÓDULO DOS: transferencia de responsable a encargado

a) El importador de datos cuenta con una autorización general del exportador de datos para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al exportador de datos específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el exportador de datos tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al exportador de datos la información necesaria para que este pueda ejercer su derecho a formular objeción.

b) Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del exportador de datos), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto que terceros beneficiarios. (8) Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.

c) El importador de datos proporcionará al exportador de datos, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.

d) El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.

e) El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

MÓDULO TRES: transferencia de encargado a encargado

a) El importador de datos cuenta con una autorización general del responsable para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al responsable específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el responsable tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al responsable la información necesaria para que pueda ejercer su derecho a formular objeción. El importador de datos informará al exportador de datos de la contratación del subencargado o subencargados.

b) Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del responsable), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto que terceros beneficiarios. (9) Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.

c) El importador de datos proporcionará al exportador de datos o al responsable, a instancia del exportador de datos o el responsable, respectivamente, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.

d) El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.

e) El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

Cláusula 10 Derechos del interesado

MÓDULO UNO: transferencia de responsable a responsable

a) El importador de datos, en su caso con la asistencia del exportador de datos, tramitará, sin dilación indebida y como tarde en un plazo de un mes desde la recepción de la consulta o solicitud, las consultas y solicitudes que reciba de interesados en relación con el tratamiento de sus datos personales y el ejercicio de los derechos que les otorga el presente pliego de cláusulas. (10) El importador de datos adoptará medidas adecuadas para facilitar dichas consultas y solicitudes y el ejercicio de los derechos de los interesados. Toda la información que se proporcione a los interesados deberá ser inteligible y de fácil acceso, con un lenguaje claro y sencillo.

b) En particular, el importador de datos deberá, a petición del interesado y de forma gratuita:

i) confirmar al interesado si se están tratando datos personales que le conciernan y, en su caso, proporcionar una copia de los datos que le conciernan, así como la información que figura en el anexo I; si los datos personales han sido o serán ulteriormente transferidos, información sobre los destinatarios o las categorías de destinatarios (según proceda, con vistas a proporcionar información significativa) a los que se haya realizado o vaya realizarse la transferencia ulterior de los datos personales, la finalidad de dichas transferencias ulteriores y su motivo de conformidad con la cláusula 8.7; e información sobre el derecho a presentar una reclamación ante una autoridad de control en virtud de la cláusula 12, letra c), inciso i);

ii) rectificar los datos inexactos o incompletos relativos al interesado;

iii) suprimir los datos personales relativos al interesado si dichos datos se están tratando o han sido tratados en contravención de cualquiera de las cláusulas que garantizan los derechos de terceros beneficiarios o si el interesado retira el consentimiento en que se basa el tratamiento.

c) Cuando el importador de datos trate los datos personales con fines de mercadotecnia directa, dejará de tratarlos para tales fines si el interesado se opone a ello.

d) El importador de datos no tomará una decisión, basándose únicamente en el tratamiento automatizado de los datos personales transferidos («decisión automatizada»), que produzca efectos jurídicos para el interesado o le afecte de forma igualmente significativa, salvo con el consentimiento expreso del interesado o si así lo autoriza el Derecho del país de destino, siempre que dicho Derecho disponga medidas adecuadas para garantizar los intereses legítimos y los derechos del interesado. En este caso, el importador de datos, con la colaboración del exportador de datos cuando sea necesario:

i) informará al interesado de la decisión automatizada prevista y de las consecuencias previstas, así como de la lógica aplicada; y

ii) aplicará garantías adecuadas, como mínimo permitiendo al interesado impugnar la decisión, expresar su punto de vista y solicitar una revisión por parte de un ser humano.

e) Cuando las solicitudes de un interesado sean excesivas, especialmente debido a su carácter repetitivo, el importador de datos podrá establecer una tasa razonable en función del coste administrativo que implique la concesión de la solicitud o negarse a actuar respecto de la solicitud.

f) El importador de datos podrá denegar la solicitud de un interesado cuando ello esté permitido con arreglo al Derecho del país de destino y sea necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

g) Si el importador de datos pretende denegar la solicitud de un interesado, le informará de los motivos de la denegación y de la posibilidad de presentar una reclamación ante la autoridad de control competente o de ejercitar una acción judicial.

MÓDULO DOS: transferencia de responsable a encargado

a) El importador de datos notificará con presteza al exportador de datos las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el exportador de datos le haya autorizado a hacerlo.

b) El importador de datos ayudará al exportador de datos a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 atribuye a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

c) En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del exportador de datos.

MÓDULO TRES: transferencia de encargado a encargado

a) El importador de datos notificará con presteza al exportador de datos y, en su caso, al responsable toda solicitud que reciba de un interesado, sin responder a dicha solicitud, a menos que haya sido autorizado a hacerlo por el responsable.

b) El importador de datos ayudará al exportador de datos, cuando proceda con la colaboración del exportador de datos, a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725 atribuyen a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

c) En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del responsable, comunicadas por el exportador de datos.

MÓDULO CUATRO: transferencia de encargado a responsable

Las partes se prestarán ayuda recíproca para responder a las consultas y solicitudes de los interesados en virtud del Derecho doméstico aplicable al importador de datos o, respecto del tratamiento de datos por parte del exportador de datos en la Unión, en virtud del Reglamento (UE) 2016/679.

Cláusula 11 Reparación

a) El importador de datos informará a los interesados, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará con presteza las reclamaciones que reciba de los interesados.

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

b) En caso de litigio entre un interesado y una de las partes en relación con el cumplimiento del presente pliego de cláusulas, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán para resolverlos.

c) El importador de datos se compromete a aceptar, cuando el interesado invoque un derecho de tercero beneficiario con arreglo a la cláusula 3, la decisión del interesado de:

i) presentar una reclamación ante la autoridad de control del Estado miembro de su residencia habitual o su lugar de trabajo o ante la autoridad de control competente con arreglo a la cláusula 13;

ii) ejercitar una acción judicial en el sentido de la cláusula 18.

d) Las partes aceptan que el interesado pueda estar representado por una entidad, organización o asociación sin ánimo de lucro en las condiciones establecidas en el artículo 80, apartado 1, del Reglamento (UE) 2016/679.

e) El importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo al Derecho aplicable de la UE o del Estado miembro de que se trate.

f) El importador de datos acepta que la elección del interesado no menoscabe sus derechos sustantivos y procesales a obtener reparación de conformidad con el Derecho aplicable.

Cláusula 12 Responsabilidad

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO CUATRO: transferencia de encargado a responsable

a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

b) Cada parte será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que la parte ocasione al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Ello se entiende sin perjuicio de la responsabilidad que le atribuye el Reglamento (UE) 2016/679 al exportador de datos.

c) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

d) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra c), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

e) El importador de datos no puede alegar la conducta de un encargado o subencargado del tratamiento para eludir su propia responsabilidad.

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

b) El importador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el importador de datos o su subencargado ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas.

c) A pesar de lo dispuesto en la letra b), el exportador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el exportador de datos o el importador de datos (o su subencargado) ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Lo anterior se entiende sin perjuicio de la responsabilidad del exportador de datos y, cuando el exportador de datos sea un encargado que actúe por cuenta de un responsable, de la responsabilidad del responsable con arreglo al Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725, según cuál sea de aplicación.

d) Las partes acuerdan que, si el exportador de datos es considerado responsable, de conformidad con la letra c), de los daños o perjuicios causados por el importador de datos (o su subencargado), estará legitimado para exigir al importador de datos la parte de la indemnización que sea responsabilidad del importador de los datos.

e) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

f) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra e), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

g) El importador de datos no puede alegar la conducta de un subencargado del tratamiento para eludir su propia

responsabilidad.

Cláusula 13 Supervisión

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

a) [Cuando el exportador de datos esté establecido en un Estado miembro de la UE:] La autoridad de control responsable de garantizar que el exportador de datos cumpla el Reglamento (UE) 2016/679 en cuanto a la transferencia de los datos, indicada en el anexo I.C, actuará como autoridad de control competente.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, y haya nombrado a un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679:] La autoridad de control del Estado miembro en que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, indicada en el anexo I.C, actuará como autoridad de control competente.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679 de la Comisión, de conformidad con el artículo 3, apartado 2, y no haya nombrado a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679 de la Comisión:] La autoridad de control de uno de los Estado miembros en que estén situados los interesados cuyos datos personales se transfieran en virtud del presente pliego de cláusulas en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado, indicada en el anexo I.C, actuará como autoridad de control competente.

b) El importador de datos da su consentimiento a someterse a la jurisdicción de la autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

DERECHO DEL PAÍS Y OBLIGACIONES EN CASO DE ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

Cláusula 14 Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: Transferencia de encargado a responsable (solo si el encargado de la UE combina los datos personales recibidos del responsable del tercer país con los datos personales recopilados por el encargado en la UE)

a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:

i) las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;

ii) el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables (12);

iii) las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador de datos la información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.

d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.

e) El importador de datos se compromete a notificar con presteza al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a). [Módulo tres: El exportador de datos notificará al responsable.]

f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación [módulo tres:, si procede, tras consultar al responsable]. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone [módulo tres: el responsable o] la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).

Cláusula 15 Obligaciones del importador de datos en caso de acceso por parte de las autoridades públicas

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: Transferencia de encargado a responsable (solo si el encargado de la UE combina los datos personales recibidos del responsable del tercer país con los datos personales recopilados por el encargado en la UE)

15.1. Notificación

a) El importador de datos se compromete a notificar con presteza al exportador de datos y, cuando sea posible, al interesado (de ser necesario, con la ayuda del exportador de datos) si:

i) recibe una solicitud jurídicamente vinculante de comunicación de datos personales transferidos con arreglo al presente pliego de cláusulas presentada por una autoridad pública (sobre todo, judicial) en virtud del Derecho del país de destino; dicha notificación contendrá información sobre los datos personales solicitados, la autoridad solicitante, la base jurídica de la solicitud y la respuesta dada; o

ii) tiene conocimiento de que las autoridades públicas han tenido acceso directo a los datos personales transferidos con arreglo al presente pliego de cláusulas en virtud del Derecho del país de destino; dicha notificación incluirá toda la información de que disponga el importador de datos.

[Módulo tres: El exportador de datos notificará al responsable.]

b) Si se prohíbe al importador de datos enviar la notificación al exportador de datos y/o al interesado en virtud del Derecho del país de destino, el importador de datos se compromete a hacer todo lo posible para obtener una dispensa de la prohibición, con el fin de comunicar toda la información disponible y lo antes posible. El importador de datos se compromete a documentar las actuaciones que realice a tal fin para poder justificar su diligencia si se lo pide el exportador de datos.

c) En la medida en que lo permita el Derecho del país de destino, el importador de datos se compromete a proporcionar al exportador de datos, a intervalos regulares durante el período de vigencia del contrato, la mayor cantidad posible de información pertinente sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos solicitados, la autoridad o autoridades solicitantes, la impugnación de las solicitudes, el resultado de tales impugnaciones, etc.). [Módulo tres: El exportador de datos remitirá la información al responsable.]

d) El importador de datos se compromete a conservar la información a que se refieren las letras a) a c) durante el período de vigencia del contrato y a ponerla a disposición de la autoridad de control competente previa solicitud.

e) Las letras a) a c) se entenderán sin perjuicio de la obligación del importador de datos, contemplada en la cláusula 14, letra e), y en la cláusula 16, de informar con presteza al exportador de datos cuando no pueda dar cumplimiento al presente pliego de cláusulas.

15.2. Control de la legalidad y minimización de datos

a) El importador de datos se compromete a controlar la legalidad de la solicitud de comunicación y, en particular, si la autoridad pública solicitante está debidamente facultada para ello, así como a impugnar la solicitud si, tras una valoración minuciosa, llega a la conclusión de que existen motivos razonables para considerar que la solicitud

es ilícita con arreglo al Derecho del país de destino, incluidas las obligaciones aplicables en virtud del Derecho internacional y los principios de cortesía internacional. El importador de datos agotará, en las mismas condiciones, las vías de recurso. Al impugnar una solicitud, el importador de datos instará la aplicación de medidas cautelares para suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo. No comunicará los datos personales solicitados hasta que se lo exija la normativa procesal aplicable. Estos requisitos se entienden sin perjuicio de las obligaciones que la cláusula 14, letra e), atribuye al importador de datos.

b) El importador de datos se compromete a documentar sus valoraciones jurídicas y las impugnaciones de solicitudes de comunicación y a poner dicha documentación a disposición del exportador de datos en la medida en que lo permita el Derecho del país de destino. También pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud. [Módulo tres: El exportador de datos pondrá la valoración a disposición del responsable.]

c) El importador de datos se compromete a proporcionar la mínima información posible al responder a las solicitudes de comunicación, basándose en una interpretación razonable de la solicitud.

SECCIÓN IV: DISPOSICIONES FINALES

Cláusula 16 Incumplimiento de las cláusulas y resolución del contrato

a) El importador de datos informará con presteza al exportador de datos en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) En caso de que el importador de datos incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos suspenderá la transferencia de datos personales al importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato. Lo anterior se entiende sin perjuicio de la cláusula 14, letra f).

c) El exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

i) el exportador de datos haya suspendido la transferencia de datos personales al importador de datos con arreglo a la letra b) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

ii) el importador de datos vulnere de manera sustancial o persistente el presente pliego de cláusulas; o

iii) el importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o autoridad de control competente en relación con las obligaciones que le atribuye el presente pliego de cláusulas.

En este supuesto, informará a la autoridad de supervisión competente [módulo tres: y al responsable] de su incumplimiento. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa.

d) [Módulos uno, dos y tres: Los datos personales que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán, a elección del exportador de datos, devolverse inmediatamente al exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias de los datos.] [Módulo cuatro: Los datos personales recopilados por el exportador de datos en la UE que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán destruirse en su totalidad inmediatamente, así como cualquier copia de estos.] El importador de datos acreditará la destrucción de los datos al exportador de datos. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente

pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales transferidos, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

e) Ninguna de las partes podrá revocar su consentimiento a quedar vinculada por el presente pliego de cláusulas si: i) la Comisión Europea adopta una decisión de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 que regule la transferencia de datos personales a los que se aplique el presente pliego de cláusulas; o ii) el Reglamento (UE) 2016/679 pasa a formar parte del ordenamiento jurídico del país al que se transfieren los datos personales. Ello se entiende sin perjuicio de otras responsabilidades que sean de aplicación al tratamiento en cuestión en virtud del Reglamento (UE) 2016/679.

Cláusula 17 Ley aplicable

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

El presente pliego de cláusulas se regirá por el Derecho de uno de los Estados miembros de la Unión Europea, siempre que dicho Derecho admita la existencia de derechos de los terceros beneficiarios. Las Partes acuerdan que esta es la ley según está definida en los Términos.

MÓDULO CUATRO: transferencia de encargado a responsable

El presente pliego de cláusulas se regirá por el Derecho de un país que contemple los derechos de los terceros beneficiarios. Las Partes acuerdan que esta es la ley según está definida en los Términos.

Cláusula 18 Elección del foro y jurisdicción

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

a) Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente en un Estado miembro de la Unión Europea.

(b) Las Partes acuerdan que estos serán los tribunales según están definidos en los Términos.

c) Los interesados también podrán ejercer acciones judiciales contra el exportador de datos y/o el importador de datos en el Estado miembro en el que el interesado tenga su residencia habitual.

d) Las partes acuerdan someterse a la jurisdicción de dicho Estado miembro.

MÓDULO CUATRO: transferencia de encargado a responsable

Cualquier disputa derivada de estas Cláusulas deberá ser resuelta por los tribunales según están definidos en los Términos.

APÉNDICE

NOTA ACLARATORIA: Se debe poder distinguir claramente la información aplicable a cada transferencia o categoría de transferencias y, por tanto, determinar la función o funciones respectivas de las partes en cuanto exportador(as) de datos y/o importador(as) de datos. No es imprescindible cumplimentar y firmar apéndices separados por cada transferencia o categoría de transferencias y/o relación contractual si se puede lograr un nivel de transparencia equivalente cumplimentando un solo apéndice. No obstante, cuando sea necesario para garantizar claridad suficiente, deben utilizarse apéndices separados.

ANEXO I

A. LISTA DE PARTES

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: transferencia de encargado a responsable

Exportador(es) de datos: [Identidad y datos de contacto del exportador o exportadores de datos y, en su caso, del delegado de protección de datos de este o estos y/o del representante en la Unión Europea]

1. Responsable del tratamiento según está definido en el Acuerdo de tratamiento de datos

2. Encargado del tratamiento según está definido en el Acuerdo de tratamiento de datos

(según el flujo de datos)

Importador(es) de datos: [Identidad y datos de contacto del importador o importadores de datos, incluida cualquier persona de contacto responsable de la protección de los datos]

1. Responsable del tratamiento según está definido en el Acuerdo de tratamiento de datos

2. Encargado del tratamiento según está definido en el Acuerdo de tratamiento de datos

(según el flujo de datos)

B. DESCRIPCIÓN DE LA TRANSFERENCIA

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: transferencia de encargado a responsable

Categorías de interesados cuyos datos personales se transfieren: según están definidas en el Acuerdo de tratamiento de datos.

Categorías de datos personales transferidos: según están definidas en el Acuerdo de tratamiento de datos y la Política de privacidad.

Datos sensibles transferidos (si procede) y restricciones o garantías aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos que entrañan, como, por ejemplo, la limitación estricta de la finalidad, restricciones de acceso (incluido el acceso exclusivo del personal que haya hecho un curso especializado), un registro del acceso a los datos, restricciones a transferencias ulteriores o medidas de seguridad adicionales. según están definidas en el Acuerdo de tratamiento de datos y la Política de privacidad.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de una vez o de forma periódica): de forma continua.

Naturaleza del tratamiento: automatizado.

Finalidad(es) de la transferencia y posterior tratamiento de los datos: prestación del servicio según está definida en los Términos, sus Anexos, su Política de privacidad y la documentación del servicio.

El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo: según están definidas en el Acuerdo de tratamiento de datos.

En caso de transferencia a (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento: según están definidas en el Acuerdo de tratamiento de datos.

C. AUTORIDAD DE CONTROL COMPETENTE

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

Indíquese la autoridad o autoridades de control competentes de conformidad con la cláusula 13: según están definidas en la Política de privacidad

ANEXO II: MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

NOTA ACLARATORIA: Las medidas técnicas y organizativas deben describirse de manera concreta y no de manera genérica. Véase también el comentario general de la primera página del apéndice, especialmente en cuanto a la necesidad de indicar claramente qué medidas se aplican a cada transferencia o conjunto de transferencias.

Descripción de las medidas técnicas y organizativas aplicadas por los importadores de datos (inclusive las certificaciones pertinentes) para garantizar un nivel adecuado de seguridad, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas: según están definidas en la Política de seguridad

En el caso de las transferencias a (sub)encargados, descríbanse también las medidas técnicas y organizativas específicas que deberá adoptar el (sub)encargado para poder prestar ayudar al responsable y, en el caso de

transferencias de un encargado a un subencargado, al exportador de datos.

ANEXO III: LISTA DE SUBENCARGADOS DEL TRATAMIENTO

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

NOTA ACLARATORIA: Debe cumplimentarse este anexo respecto de los módulos dos y tres cuando sea necesaria la autorización específica de uno o más subencargados [cláusula 9, letra a), opción 1].

El responsable ha autorizado que se recurra a los subencargados siguientes: según está definido en el Acuerdo de tratamiento de datos

Referencias:

(1) Cuando el exportador de datos sea un encargado del tratamiento sujeto al Reglamento (UE) 2016/679 que actúe por cuenta de una institución u organismo de la Unión como responsable del tratamiento, se considera que la utilización del presente pliego de cláusulas al recurrir a otro encargado (subtratamiento) no sujeto al Reglamento (UE) 2016/679 también garantiza el cumplimento del artículo 29, apartado 4, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. o 45/2001 y la Decisión n. o 1247/2002/CE (DO L295 de 21.11.2018, p. 39), en la medida en que estén armonizados el presente pliego de cláusulas y las obligaciones en materia de protección de datos que imponga el contrato u otro acto jurídico celebrado entre el responsable y el encargado con arreglo al artículo 29, apartado 3, del Reglamento (UE) 2018/1725. Este será el caso, en particular, cuando el responsable y el encargado del tratamiento se basen en las cláusulas contractuales tipo incluidas en la Decisión 2021/915.

(2) Para ello es necesario anonimizar los datos de tal manera que nadie pueda identificar a la persona, de conformidad con el considerando 26 del Reglamento (UE) 2016/679, y que este proceso sea irreversible.

(3) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(4) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(5) Véase el artículo 28, apartado 4, del Reglamento (UE) 2016/679 y, cuando el responsable sea una institución u organismo de la UE, el artículo 29, apartado 4, del Reglamento (UE) 2018/1725.

(6) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el

Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(7) En concreto, si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales.

(8) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

(9) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

(10) Dicho plazo podrá prorrogarse por un máximo de dos meses adicionales en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El importador de datos informará debidamente y con prontitud al interesado de cualquier prórroga de este tipo.

(11) El importador de datos solo podrá ofrecer una resolución independiente de los litigios a través de un órgano de arbitraje si está establecido en un país que haya ratificado el Convenio de Nueva York sobre la ejecución de laudos arbitrales.

(12) Por lo que se refiere al efecto de dicho Derecho y prácticas en el cumplimiento del presente pliego de cláusulas, a la hora de realizar una valoración integral de esta cuestión pueden tenerse en cuenta distintos aspectos. Uno de estos aspectos puede ser que haya experiencia práctica pertinente y documentada en casos anteriores de solicitudes de comunicación por parte de las autoridades públicas, o la ausencia de tales solicitudes, en un período suficientemente representativo. Con esto se quiere decir, en particular, los registros internos u otra documentación elaborados de forma continua con la diligencia debida y certificados en los niveles más altos de la dirección siempre que esta información pueda compartirse legalmente con terceros. Cuando se use esta experiencia práctica para llegar a la conclusión de que el importador de datos no tendrá impedimento para cumplir el presente pliego de cláusulas, deberá estar respaldada por otros elementos pertinentes y objetivos; corresponde a las partes valorar minuciosamente si la suma de estos factores es suficientemente determinante, en términos de fiabilidad y representatividad, para respaldar esta conclusión. En particular, las partes deben tener en cuenta si su experiencia práctica está corroborada y no se ve desmentida, por información que sea fiable y de dominio público o accesible de cualquier otro modo acerca de la existencia o ausencia de solicitudes en el mismo sector o acerca de la aplicación de la normativa de que se trate en la práctica, como jurisprudencia e informes de organismos de supervisión independientes.

Política de privacidad

Fecha de entrada en vigor: 19 de julio de 2023 | Consulte una versión anterior de la Política de Privacidad | Comparar cambios

La protección de los datos personales es muy importante para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, n.º de registro de la empresa: 31333532 como Responsable del tratamiento ("ESET"). Cumplimos con el requisito de transparencia que se estipula en el Reglamento general de protección de datos de la UE ("RGPD"). Para lograr este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes ("Usuario final" o "Usted") sobre los siguientes temas de protección de datos personales:

- Fundamento jurídico del tratamiento de datos personales
- Intercambio y confidencialidad de datos
- Seguridad de datos
- Sus derechos como interesado
- Tratamiento de sus datos personales
- Información de contacto.

Fundamento jurídico del tratamiento de datos personales

Solo hay varias disposiciones jurídicas para el tratamiento de datos que usamos de acuerdo con el marco jurídico aplicable a la protección de los datos personales. El tratamiento de los datos personales en ESET es necesario para la ejecución del Términos de uso ("Términos") con el Usuario final (artículo 6 1] b] del RGPD), que se aplica a la prestación de servicios o productos de ESET a menos que se indique explícitamente lo contrario, por ejemplo:

- El fundamento jurídico de interés legítimo (artículo 6 1] b] del RGPD), que nos permite tratar los datos sobre el uso que los clientes hacen de nuestros Servicios y su satisfacción para ofrecer a los usuarios los mejores niveles de protección, asistencia y experiencia que sea posible. Incluso el marketing es reconocido por la legislación aplicable como un interés legítimo, por lo que nos basamos en ese concepto para las comunicaciones de marketing con nuestros clientes.
- El consentimiento (artículo 6 1] b] del RGPD), que podemos solicitarle en situaciones concretas en las que consideramos que este fundamento jurídico es el más adecuado o si la ley lo requiere.
- El cumplimiento de una obligación legal (artículo 6 1] b] del RGPD), por ejemplo, estipulando los requisitos de comunicación electrónica o retención de facturas o documentos de facturación.

Intercambio y confidencialidad de datos

No compartimos sus datos con terceros. Sin embargo, ESET es una empresa que opera en todo el mundo a través de empresas o socios que forman parte de su red de ventas, servicio y asistencia. La información de licencias, facturación y asistencia técnica tratada por ESET puede transferirse entre filiales o socios para cumplir el EULA en aspectos como la prestación de servicios o la asistencia.

ESET prefiere procesar sus datos en la Unión Europea (UE). No obstante, en función de su ubicación (uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transferir sus datos a un país fuera de la UE. Por ejemplo, utilizamos servicios de terceros para prestar servicios de informática en la nube. En estos casos, seleccionamos cuidadosamente a los proveedores de servicios y ofrecemos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por lo general, aceptamos las cláusulas contractuales tipo de la UE con la normativa contractual aplicable si es necesario.

En algunos países de fuera de la UE, como el Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos comparable. Gracias al nivel de protección de datos, la transferencia de datos a estos países no requiere ninguna autorización o acuerdo especial.

Nos basamos en servicios de terceros relacionados con la informática en la nube proporcionados por Microsoft como proveedor de servicios en la nube.

Seguridad de datos

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar la confidencialidad, la integridad, la disponibilidad y la resistencia de los sistemas y los servicios de procesamiento. En caso de filtración de datos que pongan en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora

correspondiente y a los usuarios finales en calidad de interesados.

Derechos del titular de los datos.

Los derechos de los usuarios finales son importantes para nosotros, sean de un país de la UE o de fuera de la UE. Por lo tanto, en ESET les garantizamos los derechos siguientes. Para ejercer los derechos de los interesados, puede ponerse en contacto con nosotros a través del formulario de asistencia o por correo electrónico en la dirección dpo@eset.sk. Le pediremos la información siguiente con fines de identificación: Nombre, dirección de correo electrónico y, si procede, clave de licencia o número de cliente y empresa. No nos envíe otros datos personales, como la fecha de nacimiento. Cabe destacar que trataremos sus datos personales con fines de identificación y procesamiento de solicitudes.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento solo se aplica si se tratan los datos con su consentimiento previo. Si nos da su consentimiento para tratar sus datos personales, podrá retirarlo en cualquier momento sin explicar los motivos. La retirada del consentimiento solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite.

Derecho de objeción. El derecho a oponerse al tratamiento se aplica si el tratamiento se basa en el interés legítimo de ESET o terceros. Si tratamos sus datos personales para proteger un interés legítimo, puede oponerse a dicho interés legítimo y al tratamiento de sus datos personales en cualquier momento. La oposición solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite. Si tratamos sus datos personales con fines de marketing directo, no es necesario explicar los motivos por los que se opone. Esto también se aplica a la creación de perfiles, ya que está relacionada con el marketing directo. En el resto de casos, debe enviarnos las quejas que tenga en relación con el interés legítimo de ESET para tratar sus datos personales.

En algunos casos, a pesar de su consentimiento, podemos seguir tratando sus datos personales sobre la base de otro fundamento jurídico (como la ejecución de un contrato).

Derecho de acceso. Como interesado, puede solicitar información sobre los datos personales que ESET almacena en cualquier momento sin coste alguno.

Derecho de rectificación. Si tratamos datos personales incorrectos de manera involuntaria, puede pedir que se corrija esta información.

Derecho a eliminar y restringir el tratamiento de datos personales. Como interesado, puede solicitar la eliminación o restricción del tratamiento de sus datos personales. Por ejemplo, si tratamos datos personales con su consentimiento y lo retira sin otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. Sus datos personales también se eliminarán cuando dejen de ser necesarios para los fines indicados al finalizar el periodo de retención.

Si solo utilizamos sus datos personales con fines de marketing directo y revoca su consentimiento o se opone al interés legítimo de ESET, restringiremos el tratamiento una vez que incluyamos sus datos de contacto en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales se eliminarán.

Puede que estemos obligados a almacenar sus datos hasta que expiren las obligaciones de retención y los periodos emitidos por el organismo de legislación o las autoridades supervisoras. También pueden surgir periodos u obligaciones de retención porque la legislación eslovaca así lo exija. En ese caso, los datos correspondientes se eliminarán de forma rutinaria a partir de ese momento.

Derecho a la portabilidad de datos. Dado que es un interesado, le proporcionamos los datos personales que trata ESET en formato XLS.

Derecho a presentar una queja. Como interesado, puede presentar una reclamación ante una autoridad supervisora en cualquier momento. 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. La autoridad supervisora que gestiona cuestiones de datos es la Oficina de protección de datos personales de Eslovaquia, situada en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Tratamiento de sus datos personales

Los servicios prestados por ESET implementados en su producto web se prestan de acuerdo con los Términos de uso ("Términos"), pero algunos pueden requerir atención especial. Queremos proporcionarle más detalles sobre el tratamiento de los datos relacionado con la prestación de nuestros productos y servicios. Prestamos distintos servicios descritos en el Términos y la documentación del documentación. Para que todo funcione, debemos recopilar la siguiente información:

- La administración de los productos de seguridad de ESET requiere el ID y el nombre del puesto, el nombre del producto, información sobre la licencia, información de activación y caducidad e información de hardware y software con relación a los dispositivos administrados 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.
- Otra información tratada puede ser la información sobre el proceso de instalación, incluida la plataforma en la que está instalado nuestro producto, y la información sobre las operaciones y la funcionalidad de nuestros productos o los dispositivos administrados, como la huella digital de hardware, los ID de instalación, los ID de licencia, la dirección IP, la dirección MAC, las direcciones de correo electrónico utilizadas, las coordenadas GPS de un dispositivo móvil o los ajustes de configuración del producto.
- Con fines de seguridad de la infraestructura y de generación de informes, se debe tratar información de telemetría como números de usuarios, políticas, inicios de sesión, tareas, notificaciones, dispositivos administrados, amenazas, etc., así como encabezados HTTP.
- La información de licencia, como el ID de licencia, y los 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 la licencia 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.
- En el caso de las funciones Evaluación de vulnerabilidades y Administración de parches se tratará más información. Para la Evaluación de vulnerabilidades se recopilará y tratará la información relacionada con el nombre e identificador de la vulnerabilidad, la gravedad y el nivel de impacto de los dispositivos gestionados. La función de Administración de revisiones también requiere el nombre, la versión y el proveedor de la aplicación, la versión del parche que falta en el dispositivo y el identificador del parche que falta.
- 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.
- Usted puede proporcionar su opinión como cliente a través de un formulario web y, con fines de seguimiento, puede solicitarse su dirección de correo electrónico, junto con información sobre la licencia y el número de dispositivos administrados.

Si la persona que utiliza nuestros productos o servicios no es el Usuario final que ha adquirido el producto o servicio ni ejecutado los Términos con ESET (como un empleado o familiar del Usuario final o una persona autorizada por este para utilizar el producto o servicio en virtud de los Términos, el tratamiento de los datos se

llevará a cabo según el interés legítimo de ESET conforme al artículo 6 1) f) del RGPD. De este modo, la persona autorizada por el Usuario final podrá utilizar nuestros productos y servicios en virtud de los Términos.

Información de contacto

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