ESET Server Security

Manual de usuario

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

ESET Server Security está desarrollado por ESET, spol. s r.o.

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

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

REV. 19/03/2023

Prólogo

El objetivo de esta guía es ayudarle a sacar el máximo partido de ESET Server Security. Si desea obtener más información sobre cualquiera de las ventanas del programa, pulse **F1** en el teclado con la ventana en cuestión abierta. Aparecerá la página de Ayuda relacionada con la ventana que esté visualizando.

Por motivos de coherencia y para ayudar a evitar confusiones, la terminología empleada en esta guía se basa en los nombres de parámetros de ESET Server Security. Además, utilizamos una serie de símbolos uniformes para destacar temas de interés o importancia especial.

NOTA
Una nota es simplemente una breve observación. A pesar de que puede omitirlas, las notas contienen información valiosa como características específicas o un enlace a un tema relacionado.

IMPORTANTE
Esta información requiere su atención y no se recomienda omitirla. Las notas importantes incluyen información que no resulta esencial, pero sí significativa.

ADVERTENCIA
Se trata de información esencial que debe tratar con más cuidado. Las advertencias se incluyen específicamente para evitar que cometa errores potencialmente peligrosos. Lea y comprenda el texto colocado en indicadores de advertencia, ya que hace referencia a una configuración del sistema muy delicada o a algún aspecto del sistema que conlleva ciertos riesgos.

EJEMPLO
Este es un caso o ejemplo práctico cuyo objetivo es ayudarle a comprender cómo se utiliza una determinada función o característica.

Cuando el elemento que se muestra a continuación aparece en la esquina superior derecha de una página de ayuda, indica una navegación por las ventanas de una interfaz gráfica de usuario (GUI) de ESET Server Security. Utilice estas indicaciones para llegar a la ventana descrita en la página de ayuda correspondiente.

Abrir ESET Server Security
Haga clic en Configuración > Servidor > Configuración del análisis de OneDrive > Registrar. 

Convenciones de formato:

Convención	Significado
Negrita	Encabezados de secciones, nombres de funciones o elementos de la interfaz de usuario, como botones.

Convención	Significado
Cursiva	Marcadores de posición de información que debe proporcionar. Por ejemplo, nombre de archivo o ruta de acceso significa que debe escribir la ruta de acceso real de un nombre o un archivo.
`Courier New`	Ejemplos de código o comandos.
Hipervínculo	Permite acceder de un modo rápido y sencillo a temas con referencias cruzadas o a ubicaciones web externas. Los hipervínculos aparecen resaltados en color azul, y pueden estar subrayados.
%ProgramFiles%	El directorio del sistema operativo Windows que contiene los programas instalados de Windows y otros desarrolladores.

Las páginas de ayuda en línea de ESET Server Security están divididas en diversos capítulos y subcapítulos. Para acceder a la información relevante, explore el contenido de las páginas de ayuda. Igualmente, puede utilizar la búsqueda de texto completo si especifica palabras o frases.

Visión general

ESET Server Security es una solución integrada diseñada especialmente para el entorno de Microsoft Windows Server. ESET Server Security proporciona una protección sólida y eficaz frente a diversos tipos de malware y ofrece dos tipos de protección: antimalware y antiespía.

Características principales

En la siguiente tabla se proporciona una lista de funciones disponibles en ESET Server Security. ESET Server Security es compatible con la mayoría de las ediciones de Microsoft Windows Server 2008 R2 SP1, 2012, 2016 y 2019 en entornos independientes y de clúster. En redes de mayor tamaño, puede utilizar ESET PROTECT para administrar ESET Server Security de forma remota.

Núcleo de producto de 64 bits auténtico	Añadir mayor rendimiento y estabilidad a los componentes principales del producto
Anti-Malware	Una defensa galardonada e innovadora contra el malware. Esta tecnología de vanguardia impide ataques y elimina todo tipo de amenazas, incluidos virus, ransomware, rootkits, gusanos y spyware, con análisis en la nube para conseguir tasas de detección aún mejores. Con un tamaño reducido, no sobrecarga los recursos del sistema, por lo que no compromete su rendimiento. Utiliza un modelo de seguridad por capas. Cada capa, o fase, tiene varias tecnologías básicas. La fase *anterior a la ejecución* tiene tecnologías como *Análisis UEFI, Protección contra los ataques de red, Reputación y caché, Sandbox en el producto y Detecciones de ADN*. Las tecnologías de la fase de *ejecución* son *Bloqueador de exploits, Protección contra ransomware, Análisis avanzado de memoria* y *Análisis de scripts (AMSI)*, y la fase *posterior a la ejecución* utiliza *Protección contra botnets, Sistema de protección de malware en la nube* y *Entorno de pruebas*. Este rico conjunto de funciones con tecnologías básicas proporciona un nivel de protección sin rival.
Análisis de OneDrive	Se trata de una nueva posibilidad añadida a la función para analizar archivos ubicados en el almacenamiento en la nube OneDrive (para la cuenta empresarial de Office 365).
Análisis Hyper-V	Se trata de una nueva tecnología que permite analizar discos de máquina virtual en Microsoft Hyper-V Server sin necesidad de tener ningún "Agente" instalado en la máquina virtual determinada.

Núcleo de producto de 64 bits auténtico	Añadir mayor rendimiento y estabilidad a los componentes principales del producto
ESET Dynamic Threat Defense (EDTD)	Servicio de ESET en la nube. Cuando ESET Server Security detecta código o comportamiento sospechosos, impide futuras actividades que supongan una amenaza poniendo ese código temporalmente en cuarentena en ESET Dynamic Threat Defense. Una muestra sospechosa se envía automáticamente al servidor de ESET Dynamic Threat Defense para que la analicen motores de detección de malware avanzados. A continuación, su ESET Server Security recibe un recibe un resultado del análisis. El archivo sospechoso se trata en función del resultado.
Clúster de ESET	El Clúster de ESET permite la administración de varios servidores desde una misma ubicación. La unión de estaciones de trabajos a nodos ofrecerá automatización adicional de la administración gracias a la posibilidad de distribuir una política de configuración entre todos los miembros del clúster. La creación de los propios clústeres puede efectuarse con el nodo instalado, que posteriormente puede instalar e iniciar todos los nodos de forma remota. Los productos para servidor de ESET se pueden comunicar entre sí e intercambiar datos como configuración y notificaciones, así como sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias de productos. Esto permite contar con la misma configuración del producto en todos los miembros de un clúster. Los clústeres de conmutación por error de Windows y los clústeres de equilibrio de carga de red (NLB) son compatibles con ESET Server Security. Además, puede agregar miembros al Clúster de ESET manualmente sin necesidad de contar con un clúster de Windows específico. Los Clústeres de ESET funcionan tanto en entornos de dominio como en entornos de grupo de trabajo.
Exclusiones automáticas	Detección y exclusión automáticas de aplicaciones y archivos del servidor críticos para garantizar un funcionamiento y un rendimiento óptimos.
Exclusiones de procesos	Excluye procesos específicos del análisis en el acceso antimalware. El análisis en el acceso antimalware puede causar conflictos en determinadas situaciones, por ejemplo, durante un proceso de copia de seguridad o migraciones en vivo de máquinas virtuales. Las exclusiones de procesos ayudan a reducir al mínimo el riesgo de que se produzcan esos conflictos y a mejorar el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo en el rendimiento y la estabilidad generales de todo el sistema. La exclusión de un proceso o una aplicación es una exclusión de su archivo ejecutable (*.exe*).
eShell ESET Shell	eShell es una interfaz de línea de comandos que ofrece a los usuarios avanzados y a los administradores opciones más completas para la gestión de los productos de servidor de ESET.
ESET PROTECT	Una mejor integración con ESET PROTECT, incluida la capacidad de programar análisis a petición. Si desea obtener más información, consulte la Ayuda en línea de ESET PROTECT.
Instalación basada en componentes	La instalación se puede personalizar para que contenga solo determinados módulos del producto.

Novedades

Nuevas funciones y mejoras en ESET Server Security:

- Núcleo de producto de 64 bits auténtico
- Análisis de OneDrive
- ESET Dynamic Threat Defense (EDTD)
- Compatibilidad con ESET Enterprise Inspector
- ESET RMM
- Aislamiento de la red
- Detección de aprendizaje automático
- Registros de auditoría

- Microactualizaciones de componentes del programa

Tipos de protección

Hay dos tipos de protección:

- Protección Anti-Malware
- Protección antiespía

La protección antimalware y antiespía es una de las funciones básicas del producto ESET Server Security. Esta protección evita ataques maliciosos contra el sistema controlando las comunicaciones de archivos, correo electrónico e Internet. Si se detecta una amenaza, el módulo de detección puede eliminarla bloqueándola y, a continuación, desinfectándola, eliminándola o poniéndola en cuarentena.

Preparativos de la instalación

Hay algunos pasos que le recomendados realizar durante los preparativos de la instalación del producto:

- Después de adquirir ESET Server Security, descargue el paquete de instalación `.msi` del sitio web de ESET.

- Asegúrese de que el servidor en el que tiene previsto instalar ESET Server Security cumple con los requisitos del sistema.

- Inicie sesión en el servidor con una Cuenta de administrador.

> NOTA
> Recuerde que el instalador debe ejecutarse con la cuenta de administrador integrado o la cuenta de administrador de dominio (en el caso de que tenga la cuenta de administrador local desactivada). Los demás usuarios no tienen los derechos de acceso suficientes, aunque sean miembros de un grupo de administradores. Por este motivo debe utilizar la cuenta de administrador integrado, ya que la instalación solo se puede completar con la cuenta de administrador local o de dominio.

- Si va a realizar una actualización desde una instalación existente de ESET Server Security, le recomendamos realizar una copia de seguridad de su configuración actual con la función Exportar configuración.

- Quite o desinstale cualquier software antivirus de terceros del sistema, si procede. Se recomienda usar ESET AV Remover. Para obtener una lista de software antivirus de terceros que puede quitarse con ESET AV Remover, consulte este artículo de la Base de conocimiento.

- Si va a realizar ESET Server Security la instalación sobre Windows Server 2016, Microsoft recomienda desinstalar Características de Windows Defender y cancelar la inscripción en la ATP de Windows Defender para evitar problemas causados por tener varios productos antivirus instalados en una máquina.

- Si está instalando ESET Server Security en Windows Server 2019, Microsoft Windows Server 2022 Microsoft recomienda poner Windows Defender en el **modo pasivo** para evitar los problemas que puede ocasionar tener varios productos antivirus instalados en un equipo.

Puede ejecutar el instalador de ESET Server Security en dos modos de instalación:

- Interfaz gráfica de usuario (GUI)
  Este es el tipo de instalación recomendado de un asistente de instalación.

- Instalación silenciosa/desatendida
  Además del asistente de instalación, puede optar por instalar ESET Server Security de forma silenciosa a través de la línea de comandos.

> IMPORTANTE
> Si es posible, le recomendamos encarecidamente que instale ESET Server Security en un sistema operativo recién instalado o configurado. Si tiene que instalarlo en un sistema existente, le recomendamos que desinstale la versión de ESET Server Security, reinicie el servidor e instale el nuevo ESET Server Security a continuación.

- Actualización a una versión más reciente
  Si utiliza una versión anterior de ESET Server Security, puede elegir el método de actualización adecuado.

Una vez que haya instalado o actualizado correctamente ESET Server Security, tendrá que realizar los siguientes pasos:

- Activación del producto
  La disponibilidad de un método concreto de activación en la ventana de activación puede variar en función del país, además de los medios de distribución.

- Ajuste de la configuración general
  Si desea ajustar su ESET Server Security, modifique la configuración avanzada de cada una de sus funciones para adaptarse a sus necesidades.

Requisitos del sistema

Sistemas operativos compatibles:

- Microsoft Windows Server 2022 (Server Core y Experiencia de escritorio)
- Microsoft Windows Server 2019 (Server Core y Experiencia de escritorio)
- Microsoft Windows Server 2016 (Server Core y Experiencia de escritorio)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 con KB4474419 y KB4490628 instalados (lea la compatibilidad necesaria con SHA-2)
- Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2)

> NOTA
> En Windows Server 2008 R2 SP1, el componente **Protección de la red** está desactivado de forma predeterminada en la instalación **Típica**. Utilice la instalación **Personalizada** para instalar este componente.

Servidores Storage, Small Business y MultiPoint:

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation
- Microsoft Windows Small Business Server 2011 SP1 (x64) con KB4474419 y KB4490628 instalado

- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2010

Sistemas operativos host compatibles con el rol Hyper-V:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1: las máquinas virtuales solo se pueden analizar cuando están desconectadas

Los requisitos de hardware dependen de la versión del sistema operativo. Recomendamos la lectura de la documentación del producto Microsoft Windows Server para obtener información detallada sobre los requisitos de hardware.

> NOTA
> Se recomienda encarecidamente instalar el Service Pack más reciente de su sistema operativo Microsoft Server y la versión para servidor de la aplicación antes de instalar el producto de seguridad ESET. Además, le recomendamos que instale las actualizaciones y las correcciones de errores de Windows más recientes en cuanto estén disponibles.

Requisitos mínimos de hardware:

Componente	Requisito
Procesador	Intel o AMD x64 de un núcleo
Memoria	256 MB de memoria libre
Disco duro	700 MB de espacio libre en disco
Resolución de la pantalla	800 × 600 píxeles o superior

Compatibilidad necesaria con SHA-2

Microsoft anunció el desuso del algoritmo hash seguro 1 (SHA-1) e inició el proceso de migración a SHA-2 a principios de 2019. Por lo tanto, todos los certificados firmados con el algoritmo SHA-1 dejarán de reconocerse y provocarán alertas de seguridad. Por desgracia, la seguridad del algoritmo hash SHA-1 se ha reducido con el

tiempo debido a los puntos débiles detectados en el algoritmo, el mayor rendimiento de los procesadores y la llegada de la informática en nube.

El algoritmo hash SHA-2 (como sucesor de SHA-1) es ahora el método preferido para garantizar la durabilidad de la seguridad SSL. Consulte el artículo de Microsoft Docs acerca de Algoritmos hash y de firma para obtener más información.

> NOTA
> Este cambio significa que en sistemas operativos sin compatibilidad con SHA-2, su solución de seguridad de ESET ya no podrá actualizar sus módulos, incluido el motor de detección, por lo que ESET Server Security deja de ser totalmente funcional y no puede ofrecer una protección suficiente.

Si ejecuta **Microsoft Windows Server 2008 R2 SP1** o **Microsoft Windows Small Business Server 2011 SP1**, asegúrese de que su sistema sea compatible con SHA-2. Aplique los parches de acuerdo con la versión concreta de su sistema operativo, como se indica a continuación:

- **Microsoft Windows Server 2008 R2 SP1**: aplique KB4474419 y KB4490628 (puede que sea necesario reiniciar otra vez el sistema)
- **Microsoft Windows Server 2011 SP1** (x64): aplique KB4474419 y KB4490628 (puede que sea necesario reiniciar otra vez el sistema)

> IMPORTANTE
> Una vez que haya instalado las actualizaciones y reiniciado el sistema, abra la GUI de ESET Server Security para comprobar su estado. Si el estado es naranja, realice un reinicio adicional del sistema. A continuación, el estado debe ser verde, lo que indica la protección máxima.

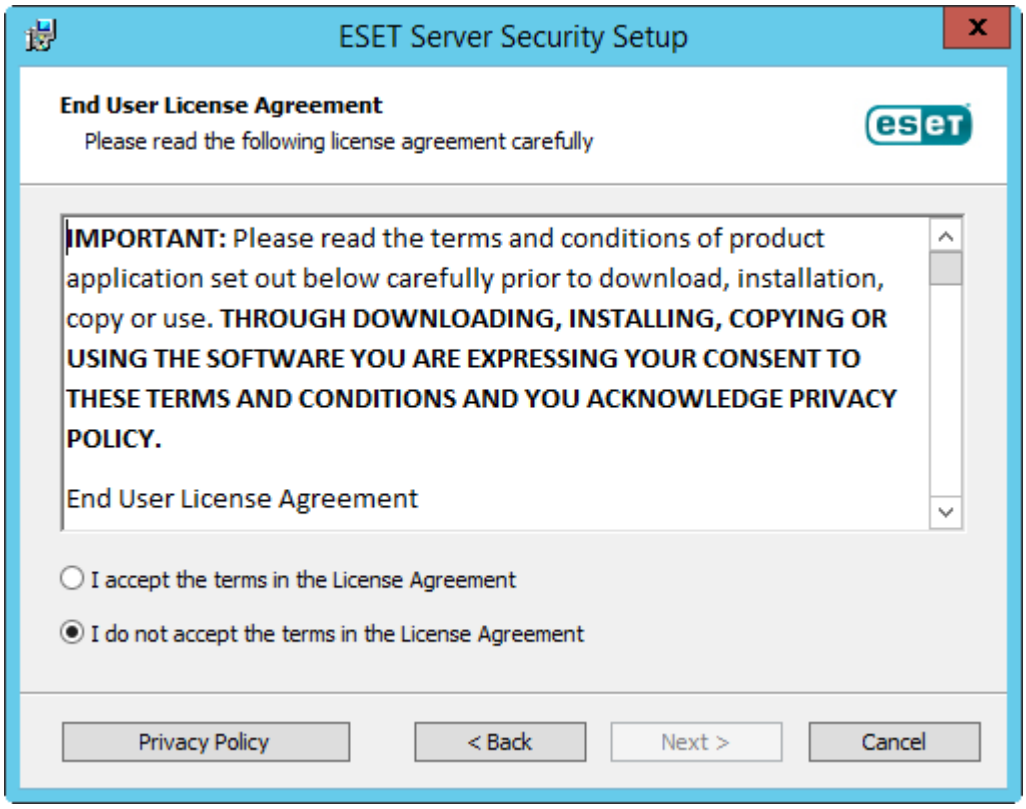
> NOTA
> Se recomienda encarecidamente instalar el Service Pack más reciente de su sistema operativo Microsoft Server y la versión para servidor de la aplicación. Además, le recomendamos que instale las actualizaciones y las correcciones de errores de Windows más recientes en cuanto estén disponibles.

Pasos de instalación de ESET Server Security

Se trata de un asistente de instalación típica de interfaz gráfica de usuario (GUI). Haga doble clic en el paquete `.msi` y siga los pasos para instalar ESET Server Security:

1. Haga clic en **Siguiente** para continuar o en **Cancelar** si desea salir de la instalación.
2. El asistente de instalación se ejecuta en un idioma que se especifica como **Ubicación principal** de un ajuste **Región** > **Ubicación** del sistema operativo (o **Ubicación actual** de un ajuste **Región e idioma** > **Ubicación** de sistemas anteriores). Utilice el menú desplegable para seleccionar **Idioma del producto** en el que se instalará ESET Server Security. El idioma seleccionado para ESET Server Security es independiente del idioma que se mostrará en el asistente de instalación.

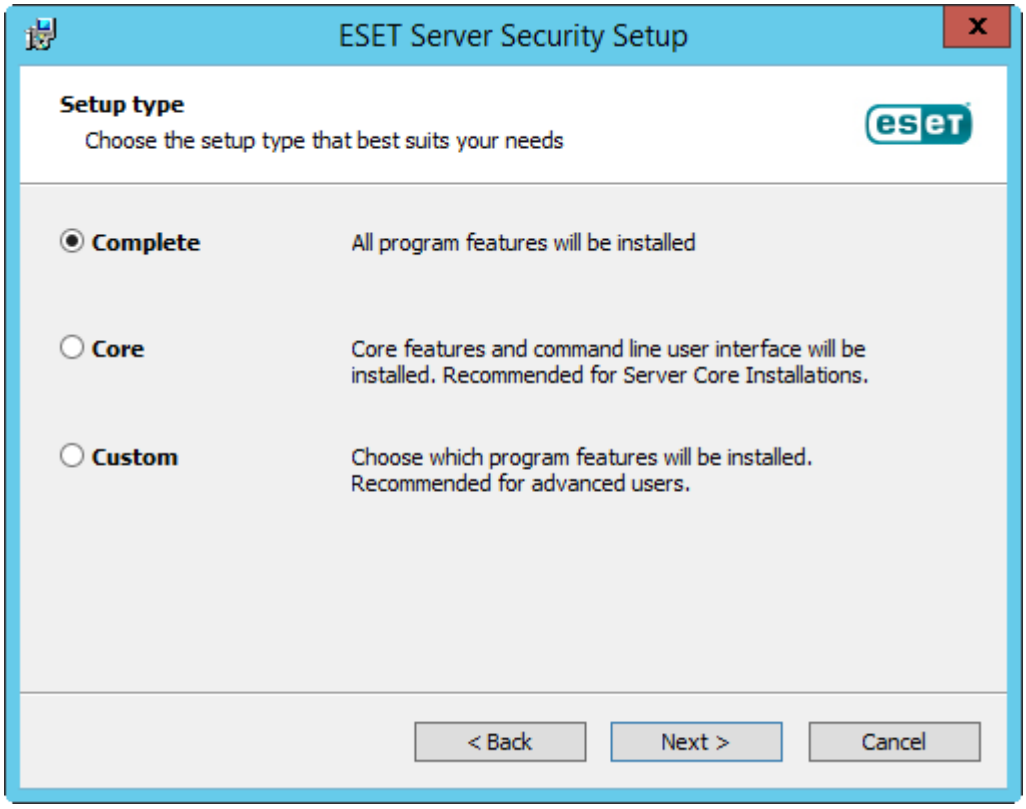
3.Haga clic en **Siguiente** y se mostrará el Acuerdo de licencia para el usuario final. Después de confirmar que acepta el **Acuerdo de licencia para el usuario final** (EULA) y la Política de privacidad, haga clic en **Siguiente**.



4.Seleccione uno de los tipos de instalación disponibles (la disponibilidad dependerá de su sistema operativo):

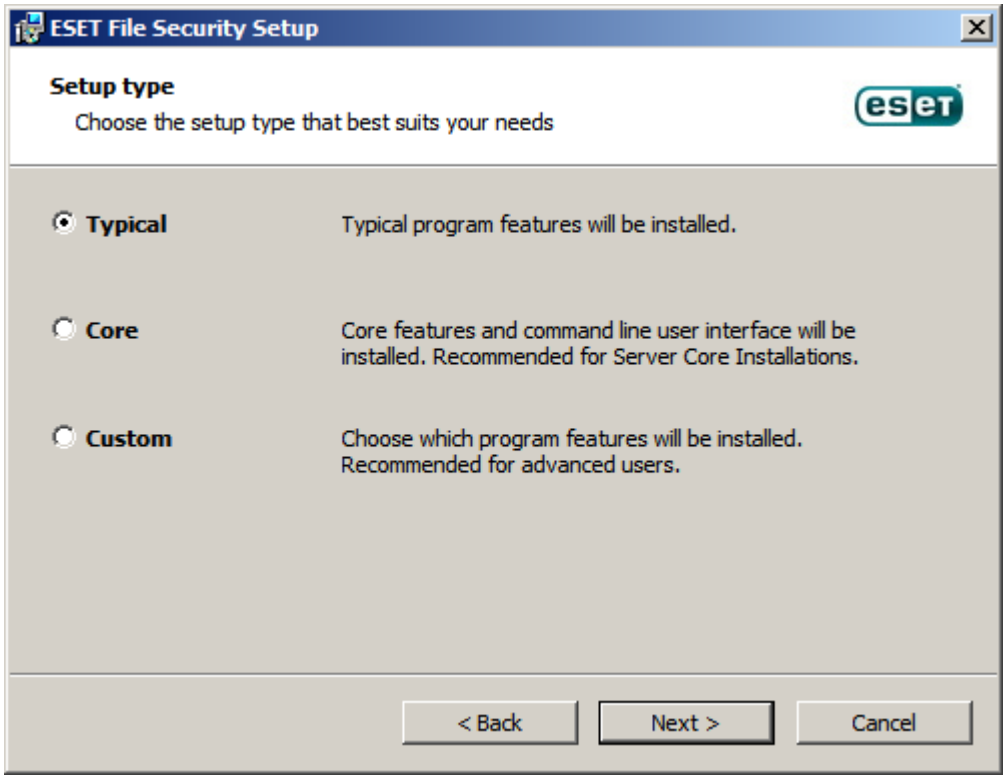
Completo

Instala todas las funciones de ESET Server Security (también se denomina instalación completa). Este es el tipo de instalación recomendada, disponible para **Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials y 2019 Essentials**.



Típico

Instala las funciones recomendadas de ESET Server Security. Disponible para 2008 R2 SP1 y 2011.



Núcleo

Este tipo de instalación está pensado para las versiones Core de Windows Server. Los pasos de instalación son los mismos que en el caso de la instalación completa, pero solo se instalarán las funciones principales y la interfaz de usuario de la línea de comandos. A pesar de que la instalación de tipo Núcleo está pensada principalmente para las versiones Core de Windows Server, también puede usarla en versiones normales de Windows Server si lo prefiere. El producto de seguridad de ESET instalado con la opción de instalación de tipo Núcleo no tendrá interfaz gráfica de usuario. Esto significa que, al trabajar con ESET Server Security, solo podrá utilizar la interfaz de usuario de la línea de comandos. Si desea obtener información detallada y otros parámetros especiales, consulte la sección Instalación de la línea de comandos.

EJEMPLO
Para ejecutar la instalación de tipo Core a través de la línea de comandos, utilice el siguiente comando de muestra:

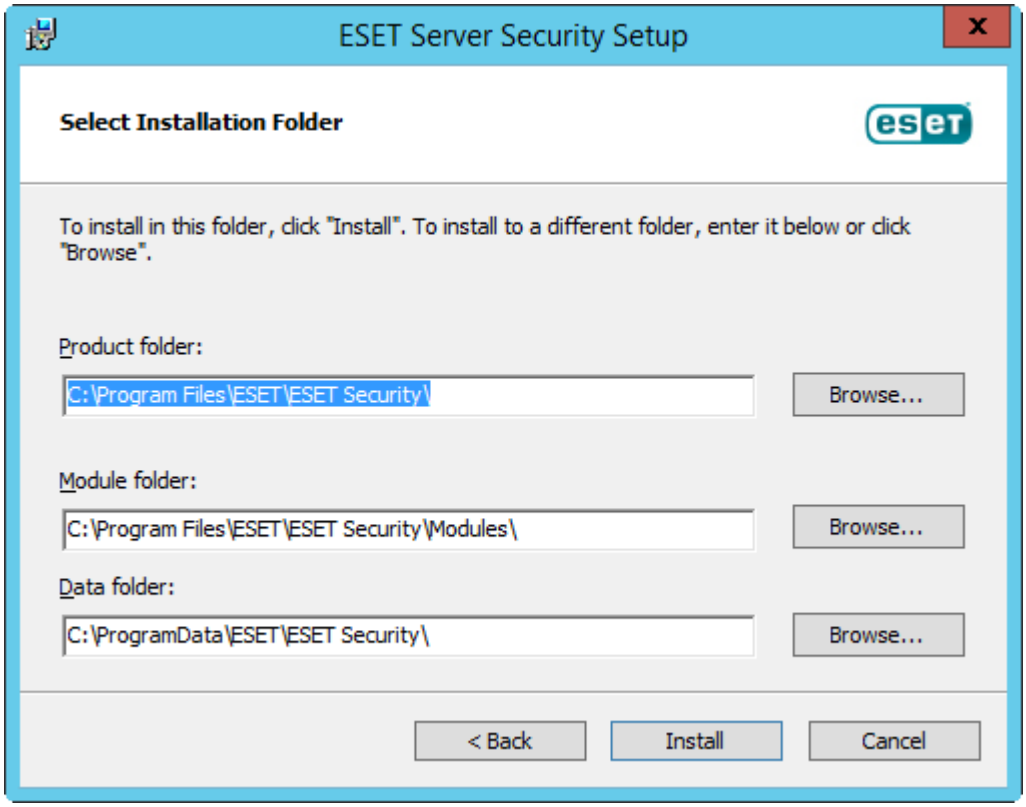
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base
```

Personalizado

Le permite elegir las funciones de ESET Server Security que se instalarán en el sistema. Antes de que se inicie la instalación aparecerá una lista de módulos y funciones del producto. Resulta útil si desea personalizar ESET Server Security con solo los componentes que necesita.

NOTA
En Windows Server 2008 R2 SP1, la instalación del componente **Protección de la red** está desactivada de forma predeterminada (instalación **Típica**). Si desea instalar este componente, elija el tipo de instalación **Personalizada**.

5.Se le pedirá que seleccione la ubicación en la que se instalará ESET Server Security. De forma predeterminada, el programa se instala en *C:\Program Files\ESET\ESET Server Security*. Haga clic en **Examinar** para cambiar esta ubicación (no recomendado).



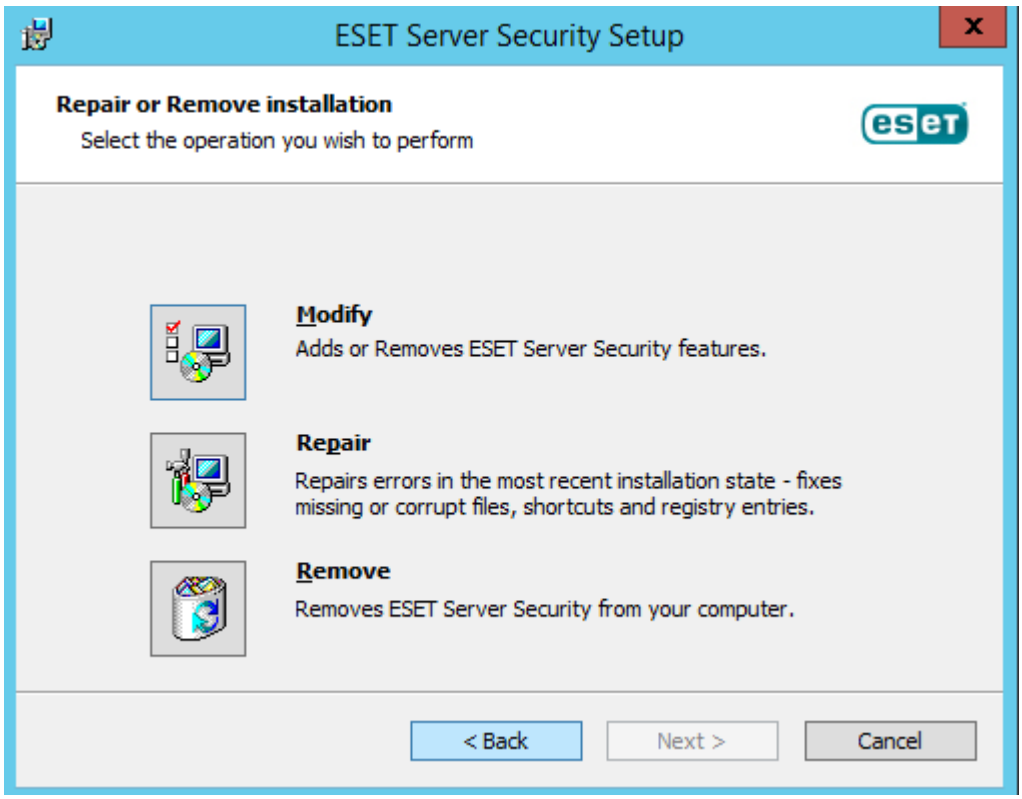
6.Haga clic en **Instalar** para comenzar la instalación. Cuando la instalación finalice, se iniciará la interfaz gráfica de usuario (GUI) de ESET y se mostrará el icono de bandeja en el área de notificación (bandeja

del sistema).

Modificación de una instalación existente

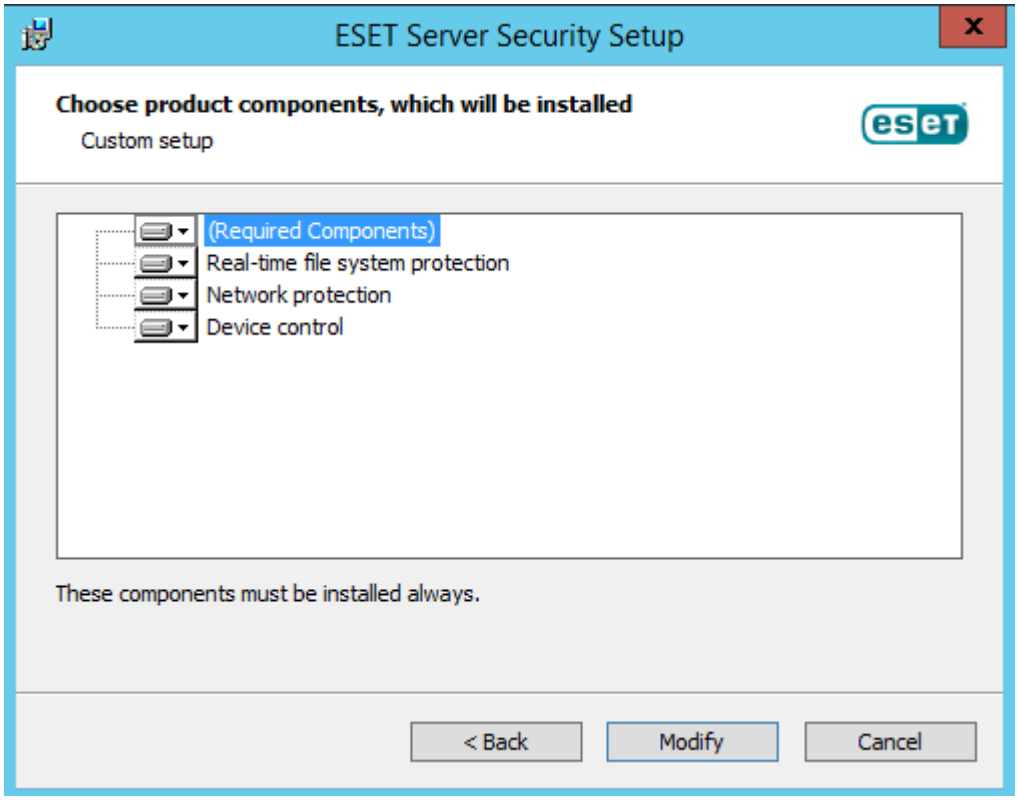
Es posible agregar o quitar componentes que se incluyen en la instalación. Para ello, puede ejecutar el paquete de instalación `.msi` que utilizó en la instalación inicial o acceder a **Programas y características** (disponible desde el Panel de control de Windows), hacer clic con el botón derecho en ESET Server Security y seleccionar **Cambiar**. Siga los pasos indicados a continuación para agregar o quitar componentes.

Existen tres opciones disponibles: puede **Modificar** los componentes instalados, **Reparar** la instalación de ESET Server Security o **Quitar** (desinstalar) por completo.



Si elige **Modificar**, aparecerá una lista de los componentes del programa disponibles.

Elija los componentes que desee agregar o quitar. Es posible agregar o quitar varios componentes al mismo tiempo. Haga clic en el componente y seleccione la opción que desee en el menú desplegable:



Tras seleccionar una opción, haga clic en **Modificar** para efectuar las modificaciones.

NOTA
Puede modificar los componentes instalados en cualquier momento con solo ejecutar el instalador. En el caso de la mayoría de los componentes, no es necesario reiniciar el servidor para efectuar el cambio. La interfaz gráfica de usuario (GUI) se reiniciará y solo verá los componentes que ha elegido instalar. En el caso de los componentes que requieren un reinicio del servidor, el instalador de Windows le pedirá que reinicie y los nuevos componentes estarán disponibles cuando el servidor esté en línea de nuevo.

Instalación silenciosa/desatendida

Ejecute el siguiente comando para completar la instalación a través de la línea de comandos: `msiexec /i <packagename> /qn /l*xv msi.log`

NOTA
En Windows Server 2008 R2 SP1, no se instalará la función **Protección de la red**.

Para garantizar que la instalación se ha realizado correctamente, o en el caso de que se produzca algún problema con la instalación, utilice el Visor de eventos de Windows para comprobar el **Registro de aplicaciones** (busque los registros de Source: MsiInstaller).

EJEMPLO
Instalación completa en un sistema de 64 bits:

```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Cuando la instalación finalice, se iniciará la interfaz gráfica de usuario (GUI) de ESET y se mostrará el icono de bandeja en el área de notificación (bandeja del sistema).

EJEMPLO
Instalación del producto en un **idioma determinado** (alemán):
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
Consulte los **Parámetros de idioma** en la instalación de línea de comandos para obtener más información y la lista de los códigos de idioma.

IMPORTANTE
Cuando especifique valores para el parámetro `REINSTALL`, debe indicar el resto de funciones que no se utilizarán como valores para los parámetros `ADDLOCAL` o `REMOVE`. Para que la instalación de línea de comandos se ejecute correctamente debe indicar todas las funciones como valores para los parámetros `REINSTALL`, `ADDLOCAL` y `REMOVE`. Es posible que no pueda añadir ni quitar una función si no utiliza el parámetro `REINSTALL`.
Consulte la sección Instalación de la línea de comandos para obtener una lista completa de funciones.

EJEMPLO
Eliminación completa (desinstalación) de un sistema de 64 bits:
```
msiexec /x efsw_nt64.msi /qn /l*xv msi.log
```

NOTA
El servidor se reiniciará automáticamente después de realizar la desinstalación correctamente.

Instalación de la línea de comandos

Las siguientes opciones están pensadas para usarlas **solo para la interfaz de usuario con nivel reducido**, **básico** y **ninguno**. Consulte la documentación de la versión de **msiexec** utilizada para los modificadores de la línea de comandos correspondientes.

Parámetros admitidos:

APPDIR=<ruta de acceso>

- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de la aplicación
- Por ejemplo: `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<ruta de acceso>

- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de los datos de la aplicación

MODULEDIR=<ruta de acceso>

- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación del módulo

ADDLOCAL=<lista>

- Instalación de componentes: lista de características no obligatorias que se pueden instalar localmente.
- Uso con los paquetes ESET `.msi`: `efsw_nt64.msi /qn ADDLOCAL=<list>`

- Para obtener más información sobre la propiedad `ADDLOCAL`, consulte https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- La lista `ADDLOCAL` es una lista separada por comas de todas las funciones que se van a instalar.
- Al seleccionar una función para instalarla, se debe incluir en la lista y de forma explícita toda la ruta de acceso (todas las funciones principales).

REMOVE=<lista>

- Instalación de componentes: función principal que no desea tener instalada localmente.
- Uso con los paquetes ESET `.msi`: `efsw_nt64.msi /qn REMOVE=<list>`
- Para obtener más información sobre la propiedad `REMOVE`, consulte https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove
- La lista `REMOVE` es una lista separada por comas de funciones principales que no se instalarán (o que se quitarán, si ya están instaladas).
- Es suficiente especificar las funciones principales. No es necesario incluir explícitamente en la lista todas las funciones secundarias.

ADDEXCLUDE=<lista>

- La lista `ADDEXCLUDE` es una lista separada por comas de todos los nombres de funciones que no se instalarán.
- Cuando seleccione una función para no instalarla, toda la ruta de acceso (es decir, todas sus funciones secundarias) y las funciones invisibles relacionadas deberán incluirse en la lista de forma explícita.
- Uso con los paquetes ESET `.msi`: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

> NOTA
> `ADDEXCLUDE` no se puede usar con `ADDLOCAL`.

Presencia de características

- **Obligatoria**: la característica se instala siempre.
- **Opcional**: puede cancelarse la selección de la función para que no se instale.
- **Invisible**: característica lógica obligatoria para que otras características funcionen correctamente.

Lista de funciones de ESET Server Security:

> IMPORTANTE
> Los nombres de las funciones distinguen entre mayúsculas y minúsculas, por ejemplo, `RealtimeProtection` no es igual que `REALTIMEPROTECTION`.

Nombre de la característica	Presencia de características
`SERVER`	Obligatoria
`RealtimeProtection`	Obligatoria
`WMIProvider`	Obligatoria
`HIPS`	Obligatoria
`Updater`	Obligatoria
`eShell`	Obligatoria
`UpdateMirror`	Obligatoria
`DeviceControl`	Opcional

Nombre de la característica	Presencia de características
DocumentProtection	Opcional
WebAndEmail	Opcional
ProtocolFiltering	Invisible
NetworkProtection	Opcional
IdsAndBotnetProtection	Opcional
Rmm	Opcional
WebAccessProtection	Opcional
EmailClientProtection	Opcional
MailPlugins	Invisible
Cluster	Opcional
_Base	Obligatoria
eula	Obligatoria
ShellExt	Opcional
_FeaturesCore	Obligatoria
GraphicUserInterface	Opcional
SysInspector	Opcional
SysRescue	Opcional
EnterpriseInspector	Opcional

Si desea quitar cualquiera de las funciones que se indican a continuación, debe quitar todo el grupo especificando todas las funciones que pertenezcan al grupo. De lo contrario, la función no se quitará. Aquí hay dos grupos (cada línea representa un grupo):

```
GraphicUserInterface,ShellExt

NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailP
lugins,EmailClientProtection
```

EJEMPLO
Excluya la sección **Protección de la red** (incluidas las funciones secundarias) de la instalación con el parámetro `REMOVE` y la especificación de la función principal únicamente:
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```
También puede utilizar el parámetro `ADDEXCLUDE`, pero deberá especificar además todas las funciones secundarias:
```
msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

EJEMPLO
Ejemplo de instalación de tipo **Núcleo**:
```
msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

Si desea que ESET Server Security se configure automáticamente después de realizar la instalación, puede especificar los parámetros de configuración básicos en el comando de instalación.

EJEMPLO
Instalación de ESET Server Security y desactivación de ESET LiveGrid®:
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

Lista de todas las propiedades de configuración:

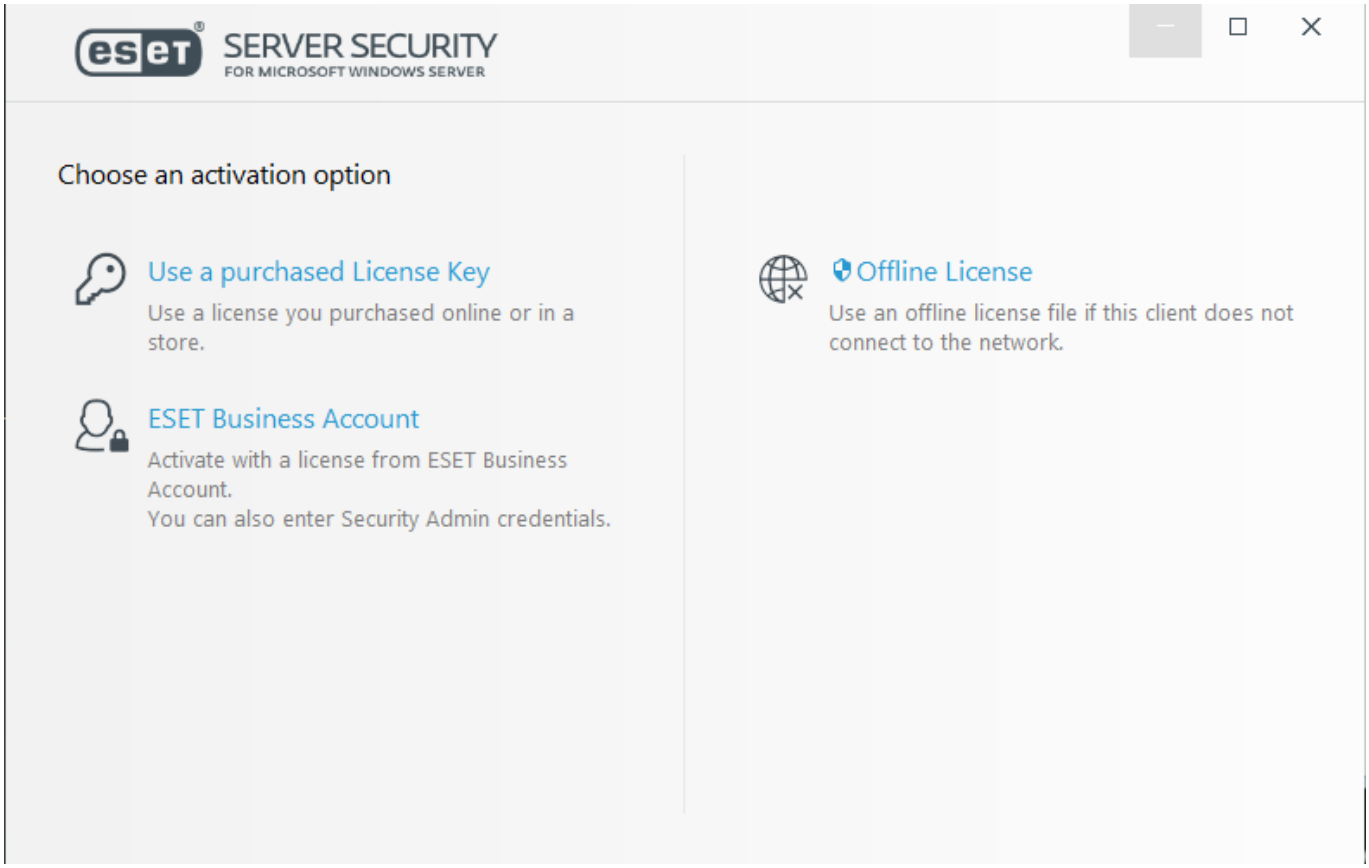
Interruptor	Valor
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0: desactivado, 1: activado
CFG_LIVEGRID_ENABLED=1/0	0: desactivado, 1: activado
FIRSTSCAN_ENABLE=1/0	0: desactivado, 1: activado
CFG_PROXY_ENABLED=0/1	0: desactivado, 1: activado
CFG_PROXY_ADDRESS=<ip>	Dirección IP del proxy
CFG_PROXY_PORT=<port>	Número de puerto de proxy
CFG_PROXY_USERNAME=<user>	Nombre de usuario para autenticación
CFG_PROXY_PASSWORD=<pass>	Contraseña para autenticación

Parámetros de idioma: Idioma del producto (debe especificar ambos parámetros)

Interruptor	Valor
PRODUCT_LANG=	Decimal de LCID (ID de configuración regional), por ejemplo, 1033 para *English - United States*; consulte la lista de códigos de idiomas.
PRODUCT_LANG_CODE=	Cadena de LCID (nombre de cultura de idioma) en minúsculas, por ejemplo, en-us para *English - United States*; consulte la lista de códigos de idiomas.

Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto.



Puede utilizar cualquiera de estos métodos para activar ESET Server Security:

Introduzca una clave de licencia

Se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.

ESET Business Account

Utilice esta opción si se ha registrado y tiene la ESET Business Account (EBA) donde se ha importado la licencia de ESET Server Security. También puede especificar las credenciales de **Administrador de seguridad** que utiliza en el portal de ESET License Administrator.

Archivo de licencia sin conexión

Se trata de un archivo generado automáticamente que se transferirá al producto de ESET para proporcionar información sobre la licencia. El archivo de licencia sin conexión se genera en el portal de licencias y se utiliza en aquellos entornos en los que la aplicación no se puede conectar a la autoridad de concesión de licencias.

Haga clic en **Activar más tarde** con ESET PROTECT si su ordenador es miembro de una red administrada y el administrador realizará la activación remota desde ESET PROTECT. Si desea activar este cliente más adelante, también puede usar esta opción.

Seleccione **Ayuda y soporte técnico** > **Administrar licencias** en la ventana principal del programa para administrar la información de su licencia cuando desee. Verá el ID de la licencia pública utilizado para que ESET identifique su producto y para la identificación de la licencia. El nombre de usuario con el que se ha registrado el ordenador está disponible en la sección Acerca de; esta puede mostrarse al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema .

Tras activar correctamente ESET Server Security, se abrirá la ventana principal del programa y se mostrará el estado actual en la página Estado de la protección. Es posible que, en un primer momento, se requiera su atención; por ejemplo se le preguntará si desea formar parte de ESET LiveGrid®.

En la ventana principal del programa también se mostrarán notificaciones sobre otros elementos, como actualizaciones del sistema (actualizaciones de Windows) o actualizaciones del motor de detección. Una vez resueltos todos los asuntos que requieran atención, el estado de supervisión cambiará a verde y mostrará el estado **Está protegido**.

El producto también se puede activar desde el menú principal en **Ayuda y soporte técnico** > **Activar producto** o **Estado de supervisión** > **El producto no está activado**.

NOTA
ESET PROTECT puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador.

ESET Business Account

ESET Business Account le permite administrar varias licencias. Si no tiene ESET Business Account, haga clic en **Crear cuenta** para que se abra el portal de ESET Business Account, donde podrá registrarse.

NOTA
Para obtener más información, consulte el manual de usuario de ESET Business Account (EBA).

Si utiliza las credenciales de Administrador de seguridad y ha olvidado su contraseña, haga clic en **¿Ha olvidado su**

contraseña? y será redirigido al portal de ESET License Administrator. Introduzca su dirección de correo electrónico y haga clic en **Enviar** para confirmar. A continuación, recibirá un mensaje con instrucciones para restablecer la contraseña.

La activación se ha realizado correctamente

ESET Server Security se ha activado correctamente. A partir de ahora, ESET Server Security recibirá actualizaciones periódicas para identificar las amenazas más recientes y proteger su ordenador. Haga clic en **Listo** para finalizar la activación del producto.

Error de activación

ESET Server Security no se ha activado correctamente. Asegúrese de que ha introducido la **Clave de licencia** correcta o adjuntado una **Licencia sin conexión**. Si dispone de una **Licencia sin conexión** diferente, introdúzcala. Para comprobar la clave de licencia introducida, haga clic en **Comprobar la clave de licencia de nuevo** o en **Introducir una licencia distinta**.

Si no puede realizar la activación, consulte el asistente de solución de problemas de activación.

Licencia

Se le solicitará que seleccione la licencia asociada a su cuenta que se usará con ESET Server Security. Haga clic en **Continuar** para seguir con la activación.

Actualización a una versión más reciente

Las versiones nuevas de ESET Server Security ofrecen mejoras o solucionan problemas que no se pueden corregir con las actualizaciones automáticas de los módulos del programa.

Métodos de actualización:

- **Desinstalar/Instalar**: quitar la versión anterior antes de instalar la nueva. versión más reciente de ESET Server Security. Exporte los ajustes de su ESET Server Security existente si desea conservar la configuración. Desinstale ESET Server Security y reinicie el servidor. Realice una nueva instalación con el instalador que ha descargado. Importe los ajustes para cargar su configuración. Recomendamos este procedimiento si tiene un solo servidor que ejecuta ESET Server Security.

- **Sobrescritura**: un método de actualización que no elimina la versión existente, sino que instala la nueva versión de ESET Server Security sobre ella.

> IMPORTANTE
> Es necesario que **no tenga actualizaciones de Windows pendientes** en el servidor, **ni reinicios pendientes** debidos a actualizaciones de Windows o a cualquier otro motivo. Si intenta realizar la actualización local con actualizaciones de Windows o reinicios pendientes, es posible que la versión existente de ESET Server Security no se quite correctamente. También tendrá problemas si decide quitar la versión anterior de ESET Server Security de forma manual más adelante.

NOTA
Durante la actualización de ESET Server Security será necesario reiniciar el servidor.

- Remoto: para entornos de red de grandes dimensiones administrados por ESET PROTECT. Este es, básicamente, un método de actualización limpio, pero se lleva a cabo de forma remota. Es útil si tiene varios servidores que ejecutan ESET Server Security.

- Asistente de Clúster de ESET: también puede utilizarse como método de actualización. Recomendamos este método para 2 o más servidores con ESET Server Security. Este es, básicamente, un método de actualización local, pero ejecutado mediante el Clúster de ESET. Una vez completada la actualización, puede continuar utilizando el Clúster de ESET y aprovechar sus funciones.

NOTA
Una vez actualizado ESET Server Security, se recomienda revisar todos los ajustes para verificar que están correctamente configurados y cumplen sus necesidades.

Actualización a través de ESET PROTECT

ESET PROTECT le permite actualizar varios servidores que ejecuten una versión anterior de ESET Server Security. Este método tiene la ventaja de actualizar muchos servidores al mismo tiempo y garantizar que cada ESET Server Security se configure de forma idéntica (si se desea).

El procedimiento consta de las siguientes fases:

- Debe **Actualizar el primer servidor** manualmente mediante la instalación de la versión más reciente de ESET Server Security sobre su versión existente para conservar toda la configuración, incluidas las reglas, numerosas listas blancas y negras, etc. Esta fase se realiza localmente en el servidor que ejecuta ESET Server Security.

- Debe **Solicitar configuración** de la nueva actualización de ESET Server Security a la versión 7.x y **Convertir en política** en ESET PROTECT. Más adelante, la política se aplicará a todos los servidores actualizados. Esta fase se realiza de forma remota con ESET PROTECT, así como las siguientes fases.

- **Ejecutar la tarea de Desinstalación de software** en todos los servidores que utilicen la versión anterior de ESET Server Security.

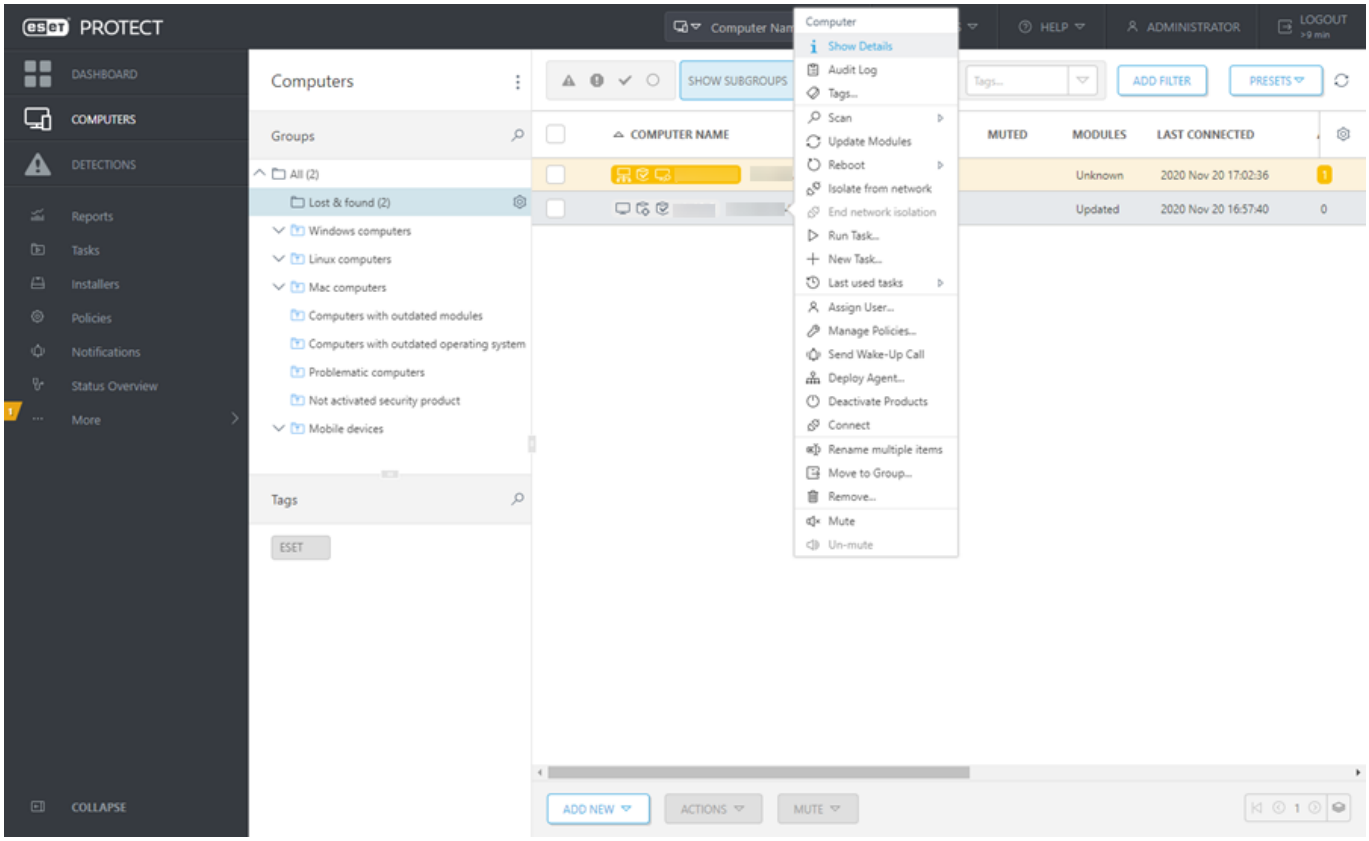
- **Ejecutar la tarea de Instalación de software** en todos los servidores en los que desee utilizar la versión más reciente de ESET Server Security.

- **Asignar política de configuración** a todos los servidores que ejecuten la versión más reciente de ESET Server Security.

Procedimiento paso a paso:

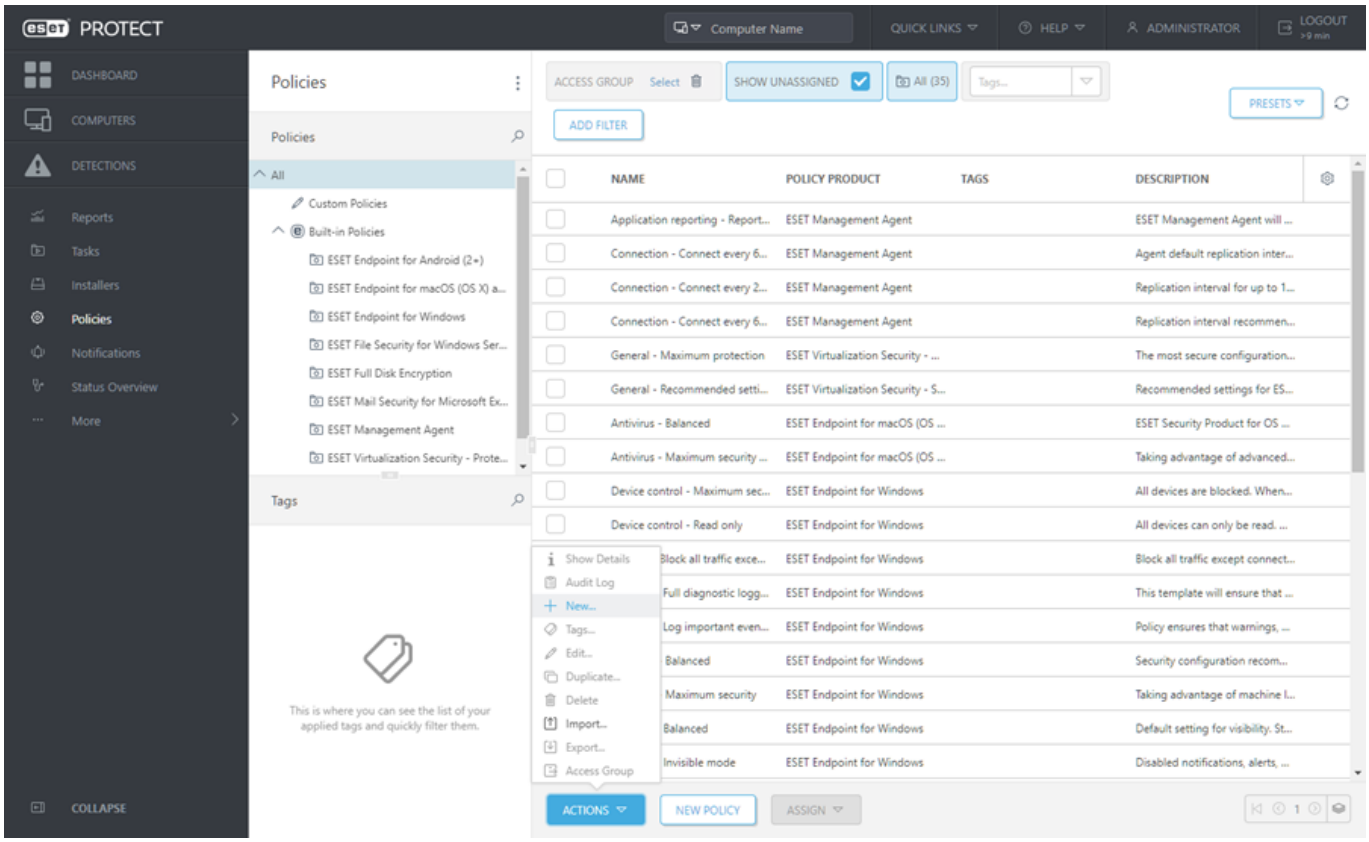
1. Inicie sesión en uno de los servidores que ejecuten ESET Server Security y actualícelo descargando e instalando la versión más reciente sobre la existente. Siga los pasos de instalación habituales. Toda la configuración original de ESET Server Security se conservará durante la instalación.

2. Abra **ESET PROTECTWeb Console**, seleccione un ordenador cliente de un grupo estático o dinámico y haga clic en **Mostrar Detalles**.



3.Desplácese hasta la ficha Configuración y haga clic en el botón **Solicitar configuración** para recopilar toda la configuración del producto administrado. Obtener la configuración llevará unos minutos. Cuando la configuración más reciente aparezca en la lista, haga clic en **Producto de seguridad** y seleccione **Abrir configuración**.

4.Cree la política de configuración haciendo clic en el botón **Convertir en política**. Introduzca el **Nombre** de la nueva política y haga clic en **Finalizar**.



5.Diríjase a **Tareas del cliente** y seleccione la tarea Desinstalación de software. Cuando cree la tarea de desinstalación, le recomendamos que reinicie el servidor tras la desinstalación. Para ello, marque la casilla de verificación **Reiniciar automáticamente cuando sea necesario**. Una vez creada la tarea, agregue los ordenadores en los que desee realizar la desinstalación.

6.Asegúrese de que ESET Server Security se desinstale de todos estos ordenadores.

7.Cree la tarea Instalación de software para instalar la versión más reciente de ESET Server Security en todos los ordenadores que desee.

8.Seleccione la opción **Asignar política de configuración** a todos los servidores que ejecuten ESET Server Security, preferiblemente reunidos en un grupo.

Actualización a través de un Clúster de ESET

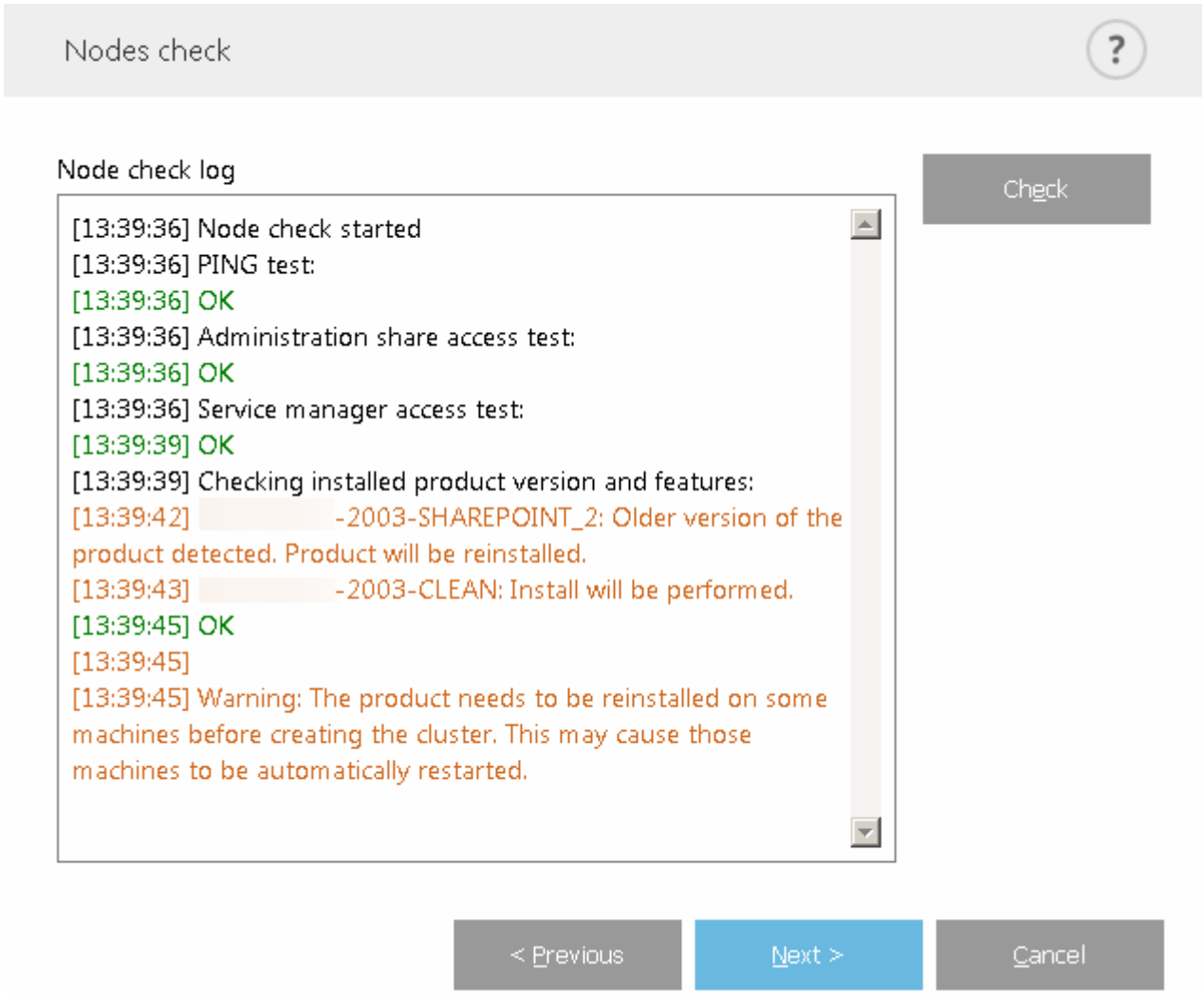
Crear un Clúster de ESET le permite actualizar varios servidores con versiones anteriores de ESET Server Security. Es una alternativa a la actualización de ESET PROTECT. Le recomendamos que utilice el método Clúster de ESET si tiene 2 o más servidores con ESET Server Security en su entorno. Otra ventaja de este método de actualización es que podrá continuar utilizando el Clúster de ESET para sincronizar la configuración de ESET Server Security en todos los nodos de miembros.

Siga los pasos que se indican a continuación para realizar la actualización con este método:

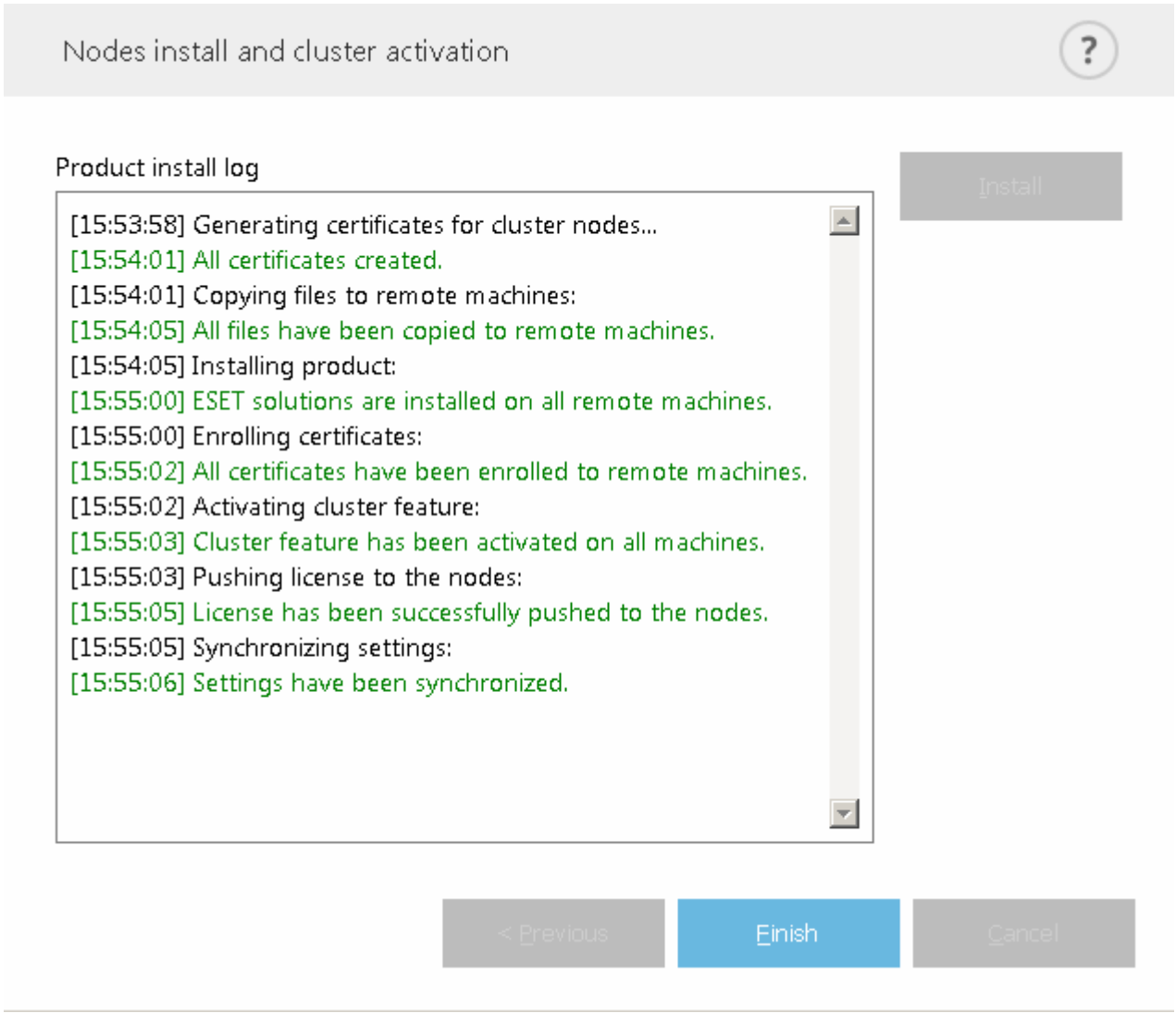
1.Inicie sesión en uno de los servidores que ejecuten ESET Server Security y actualícelo descargando e instalando la versión más reciente sobre la existente. Siga los pasos de instalación habituales. Toda la configuración original de ESET Server Security se conservará durante la instalación.

2.Ejecute el Asistente del Clúster de ESET y agregue nodos al clúster (los servidores en los que desee actualizar ESET Server Security). Si es necesario, puede agregar otros servidores en los que aún no se ejecute ESET Server Security (en estos se realizará una instalación). Le recomendamos que conserve la configuración predeterminada en Nombre del clúster y tipo de instalación (asegúrese de seleccionar **Enviar licencia a nodos sin el producto activado**).

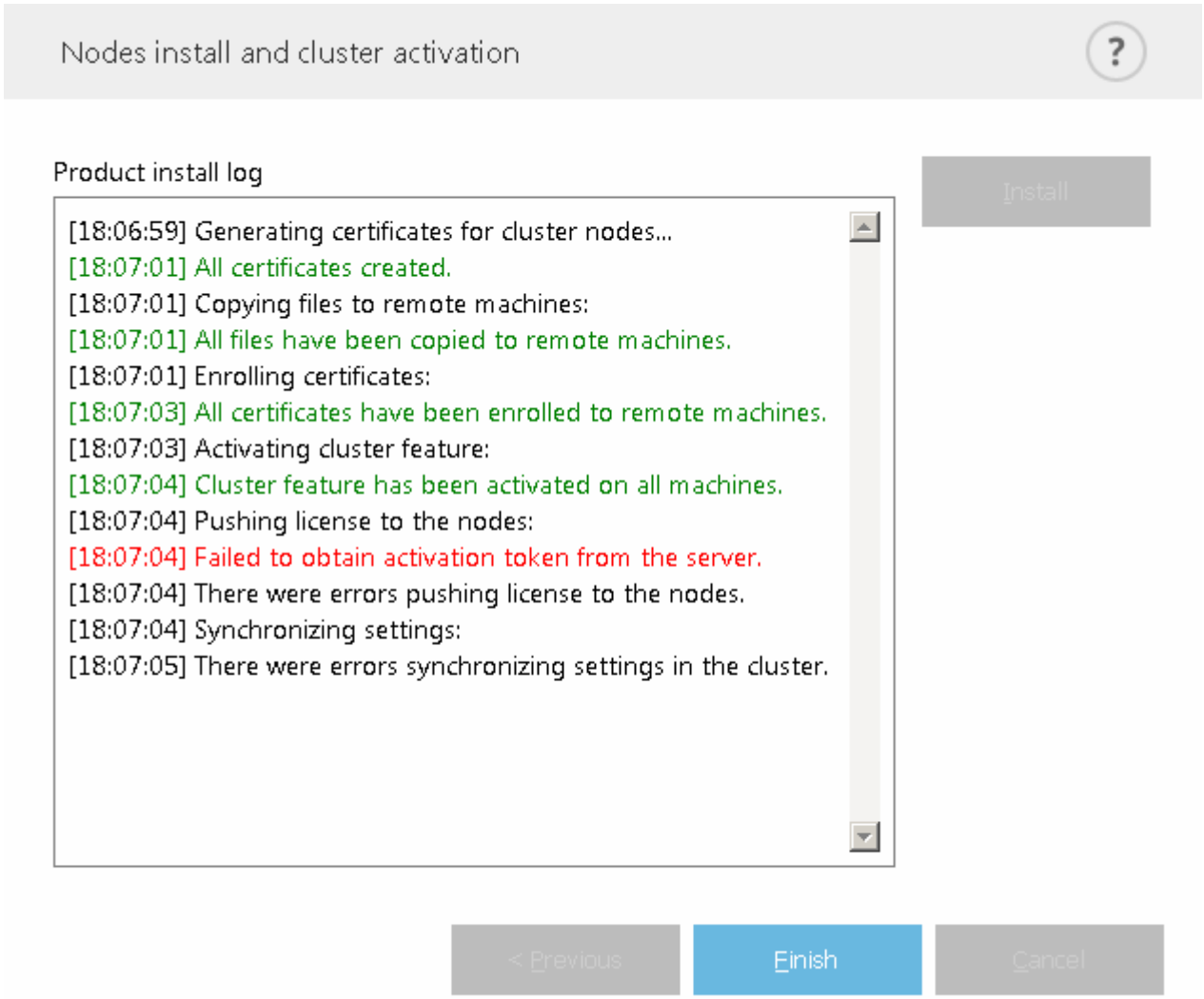
3.Compruebe la pantalla **Registro de comprobación de nodos**. En ella aparecerán los servidores con versiones anteriores del producto en los que se reinstalará el producto. ESET Server Security también se instalará en los servidores agregados en los que no esté instalado.



4.En la pantalla **Instalación de nodos y activación del clúster** se mostrará el progreso de la instalación. Cuando la instalación se haya completado correctamente, deberían verse unos resultados similares a los siguientes:



Si su red o DNS no están correctamente configurados, puede recibir el siguiente mensaje de error: **No se pudo obtener el token de activación del servidor**. Pruebe a ejecutar el Asistente del Clúster de ESET de nuevo. Destruirá el clúster y creará otro nuevo (sin reinstalar el producto), y la activación debería completarse correctamente esta vez. Si el problema sigue apareciendo, compruebe la configuración de red y DNS.



Instalación en un entorno de clúster

Puede implementar ESET Server Security en un entorno de clúster (por ejemplo, clúster de conmutación por error). Le recomendamos que instale ESET Server Security en un nodo activo y, a continuación, redistribuya la instalación en nodos pasivos utilizando la característica Clúster de ESET de ESET Server Security. Además de la instalación, Clúster de ESET servirá como replicación de la configuración de ESET Server Security para garantizar la coherencia entre los nodos del clúster necesarios para el correcto funcionamiento.

Terminal Server

Si está instalando ESET Server Security en un servidor Windows Server que actúa como Terminal Server, es preferible que desactive la GUI de ESET Server Security para impedir que se inicie cada que vez que se registra un usuario. Consulte el capítulo Desactivar la GUI en Terminal Server para conocer los pasos específicos de desactivación de la GUI.

Introducción

En la siguiente sección podrá obtener ayuda para comenzar a usar ESET Server Security.

Estado de la protección

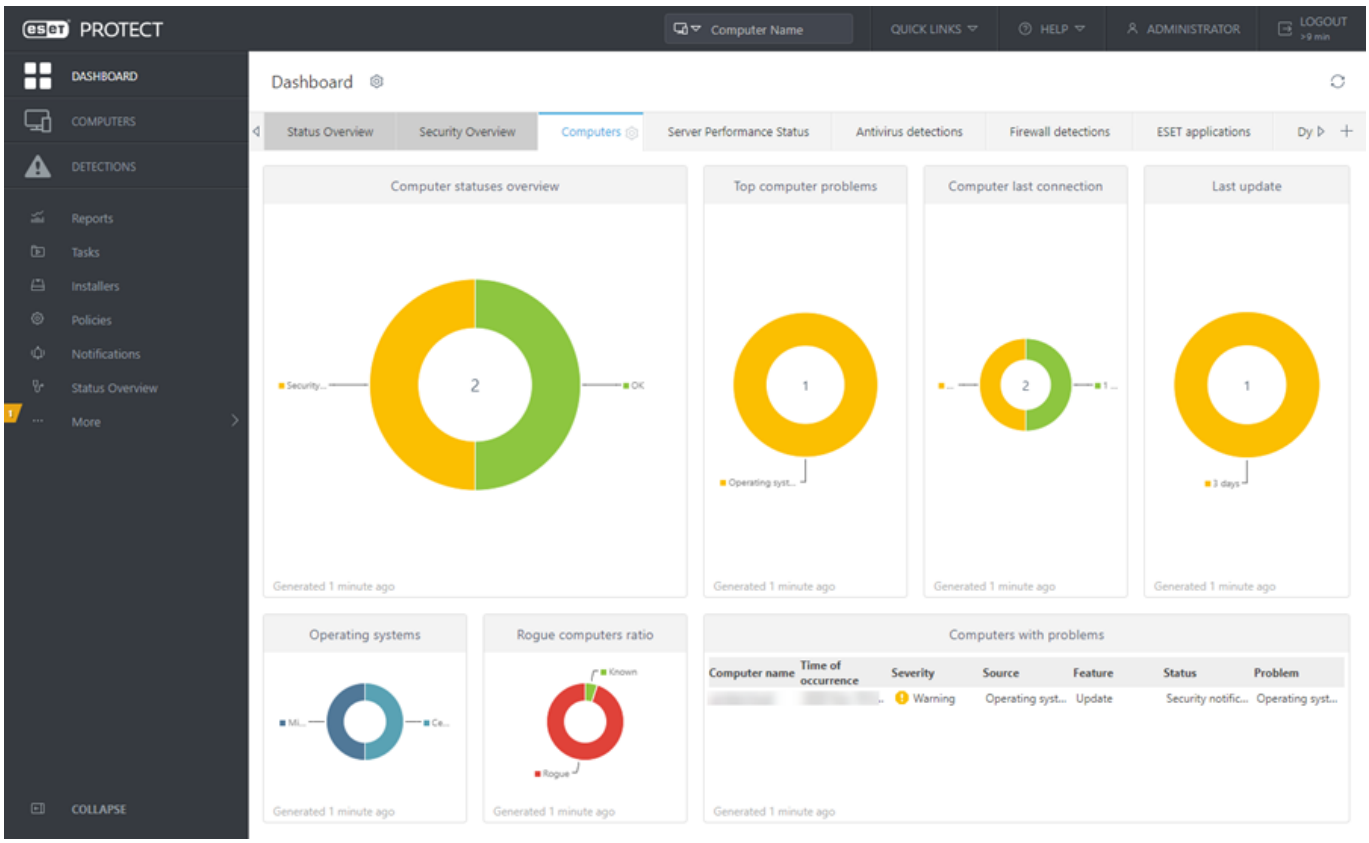
Le ofrece un resumen inmediato del estado actual de ESET Server Security. A primera vista, verá si existe algún problema que requiera su atención.

Administración a través de ESET PROTECT

Puede utilizar ESET PROTECT para administrar de forma remota ESET Server Security.

Administración a través de ESET PROTECT

ESET PROTECT es una aplicación que le permite administrar los productos de ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas de ESET PROTECT le permite instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y amenazas. ESET PROTECT no proporciona protección frente a código malicioso por sí solo, sino que confía en la presencia de soluciones de seguridad de ESET en cada cliente. Las soluciones de seguridad de ESET son compatibles con redes que incluyan varios tipos de plataforma. Su red puede incluir una combinación de los sistemas operativos de Microsoft, Linux, Mac OS y dispositivos móviles actuales.



Para obtener más información sobre ESET PROTECT, consulte la Ayuda en línea de ESET PROTECT.

Control

El estado de protección que aparece en la sección **Estado de la protección** le informa del nivel de protección actual de su ordenador. En la ventana principal se mostrará un resumen del estado de funcionamiento de ESET Server Security.

El icono de estado verde **Está protegido** indica que se garantiza la protección máxima.

El icono de estado rojo indica problemas críticos: no se garantiza la protección máxima de su ordenador. Para obtener una lista de posibles estados de protección, consulte la sección Estado.

El icono naranja indica que un problema no grave del producto de ESET requiere su atención.

Los módulos que funcionan correctamente presentan una marca de verificación de color verde. Aquellos módulos que no son totalmente funcionales presentan un símbolo de exclamación en rojo o un icono de notificación de color naranja, además de información adicional acerca del módulo en la parte superior de la ventana. También se muestra una sugerencia de solución para reparar el módulo. Para cambiar el estado de un módulo concreto, haga clic en Configuración en el menú principal y, a continuación, en el módulo deseado.

La página Estado de la protección también contiene información sobre su sistema, como por ejemplo:

- **Versión del producto**: número de versión de ESET Server Security.
- **Nombre del servidor**: nombre de host o FQDN de la máquina.
- **Sistema**: detalles del sistema operativo.
- **Ordenador**: detalles del hardware.
- **Tiempo de actividad del servidor**: muestra cuánto tiempo lleva el sistema activo y en funcionamiento; es básicamente el tiempo que no es tiempo de inactividad.

Si no consigue solucionar el problema con estas sugerencias, haga clic en **Ayuda y asistencia técnica** para acceder a los archivos de ayuda o realice una búsqueda en la Base de conocimiento de ESET. Si necesita más ayuda, puede enviar una solicitud de soporte. El soporte técnico de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

Estado

Se mostrará un resumen del estado de ESET Server Security en la ventana principal con información detallada sobre el sistema. Por lo general, si todo funciona sin problemas, el estado de la protección es verde . Sin embargo, el estado de protección podría cambiar en determinadas circunstancias. El estado de protección cambiará a naranja o se mostrará el mensaje de advertencia en rojo si tiene lugar alguna de las siguientes opciones:

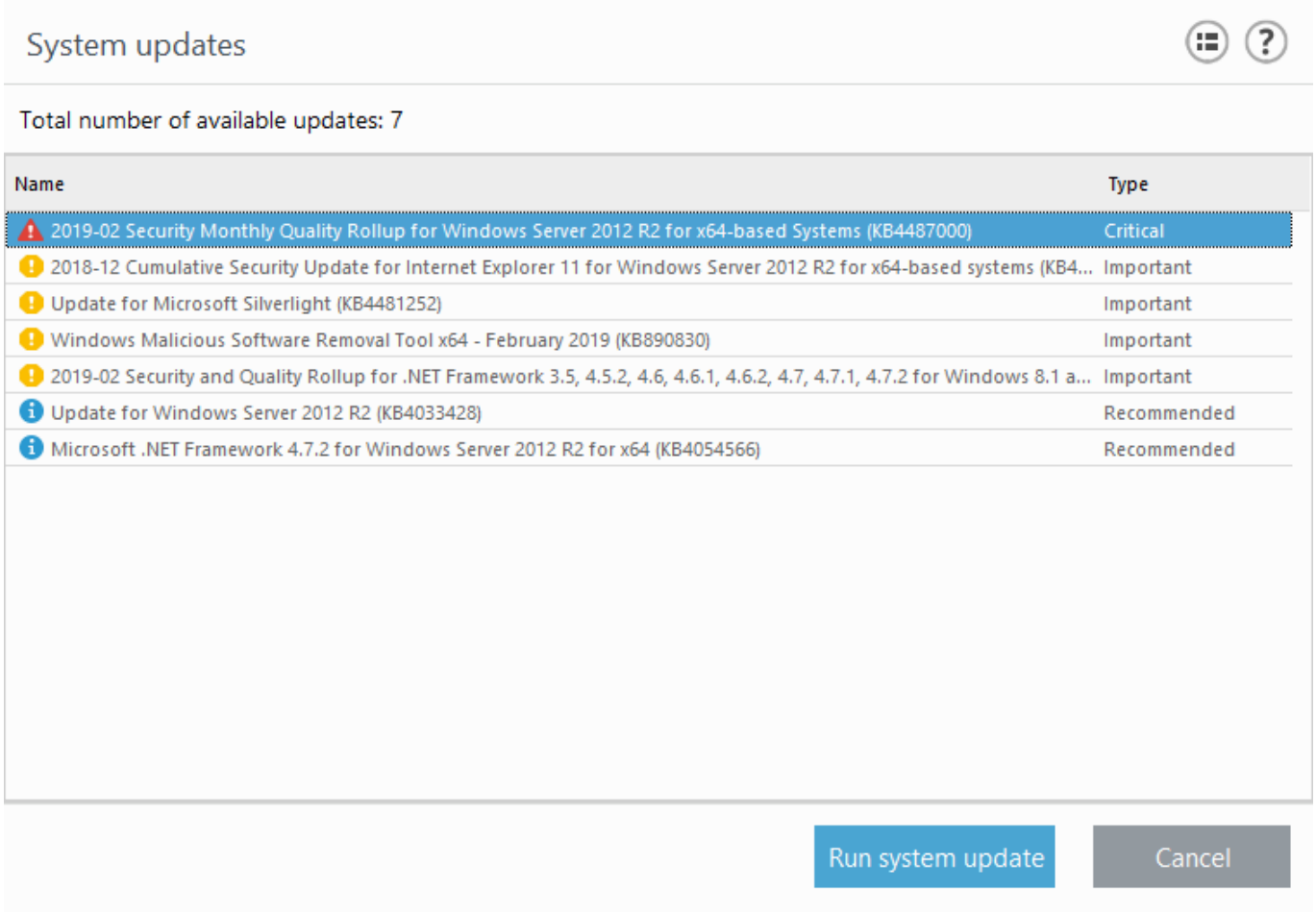
Mensaje de advertencia	Detalles del mensaje de advertencia
La detección de aplicaciones potencialmente no deseadas no está configurada	Una aplicación potencialmente no deseada (PUA) es un programa que contiene adware, instala barras de herramientas o tiene otros objetivos poco claros. Existen determinados casos en los que podría creer que las ventajas de una aplicación potencialmente no deseada compensan los riesgos asociados.
La protección del sistema de archivos en tiempo real está en pausa	Haga clic en Activar protección en tiempo real en la pestaña **Supervisión** o active de nuevo la **Protección del sistema de archivos en tiempo real** en la pestaña Configuración de la ventana principal del programa.
La protección anti-phishing no está operativa	Esta función no está operativa porque otros módulos necesarios del programa no están activos.
ESET LiveGrid® está desactivado	Este problema se indica cuando ESET LiveGrid® está desactivado en **Configuración avanzada**.
El filtrado de protocolos está desactivado	Haga clic en Activar el filtrado de protocolos para activar de nuevo esta función.
El sistema operativo no está actualizado	En la ventana Actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para descargarse e instalarse.
Su dispositivo perderá la protección dentro de poco	Haga clic en Ver las opciones para obtener más información sobre cómo actualizar su versión de Microsoft Windows. Si ejecuta **Microsoft Windows Server 2008 R2 SP1** o **Microsoft Windows Small Business Server 2011 SP1**, asegúrese de que su sistema sea compatible con SHA-2. Aplique los parches de acuerdo con la versión concreta de su sistema operativo.
El modo de presentación está activado	Se suprimen todas las ventanas emergentes y se interrumpen las tareas programadas.
La protección contra los ataques de red (IDS) está en pausa	Haga clic en Activar la protección contra los ataques de red (IDS) para activar de nuevo esta función.
La protección contra botnets está en pausa	Haga clic en Activar protección contra botnets para activar de nuevo esta función.
La protección de acceso a la web está en pausa	Haga clic en Activar la protección de acceso a la Web en **Supervisión** o active de nuevo la **Protección del acceso a la Web** en el panel Configuración de la ventana principal del programa.
Se pausó el control de dispositivos	Haga clic en Activar el Control de dispositivos para activar de nuevo esta función.
Producto no activado o Licencia caducada	Esto se indica mediante el icono de estado de la protección, que se vuelve rojo. Una vez que expire la licencia, el programa no se podrá actualizar. Siga las instrucciones de la ventana de alerta para renovar la licencia.
Anulación de la política activa	La configuración definida por la política está anulada temporalmente, posiblemente hasta que finalice la solución de problemas. Si está gestionando ESET Server Security mediante ESET PROTECT y le ha asignado una política, el enlace de estado estará bloqueado (atenuado) según las funciones que pertenezcan a la política.

Mensaje de advertencia	Detalles del mensaje de advertencia
Es necesario reiniciar el ordenador	Este mensaje puede aparecer después de que se apliquen las actualizaciones de componentes del programa (PCU) y las microactualizaciones de componentes del programa (µPCU). Consulte Actualizar configuración si desea obtener información detallada sobre las PCU y las µPCU.

Si no consigue solucionar el problema, realice una búsqueda en la Base de conocimiento de ESET. Si necesita más ayuda, puede enviar una solicitud de soporte. El soporte técnico de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

Actualización de Windows disponible

En la ventana Actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para descargarse e instalarse. El nivel de prioridad de la actualización se muestra junto al nombre de la actualización. Haga clic con el botón derecho en cualquier fila de actualización y haga clic en **Más información** para ver una ventana emergente con información adicional:



Haga clic en **Ejecutar actualización del sistema** para abrir la ventana **Windows Update** y continuar con las actualizaciones del sistema.

Aislamiento de la red

ESET Server Security le proporciona una opción para bloquear la conexión de red de su servidor, llamada aislamiento de la red. En algunos casos extremos, es posible que quiera aislar un servidor de la red como medida

preventiva. Por ejemplo, si ha detectado que el servidor se ha infectado con malware o si el equipo se ha visto comprometido de cualquier otra forma.

Mediante la activación del aislamiento de la red, se bloquea todo el tráfico de red, excepto los siguientes elementos:

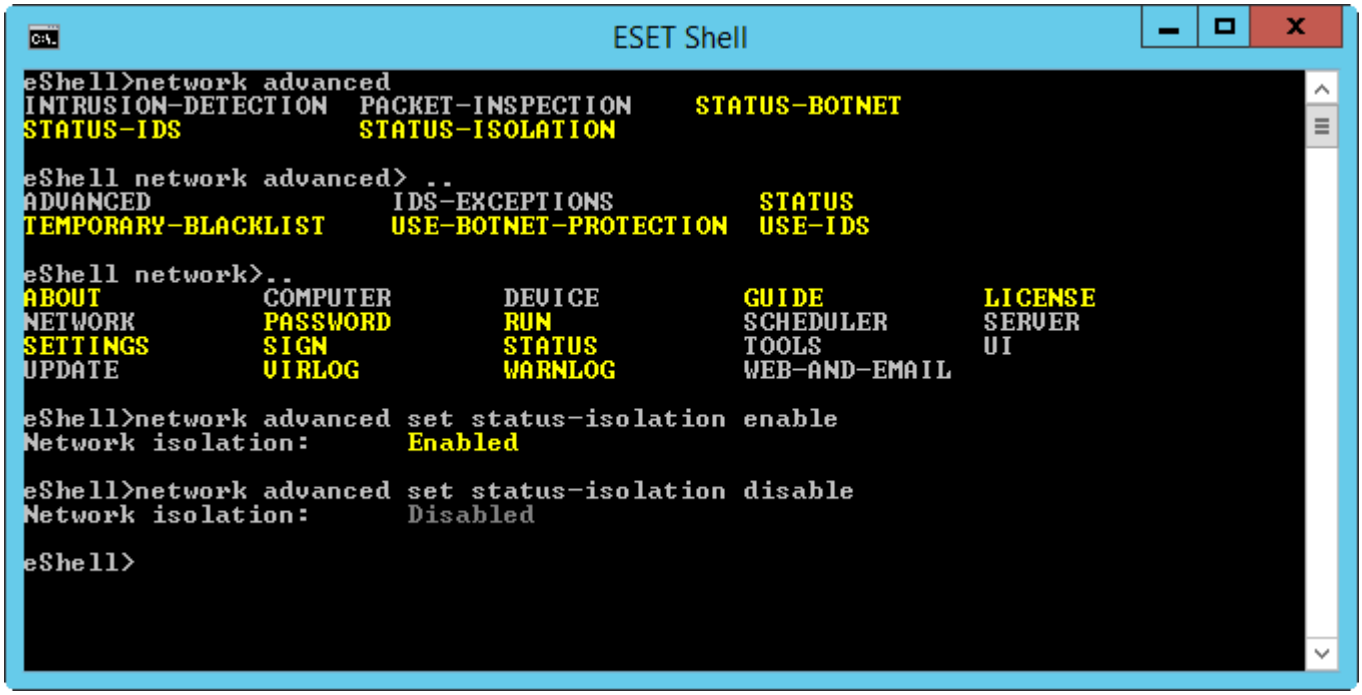
- Se mantiene la conectividad al controlador de dominio
- ESET Server Security sigue siendo capaz de comunicarse
- Si están presentes, ESET Management Agent y ESET Enterprise Inspector Agent pueden comunicarse a través de la red

Active y desactive el aislamiento de la red mediante el comando eShell o la tarea del cliente ESET PROTECT.

eShell

En modo interactivo:

- Activar aislamiento de la red: `network advanced set status-isolation enable`
- Desactivar aislamiento de la red: `network advanced set status-isolation disable`



También puede crear y ejecutar un archivo por lotes con el modo por lotes/de script.

ESET PROTECT

- Active el aislamiento de red a través de la tarea del cliente.
- Desactive el aislamiento de la red a través de la tarea del cliente.

Cuando se activa el aislamiento de la red, el estado de ESET Server Security cambia a rojo con un mensaje **Acceso a la red bloqueado**.

Si se utiliza ESET Server Security

En esta sección se incluye una descripción detallada de la interfaz de usuario del programa y se explica cómo utilizar ESET Server Security.

La interfaz de usuario le permite acceder rápidamente a funciones que se usan habitualmente:

- Estado de la protección
- Archivos de registro
- Analizar
- Actualización
- Configuración
- Herramientas

Análisis

El análisis a petición es una parte importante de ESET Server Security. Se utiliza para realizar análisis de archivos y carpetas en su ordenador. Para garantizar la seguridad de su red, es esencial que los análisis del ordenador no se ejecuten únicamente cuando se sospecha que existe una infección, sino que se realicen periódicamente como parte de las medidas de seguridad rutinarias. Le recomendamos que realice un análisis en profundidad de su sistema periódicamente (por ejemplo, una vez al mes) para detectar virus que la Protección del sistema de archivos en tiempo real no haya detectado. Esto puede suceder si aparece una amenaza cuando la protección del sistema de archivos en tiempo real está desactivada, el motor de detección no se ha actualizado o no se detectó un archivo cuando se guardó por primera vez en el disco.

Seleccione entre los análisis a petición disponibles para ESET Server Security:

Análisis del almacenamiento

Analiza todas las carpetas compartidas del servidor local. Si el Análisis del almacenamiento no está disponible, en el servidor no hay carpetas compartidas.

Analice su equipo

Le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin la intervención del usuario. La ventaja del análisis del ordenador es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis 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. Para obtener más información detallada sobre los tipos de desinfección, consulte Desinfección.

NOTA
Le recomendamos que ejecute un análisis del ordenador una vez al mes como mínimo. El análisis se puede configurar como una tarea programada.

Análisis personalizado

El análisis personalizado es una solución óptima para especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del análisis personalizado es su capacidad para configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis

definidos por el usuario, que pueden resultar útiles si el análisis se realiza varias veces con los mismos parámetros.

Análisis de medios extraíbles

Al igual que el Análisis inteligente, inicia rápidamente el análisis de medios extraíbles (como CD/DVD/USB) que están conectados al ordenador. Esto puede resultar útil cuando conecta una unidad flash USB a un ordenador y desea analizar su contenido por si contiene malware u otras posibles amenazas. Este tipo de análisis también se puede iniciar haciendo clic en **Análisis personalizado**, en **Medios extraíbles** en el menú desplegable **Objetos del análisis** y, a continuación, en **Analizar**.

Análisis Hyper-V

Esta opción está visible en el menú solo si el Administrador de Hyper-V está instalado en el servidor que ejecuta ESET Server Security. El análisis Hyper-V permite analizar discos de máquina virtual en Microsoft Hyper-V Server sin necesidad de tener ningún "Agente" instalado en la máquina virtual determinada.

Análisis de OneDrive

Le permite analizar los archivos del usuario situados en el almacenamiento en la nube OneDrive.

Repetir el último análisis

Repite la última operación de análisis utilizando exactamente la misma configuración.

> NOTA
> la repetición de la última función de análisis no estará disponible si está presente el Análisis de la base de datos a petición.

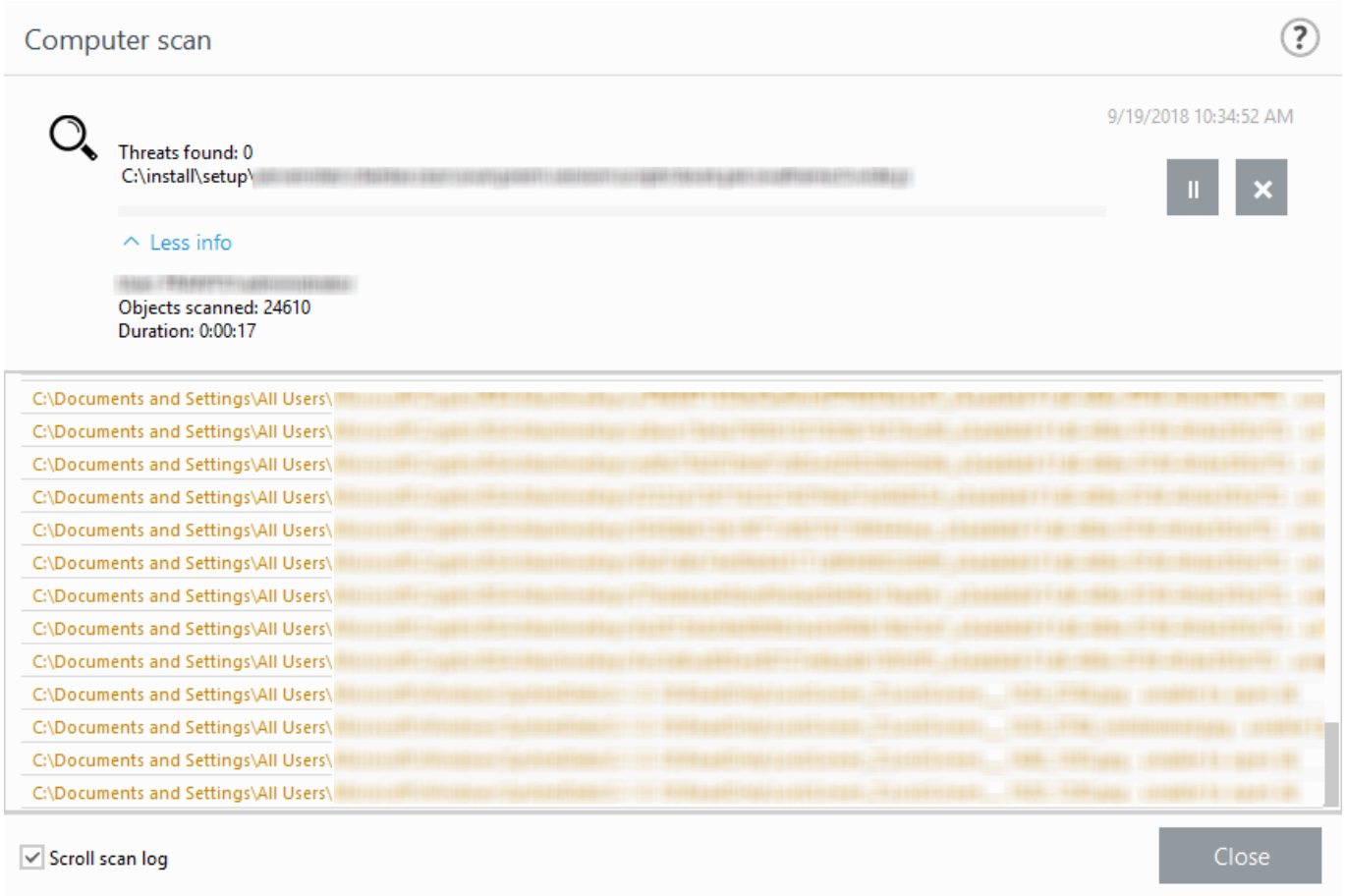
Puede usar opciones para ver más información sobre los estados de análisis:

Arrastrar y colocar archivos	**También puede arrastrar y colocar archivos en la ventana de análisis de ESET Server Security y los archivos se analizarán en busca de virus inmediatamente.**
Cerrar/Cerrar todo	Cierra los mensajes mostrados.
Estados de análisis	Muestra el estado del análisis inicial. Este análisis ha finalizado o el usuario lo ha interrumpido.
Mostrar registro	Muestra información más detallada.
Más información	Durante un análisis, muestra detalles como el **Usuario** que realizó el análisis, el número de **Objetos analizados** y la **Duración** del análisis.
Abrir ventanas de análisis	En la ventana de progreso del análisis se muestra el estado actual del análisis e información sobre el número de archivos en los que se ha detectado código malicioso.

Ventana y registro de análisis

En la ventana de análisis se muestran los objetos actualmente analizados, incluidos datos como su ubicación, el número de amenazas encontradas (En caso de haber alguna), el número de objetos analizados y la duración del análisis. La parte inferior de la ventana es un registro de análisis en el que se muestra el número de versión del motor de detección, la fecha y hora a las que comenzó el análisis y la selección de objetos.

Mientras el análisis está en curso, puede hacer clic en **En pausa** si desea interrumpir el análisis de forma temporal. Cuando el proceso de análisis está en pausa, está disponible la opción **Reanudar**.

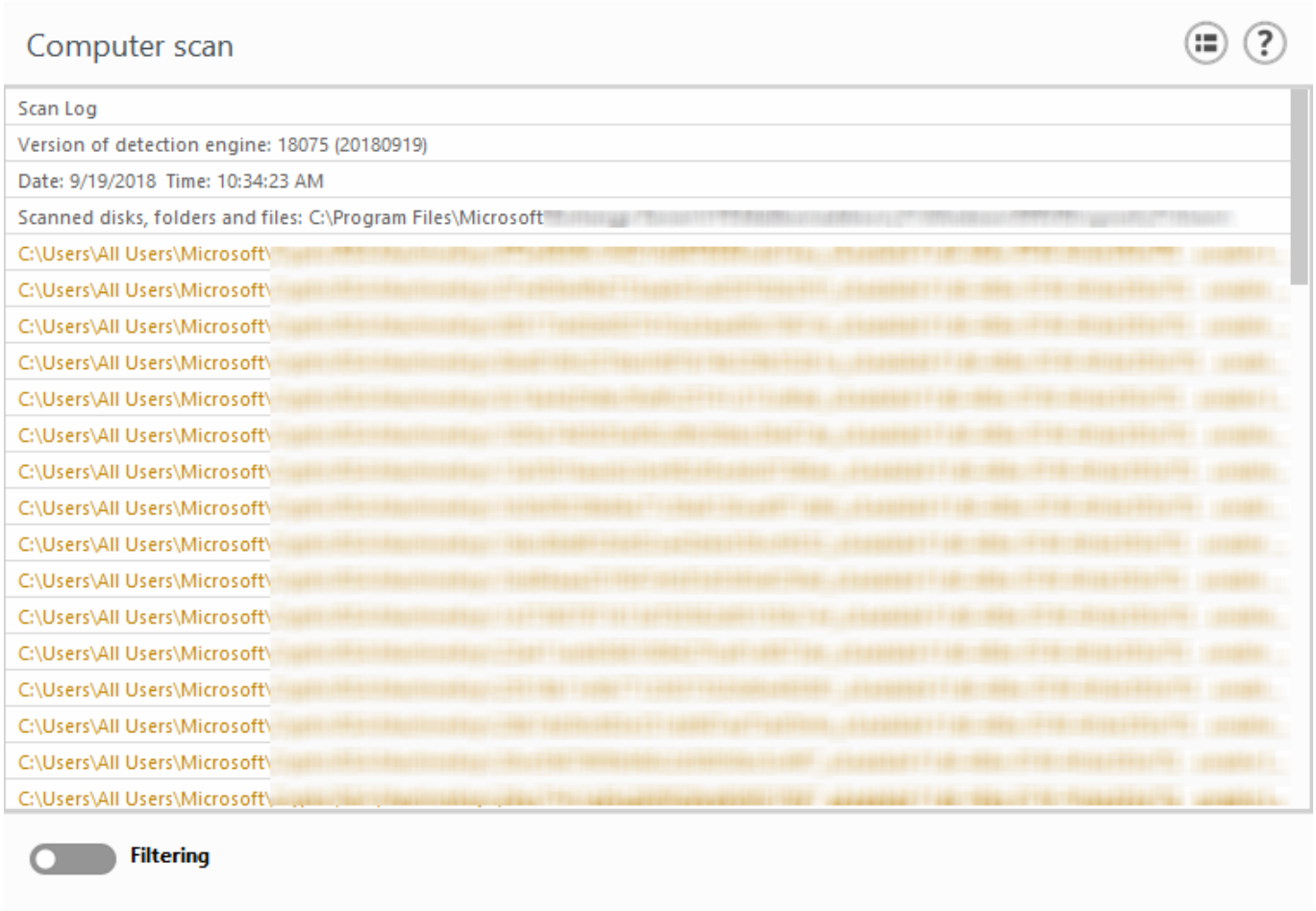


Desplazarse por el registro de exploración

Deje esta opción activada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana Archivos de registro.

NOTA
es normal que algunos archivos, como los archivos protegidos con contraseña o que solo utiliza el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar.

Una vez concluido el análisis, verá el registro del análisis con toda la información importante sobre ese análisis concreto.



Haga clic en el icono del conmutador **Filtrado** para abrir la ventana Filtrado de registros, en la que puede definir los criterios de filtrado o búsqueda. Si desea ver el menú contextual, haga clic con el botón derecho del ratón en una entrada del registro:

Acción	Uso	Acceso directo	Ver también
Filtrar los mismos registros	Esta opción activa el filtrado de registros para mostrar solo los registros del mismo tipo que el seleccionado.	Ctrl + Mayús + F	
Filtrar...	Después de hacer clic en esta opción, en la ventana Filtrado de registros podrá definir los criterios de filtrado para entradas de registro específicas.		Filtrado de registros
Activar filtro	Activa la configuración del filtro. La primera vez que active el filtrado, deberá definir la configuración.		
Desactivar filtro	Desactiva el filtrado (tiene el mismo efecto que hacer clic en el conmutador de la parte inferior).		
Copiar	Copia al portapapeles la información de los registros seleccionados o resaltados.	Ctrl + C	
Copiar todo	Copia la información de todos los registros de la ventana.		
Exportar...	Exporta la información de los registros seleccionados o resaltados a un archivo XML.		
Exportar todo...	Exporta toda la información de la ventana a un archivo XML.		

Archivos de registro

Los archivos de registro contienen información relacionada con los sucesos importantes del programa y proporcionan información general acerca de los resultados de análisis, las amenazas detectadas, etc. Los registros constituyen una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según la configuración actual del nivel de detalle de los registros. Los mensajes de texto y los archivos de registro se pueden ver directamente desde el entorno de ESET Server Security o se pueden exportar para visualizarlos en otro lugar.

Seleccione el tipo de registro que desee en el menú desplegable. Están disponibles los siguientes registros:

Detecciones

El registro de detecciones ofrece información detallada acerca de las amenazas detectadas por los módulos de ESET Server Security. La información incluye el momento de la detección, el nombre de la amenaza, la ubicación, la acción ejecutada y el nombre del usuario con sesión iniciada en el momento en el que se detectó la amenaza. Haga doble clic en cualquier entrada del registro para ver sus detalles en una ventana independiente. Si es necesario, puede crear una exclusión de detección: haga clic con el botón derecho del ratón en un registro (detección) y haga clic en **Crear exclusión**. Se abrirá el Asistente de exclusiones con los criterios predefinidos. Si hay un nombre de detección junto a un archivo excluido, significa que el archivo se excluye únicamente para la detección indicada. Si ese archivo se infecta con otro malware más adelante, se detectará.

Sucesos

Todas las acciones importantes realizadas por ESET Server Security se registran en el registro de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para ayudar a los administradores del sistema y los usuarios con la solución de problemas. Con frecuencia, la información aquí disponible puede ayudarle a encontrar una solución para un problema del programa.

Análisis del ordenador

En esta ventana se muestran todos los resultados del análisis. Cada línea se corresponde con un control informático individual. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.

Archivos bloqueados

Incluye registros de archivos que se bloquearon y a los que no se pudo acceder. El protocolo muestra el motivo y el módulo de origen que bloqueó el archivo, así como la aplicación y el usuario que ejecutaron el archivo.

Archivos enviados

Contiene registros de protección basada en la nube de archivos, ESET Dynamic Threat Defense y ESET LiveGrid®.

Registros de auditoría

Contiene registros de cambios en la configuración o el estado de la protección, y crea instantáneas para consultarlas en el futuro. Haga clic con el botón derecho sobre cualquier registro del tipo Cambios de ajuste y

seleccione **Mostrar cambios** en el menú contextual para mostrar información detallada sobre el cambio efectuado. Si desea volver al ajuste anterior, seleccione **Restaurar**. También puede usar **Eliminar todo** para quitar los registros. Si desea desactivar el registro de auditoría, diríjase a **Configuración avanzada** > **Herramientas** > **Archivos de registro** > Registro de auditoría.

HIPS

Incluye registros de reglas específicas que se marcaron para su registro. El protocolo muestra la aplicación que invocó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla creada.

Protección de la red

Incluye registros de archivos que han bloqueado la protección contra botnets e IDS (protección frente a ataques de red).

Sitios web filtrados

Lista de los sitios web que han bloqueado la Protección de acceso a la web En estos registros se muestran la hora, la URL, el usuario y la aplicación que estableció una conexión con un sitio web determinado.

Control del dispositivo

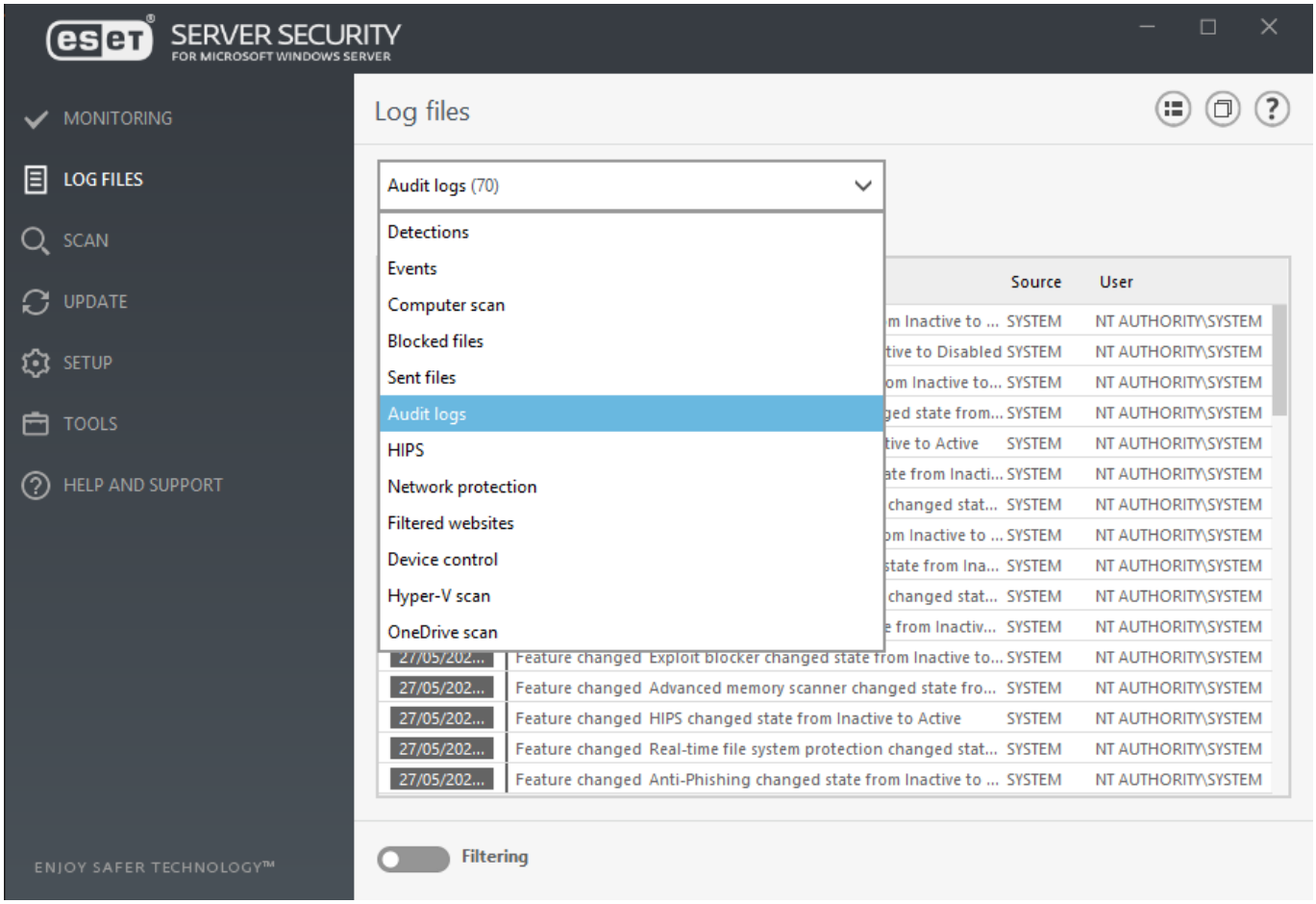
Contiene registros de los dispositivos o medios extraíbles conectados al ordenador. Solo los dispositivos con una regla de control de dispositivos se registran en el archivo de registro. Si la regla no coincide con un dispositivo conectado, no se creará una entrada de registro para un dispositivo conectado. Aquí puede ver también detalles como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).

Análisis Hyper-V

Contiene una lista de los resultados del análisis Hyper-V. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.

Análisis de OneDrive

Contiene una lista de los resultados del análisis OneDrive.



El menú contextual (con clic derecho) le permite elegir una acción con el registro seleccionado:

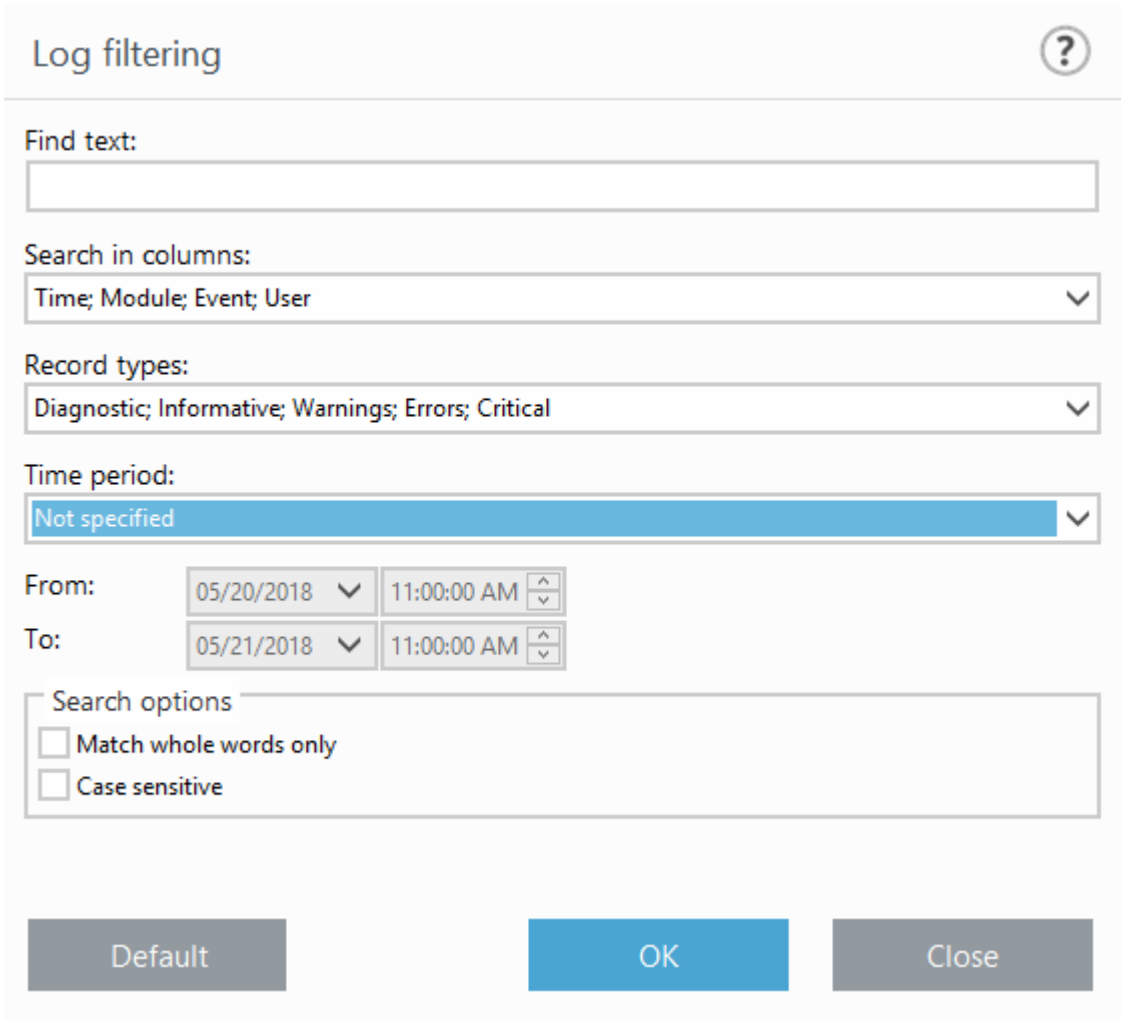
Acción	Uso	Acceso directo	Ver también
Mostrar	Muestra información detallada sobre el registro seleccionado en una ventana nueva (igual que el doble clic).		
Filtrar los mismos registros	Esta opción activa el filtrado de registros para mostrar solo los registros del mismo tipo que el seleccionado.	Ctrl + Mayús + F	
Filtrar...	Después de hacer clic en esta opción, en la ventana Filtrado de registros podrá definir los criterios de filtrado para entradas de registro específicas.		Filtrado de registros
Activar filtro	Activa la configuración del filtro. La primera vez que active el filtrado, deberá definir la configuración.		
Desactivar filtro	Desactiva el filtrado (tiene el mismo efecto que hacer clic en el conmutador de la parte inferior).		
Copiar	Copia al portapapeles la información de los registros seleccionados o resaltados.	Ctrl + C	
Copiar todo	Copia la información de todos los registros de la ventana.		
Eliminar	Elimina los registros seleccionados o resaltados; esta acción requiere privilegios de administrador.	Supr	
Eliminar todo	Elimina todos los registros de la ventana; esta acción requiere privilegios de administrador.		
Exportar...	Exporta la información de los registros seleccionados o resaltados a un archivo XML.		
Exportar todo...	Exporta toda la información de la ventana a un archivo XML.		

Acción	Uso	Acceso directo	Ver también
Buscar...	Abre la ventana Buscar en el registro y le permite definir los criterios de búsqueda. Puede utilizar la función de búsqueda para encontrar un registro específico aunque el filtrado esté activado.	Ctrl + F	Buscar en el registro
Buscar siguiente	Busca la siguiente instancia de los criterios de búsqueda definidos.	F3	
Buscar anterior	Busca la instancia anterior.	Mayús + F3	
Crear exclusión	Para excluir objetos de la desinfección mediante el nombre de la detección, la ruta de acceso o su hash.		Crear exclusión

Filtrado de registros

La función de filtrado de registros le ayudará a encontrar la información que busca, especialmente si hay un gran número de registros. Le permite reducir los historiales de registros, por ejemplo, si busca un tipo determinado de evento, estado o periodo de tiempo. Para filtrar historiales de registro, especifique determinadas opciones de búsqueda, solo se mostrarán los historiales que sean relevantes (según las opciones de búsqueda indicadas) en la ventana Archivos de registro.

Escriba la palabra clave que busca en el campo **Buscar texto**. Utilice el menú desplegable **Buscar en columnas** para limitar la búsqueda. Elija uno o más registros en el menú desplegable **Tipos de registro**. Defina el **Periodo de tiempo** desde el que desea mostrar los resultados. También puede utilizar otras opciones de búsqueda, tales como **Solo palabras completas** o **Distinguir mayúsculas y minúsculas**.



Buscar texto

Escriba una cadena (palabra completa o parcial). Solo se mostrarán los registros que contengan dicha cadena; el resto de registros se omitirá.

Buscar en columnas

Seleccione las columnas que se tendrán en cuenta en la búsqueda. Puede seleccionar las columnas que desee para la búsqueda.

Tipos de registro

Seleccione uno o más tipos de registro en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Crítico**: registra únicamente errores críticos.

Período de tiempo

Permite definir el periodo de tiempo para el que desea visualizar los resultados:

- **No especificado** (predeterminada): no busca en un período de tiempo determinado, sino en todo el registro.
- **Último día**
- **Última semana**
- **Último mes**
- **Período de tiempo**: permite especificar el período de tiempo exacto (Desde: y Hasta:) para filtrar únicamente los registros correspondientes a un período de tiempo especificado.

Solo palabras completas

Utilice esta casilla de verificación si desea buscar palabras completas para obtener resultados más precisos.

Distinguir mayúsculas y minúsculas

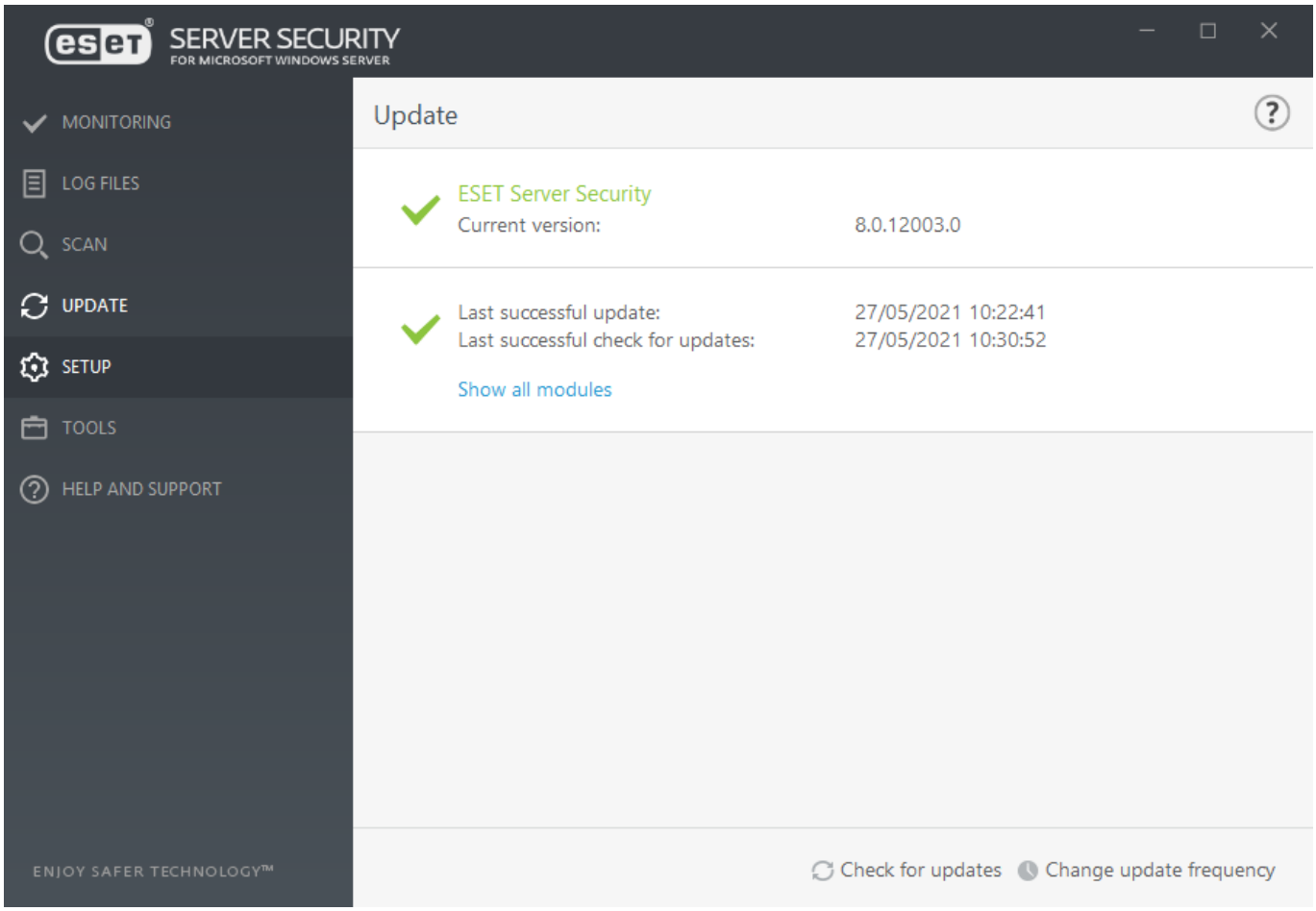
Active esta opción si considera que es importante distinguir mayúsculas y minúsculas durante el filtrado. Una vez que haya configurado las opciones de filtrado/búsqueda, haga clic en **Aceptar** para mostrar los registros filtrado o en **Buscar** para iniciar la búsqueda. La búsqueda en los archivos de registro se realiza de arriba abajo, a partir de la posición actual (registro resaltado). La búsqueda se detiene cuando se encuentra el primer registro coincidente. Pulse **F3** para buscar el siguiente registro o haga clic con el botón derecho del ratón y seleccione **Buscar** para limitar las opciones de búsqueda.

Actualización

En la sección Actualización puede ver el estado de actualización actual de su ESET Server Security, incluidas la fecha y hora de la última actualización con éxito. La mejor manera de mantener el máximo nivel de seguridad en el ordenador es actualizar ESET Server Security de forma periódica. El módulo de actualización garantiza que el

programa está siempre actualizado de dos maneras: actualizando la base de firmas de virus y los componentes del sistema. Actualizar el motor de detección y los componentes del programa es una parte importante de proporcionar protección total ante el código malicioso.

NOTA
Si aún no ha introducido una Clave de licencia, no podrá recibir actualizaciones y se le pedirá que active su producto. Para ello, diríjase a **Ayuda y asistencia técnica** > **Activar producto**.



Versión actual

La versión de compilación de ESET Server Security.

Última actualización correcta

Fecha de la última actualización. Asegúrese de que hace referencia a una fecha reciente, lo que significa que los módulos están actualizados.

Última búsqueda correcta de actualizaciones

Fecha del último intento de actualizar los módulos.

Mostrar todos los módulos

Abre la lista de los módulos instalados.

Buscar actualizaciones

La actualización de los módulos es una parte importante a la hora de mantener una protección completa frente a código malicioso.

Cambiar frecuencia de actualización

Puede editar la repetición de la tarea de Tareas programadas Actualización automática de rutina.

Si no comprueba si hay actualizaciones a la mayor brevedad posible, se mostrará uno de los mensajes siguientes:

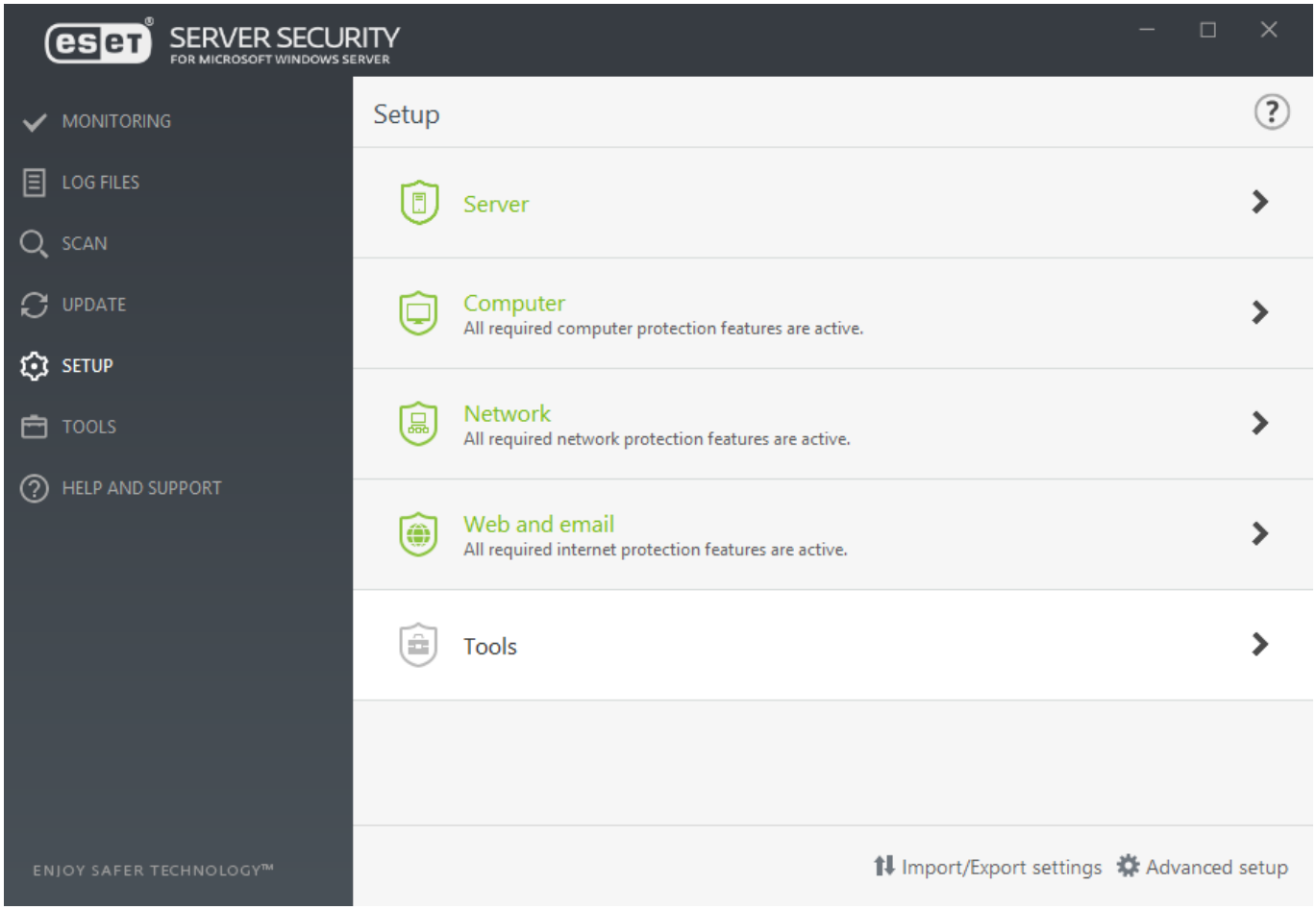
Mensaje de error	Descripciones
Los módulos no están actualizados	Este error aparecerá tras varios intentos sin éxito de actualizar los módulos. Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.
La actualización de los módulos ha fallado, el producto no está activado	La clave de licencia se ha introducido en la configuración de actualización de forma incorrecta. Recomendamos que compruebe sus datos de autenticación. La ventana **Configuración avanzada** (**F5**) contiene opciones de actualización adicionales. Haga clic en **Ayuda y asistencia técnica** > Administrar licencia en el menú principal para introducir una nueva clave de licencia.
Se produjo un error al descargar los archivos de actualización	Puede deberse a la configuración de la conexión a Internet. Es recomendable que compruebe la conectividad a Internet (por ejemplo, mediante la apertura de un sitio web en el navegador web). Si el sitio web no se abre, es probable que no se haya establecido ninguna conexión a Internet o que haya problemas de conectividad con el ordenador. Consulte a su proveedor de servicios de Internet (ISP) si no tiene una conexión activa a Internet.
Error de actualización de los módulos Error 0073	Haga clic en **Actualización** > **Buscar actualizaciones**. Para obtener más información, visite este artículo de la Base de conocimiento.

NOTA
Las opciones del servidor Proxy pueden ser diferentes para los distintos perfiles de actualización. Si este es el caso, configure los diferentes perfiles de actualización en **Configuración avanzada** (**F5**) al hacer clic en **Actualización** > Perfil.

Configuración

La ventana del menú Configuración incluye las siguientes secciones:

- Servidor
- Ordenador
- Red
- Internet y correo electrónico
- Herramientas: Registro de diagnóstico



Si desea desactivar temporalmente un módulo concreto, junto al correspondiente módulo, haga clic en la barra deslizante verde . Tenga en cuenta que esto puede disminuir el nivel de protección del servidor.

Para volver a activar la protección de un componente de seguridad desactivado, junto al correspondiente módulo, haga clic en la barra deslizante roja . El componente volverá al estado activado.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en el icono del engranaje .

Configuración de importación/exportación

Cargue los parámetros de configuración con un archivo de configuración *.xml* o guarde los parámetros de configuración actuales en un archivo de configuración.

Configuración avanzada

Establezca las opciones y la configuración avanzada en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier lugar del programa, pulse **F5**.

Servidor

Verá una lista de componentes que puede activar y desactivar con la barra deslizante.. Si desea configurar los ajustes de un elemento concreto, haga clic en el icono del engranaje .

Exclusiones automáticas

Identifica las aplicaciones de servidor y los archivos del sistema operativo de servidor esenciales y los agrega automáticamente a la lista de exclusiones. Esta funcionalidad reducirá al mínimo el riesgo de que pueda haber conflictos y aumentará el rendimiento general del servidor cuando se ejecute el software de detección de amenazas.

Clúster

Utilice esta opción para configurar y activar el Clúster de ESET.

Configuración del análisis de OneDrive

Puede registrar o anular el registro de la aplicación del módulo de análisis ESET OneDrive de Microsoft OneDrive.

Si desea desactivar temporalmente un módulo concreto, junto al correspondiente módulo, haga clic en la barra deslizante verde  . Tenga en cuenta que esto puede disminuir el nivel de protección del servidor.

Para volver a activar la protección de un componente de seguridad desactivado, junto al correspondiente módulo, haga clic en la barra deslizante roja  . El componente volverá al estado activado.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en el icono del engranaje  .

Configuración de importación/exportación

Cargue los parámetros de configuración con un archivo de configuración *.xml* o guarde los parámetros de configuración actuales en un archivo de configuración.

Configuración avanzada

Establezca las opciones y la configuración avanzada en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier lugar del programa, pulse **F5**.

Ordenador

ESET Server Security cuenta con todos los componentes necesarios para garantizar una protección eficaz del servidor como ordenador. Este módulo le permite activar/desactivar y configurar los siguientes componentes:

Protección del sistema de archivos en tiempo real

Todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. En el caso de la Protección del sistema de archivos en tiempo real existe también la opción de **Configurar** o **Editar exclusiones** con lo que se abrirá la ventana de configuración de exclusiones, en la que puede excluir archivos y carpetas del análisis.

Control del dispositivo

Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él.

Sistema de prevención de intrusiones del host (HIPS)

Este sistema supervisa los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.

- Análisis avanzado de memoria
- Bloqueador de exploits
- Protección contra ransomware

Modo de presentación

Es una función pensada para aquellos usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. Cuando se active el Modo de presentación recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal del programa cambiará a color naranja.

Pausar la protección antivirus y antiespía

Cuando desactive la protección antivirus y antiespía de forma temporal, utilice el menú desplegable para seleccionar el periodo de tiempo durante el que desea que el componente seleccionado esté desactivado y, a continuación, haga clic en **Aplicar** para desactivar el componente de seguridad. Para volver a activar la protección, haga clic en **Activar la protección antivirus y antiespía** o utilice la barra deslizante.

Si desea desactivar temporalmente un módulo concreto, junto al correspondiente módulo, haga clic en la barra deslizante verde  . Tenga en cuenta que esto puede disminuir el nivel de protección del servidor.

Para volver a activar la protección de un componente de seguridad desactivado, junto al correspondiente módulo, haga clic en la barra deslizante roja  . El componente volverá al estado activado.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en el icono del engranaje  .

Configuración de importación/exportación

Cargue los parámetros de configuración con un archivo de configuración *.xml* o guarde los parámetros de configuración actuales en un archivo de configuración.

Configuración avanzada

Establezca las opciones y la configuración avanzada en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier lugar del programa, pulse **F5**.

Red

Esto se logra mediante el permiso o denegación de conexiones de red individuales en función de sus reglas de filtrado. Ofrece protección frente a ataques de ordenadores remotos y bloquea algunos servicios potencialmente peligrosos.

El módulo Red le permite activar/desactivar y configurar los siguientes componentes:

Protección contra los ataques de red (IDS)

Analiza el contenido del tráfico de red y protege frente a ataques de red. El tráfico que se considere peligroso se bloqueará.

Protección contra botnets

Detección y bloqueo de la comunicación con botnets. Identifica de forma rápida y precisa malware en el sistema.

Lista negra temporal de direcciones IP (direcciones bloqueadas)

Ver una lista de direcciones IP que se han detectado como fuente de los ataques y se han agregado a la lista negra para bloquear la conexión durante un período de tiempo concreto

Asistente para la resolución de problemas (aplicaciones o dispositivos bloqueados recientemente)

Le ayuda a resolver problemas de conectividad provocados por la protección contra los ataques de red.

Si desea desactivar temporalmente un módulo concreto, junto al correspondiente módulo, haga clic en la barra deslizante verde. Tenga en cuenta que esto puede disminuir el nivel de protección del servidor.

Para volver a activar la protección de un componente de seguridad desactivado, junto al correspondiente módulo, haga clic en la barra deslizante roja. El componente volverá al estado activado.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en el icono del engranaje.

Configuración de importación/exportación

Cargue los parámetros de configuración con un archivo de configuración *.xml* o guarde los parámetros de configuración actuales en un archivo de configuración.

Configuración avanzada

Establezca las opciones y la configuración avanzada en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier lugar del programa, pulse **F5**.

Asistente para la resolución de problemas de red

El asistente de resolución de problemas supervisa todas las conexiones bloqueadas y lo guiará en el proceso de resolución de problemas para corregir problemas de protección frente a ataques de red con aplicaciones o dispositivos específicos. A continuación, el asistente recomendará un nuevo conjunto de reglas que se aplicarán en el caso de aprobarlas.

Web y correo electrónico

Web y correo electrónico le permite activar/desactivar y configurar los siguientes componentes:

Protección del tráfico de Internet

Si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso.

Protección del cliente de correo electrónico

Supervisa las comunicaciones recibidas a través de los protocolos POP3 e IMAP.

Protección Anti-Phishing

Le protege de intentos de obtener contraseñas, datos bancarios y otra información confidencial por parte de sitios web que suplantan a sitios legítimos.

Si desea desactivar temporalmente un módulo concreto, junto al correspondiente módulo, haga clic en la barra deslizante verde  . Tenga en cuenta que esto puede disminuir el nivel de protección del servidor.

Para volver a activar la protección de un componente de seguridad desactivado, junto al correspondiente módulo, haga clic en la barra deslizante roja  . El componente volverá al estado activado.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en el icono del engranaje  .

Configuración de importación/exportación

Cargue los parámetros de configuración con un archivo de configuración *.xml* o guarde los parámetros de configuración actuales en un archivo de configuración.

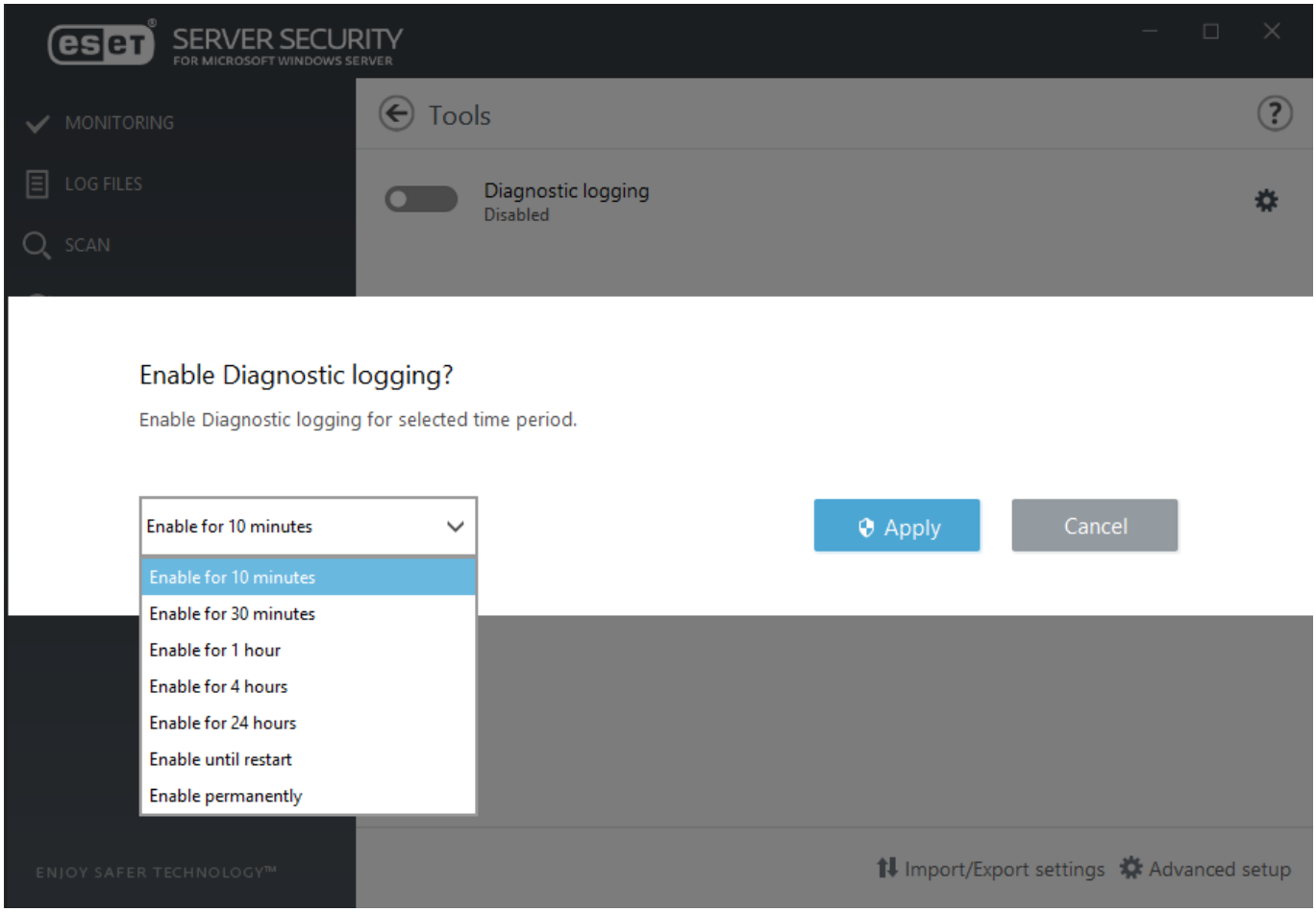
Configuración avanzada

Establezca las opciones y la configuración avanzada en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier lugar del programa, pulse **F5**.

Herramientas: Registro de diagnóstico

Puede activar el Registro de diagnóstico siempre que necesite información detallada sobre el comportamiento de una función concreta de ESET Server Security, por ejemplo durante los procesos de resolución de problemas. Al hacer clic en el icono del engranaje  , podrá configurar de qué características se deben recopilar registros de diagnóstico.

Elija durante cuánto tiempo estará activado (10 minutos, 30 minutos, 1 hora, 4 horas, 24 horas, hasta el siguiente reinicio del servidor o permanentemente). Tras activar el registro de diagnóstico, ESET Server Security recopilará registros detallados de las características que estén activadas.



Si desea desactivar temporalmente un módulo concreto, junto al correspondiente módulo, haga clic en la barra deslizante verde . Tenga en cuenta que esto puede disminuir el nivel de protección del servidor.

Para volver a activar la protección de un componente de seguridad desactivado, junto al correspondiente módulo, haga clic en la barra deslizante roja . El componente volverá al estado activado.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en el icono del engranaje .

Configuración de importación/exportación

Cargue los parámetros de configuración con un archivo de configuración *.xml* o guarde los parámetros de configuración actuales en un archivo de configuración.

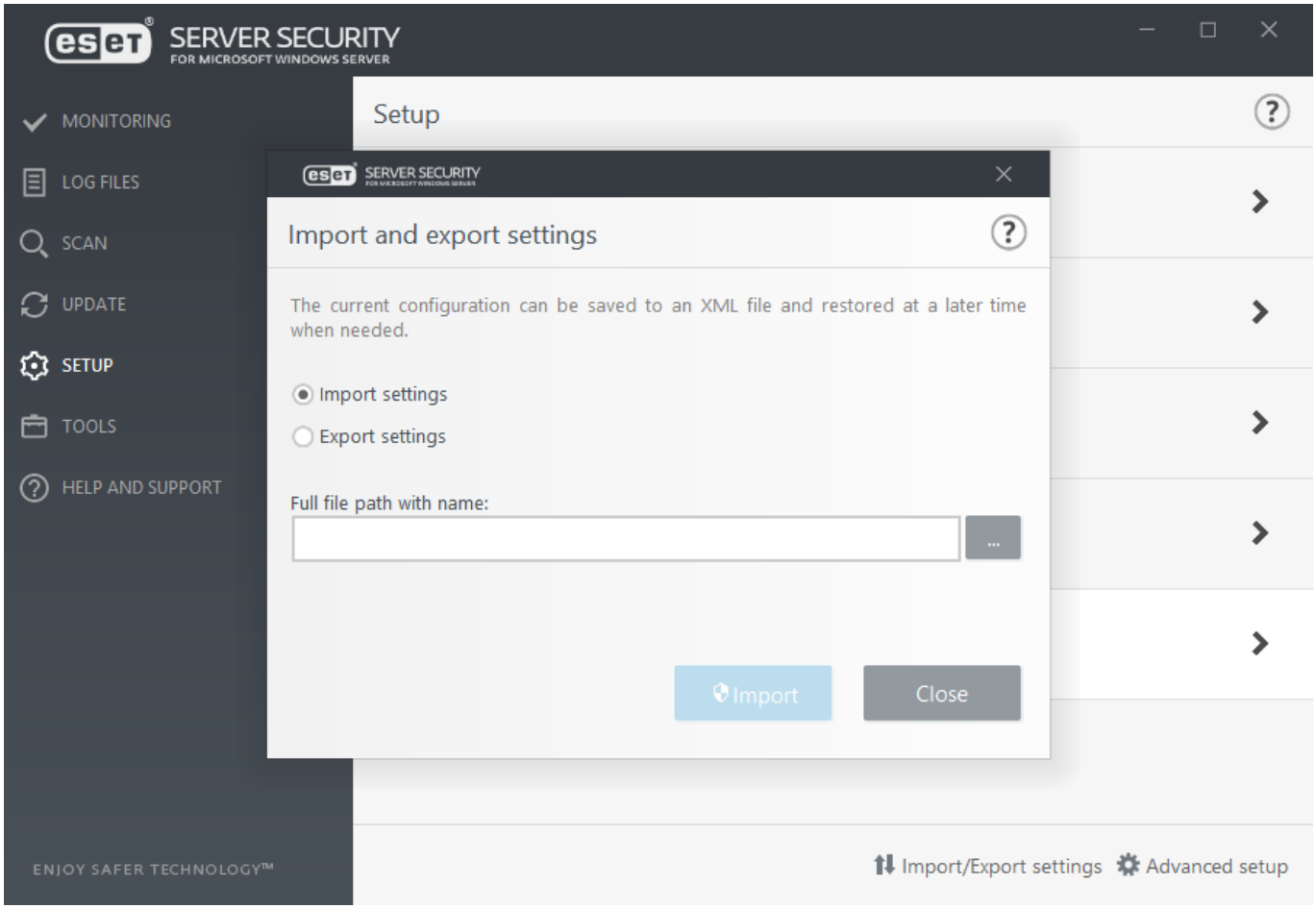
Configuración avanzada

Establezca las opciones y la configuración avanzada en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier lugar del programa, pulse **F5**.

Importar y exportar configuración

La función Importar/exportar configuración resulta útil si necesita realizar una copia de seguridad de la configuración actual de su ESET Server Security. También puede utilizar la función de importación para distribuir o aplicar la misma configuración a otros servidores con ESET Server Security. La configuración se exporta a un

archivo *.xml*.



NOTA
Si no dispone de derechos para escribir el archivo exportado en el directorio especificado, puede encontrarse con un error al exportar la configuración.

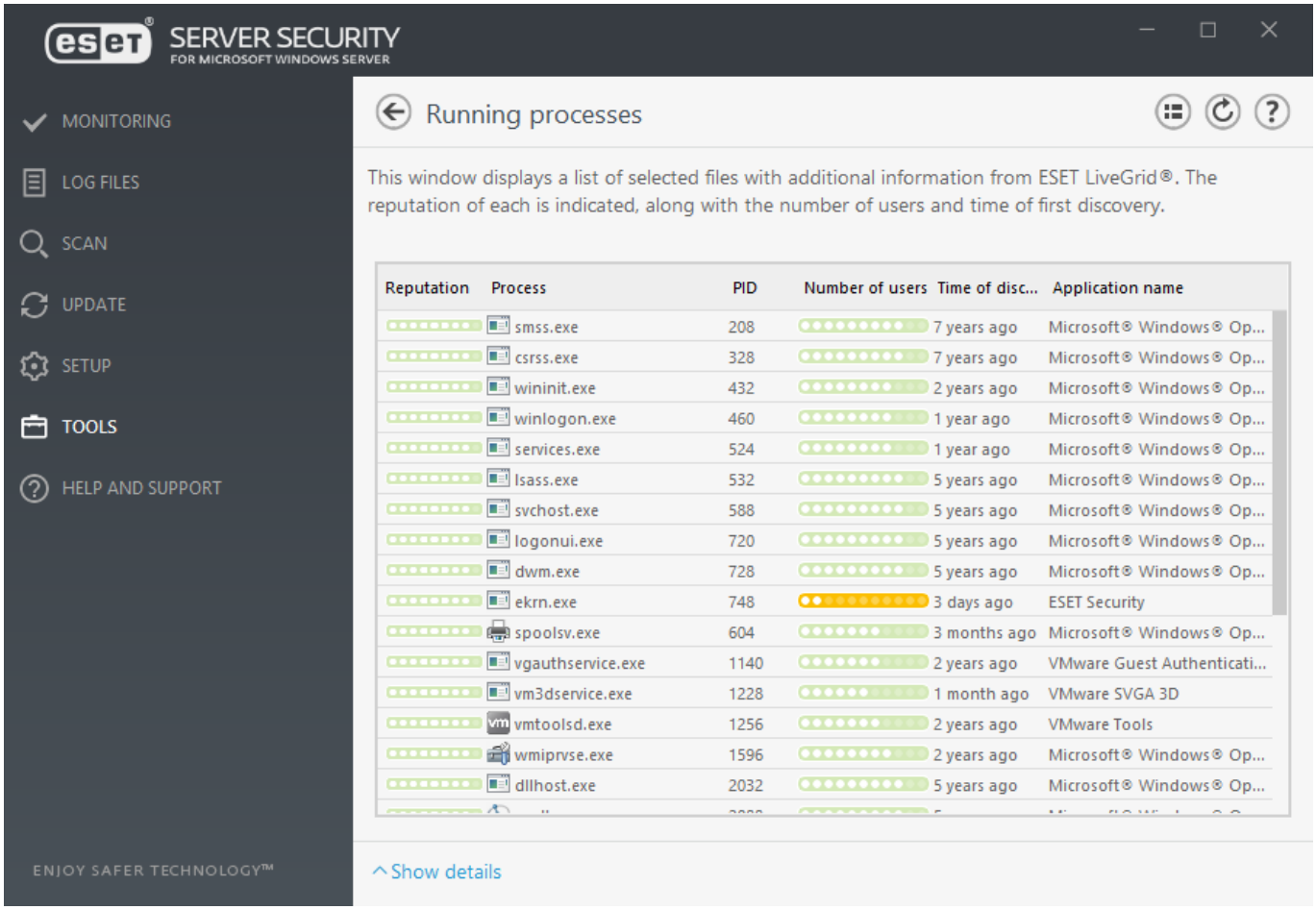
Herramientas

Están disponibles las siguientes funciones para la administración de ESET Server Security:

- Procesos en ejecución
- Observar actividad
- Estadísticas de protección
- Clúster
- ESET Shell
- ESET Dynamic Threat Defense
- ESET SysInspector
- ESET SysRescue Live
- Planificador de tareas
- Enviar muestra para el análisis
- Cuarentena

Procesos en ejecución

En Procesos en ejecución se indican los programas o procesos que se están ejecutando en el ordenador y se informa a ESET de forma inmediata y continua de las nuevas amenazas. ESET Server Security proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET LiveGrid® activada.



NOTA

Las aplicaciones conocidas marcadas como Mejor reputación (verde) son seguras (están incluidas en la lista blanca) y no se analizarán; esto aumentará la velocidad del análisis a petición del ordenador o la protección del sistema de archivos en tiempo real.

Reputación	**Generalmente, ESET Server Security y la tecnología ESET LiveGrid® determinan la reputación del objeto con una serie de reglas heurísticas que examinan las características de cada objeto (archivos, procesos, claves del registro, etc.) y, después, ponderan el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de reputación desde el valor "9: Mejor reputación" (verde) hasta "0: Peor reputación" (rojo).**
Proceso	Nombre de la imagen del programa o proceso que se está ejecutando en el ordenador. También puede utilizar el Administrador de tareas de Windows para ver todos los procesos que están en ejecución en el ordenador. Para abrir el Administrador de tareas, haga clic con el botón derecho del ratón en un área vacía de la barra de tareas y, a continuación, haga clic en Administrador de tareas o pulse la combinación Ctrl + Mayús + Esc en el teclado.
PID	Se trata de un identificador de los procesos que se ejecutan en sistemas operativos Windows.
Número de usuarios	El número de usuarios que utilizan una aplicación determinada. La tecnología ESET LiveGrid® se encarga de recopilar esta información.
Hora de la detección	Tiempo transcurrido desde que la tecnología ESET LiveGrid® detectó la aplicación.
Nombre de la aplicación	Nombre del programa al que pertenece este proceso.

NOTA
Cuando una aplicación se marca con Desconocido (naranja), no siempre se trata de software malicioso. Normalmente, se trata de una aplicación reciente. Si el archivo le plantea dudas, utilice la característica Enviar muestra para su análisis para enviarlo al laboratorio de virus de ESET. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una de las siguientes actualizaciones del motor de detección.

Mostrar detalles

La siguiente información aparecerá en la parte inferior de la ventana:

- **Ruta:** ubicación de una aplicación en el ordenador.
- **Tamaño**: tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Descripción**: características del archivo de acuerdo con la descripción del sistema operativo.
- **Empresa**: nombre del proveedor o el proceso de la aplicación.
- **Versión**: información sobre el editor de la aplicación.
- **Producto**: nombre de la aplicación o nombre comercial.
- **Fecha de creación**: fecha y hora en que se creó una aplicación.
- **Fecha de modificación**: última fecha y hora en que se modificó una aplicación.

Agregar a exclusiones de procesos

Haga clic con el botón derecho del ratón en un proceso de la ventana Procesos en ejecución para excluirlo del análisis. Su ruta de acceso se agregará a la lista de Exclusiones de procesos.

Observar actividad

La opción Observar actividad incluye actividad en formato gráfico; seleccione la siguiente actividad en el menú desplegable:

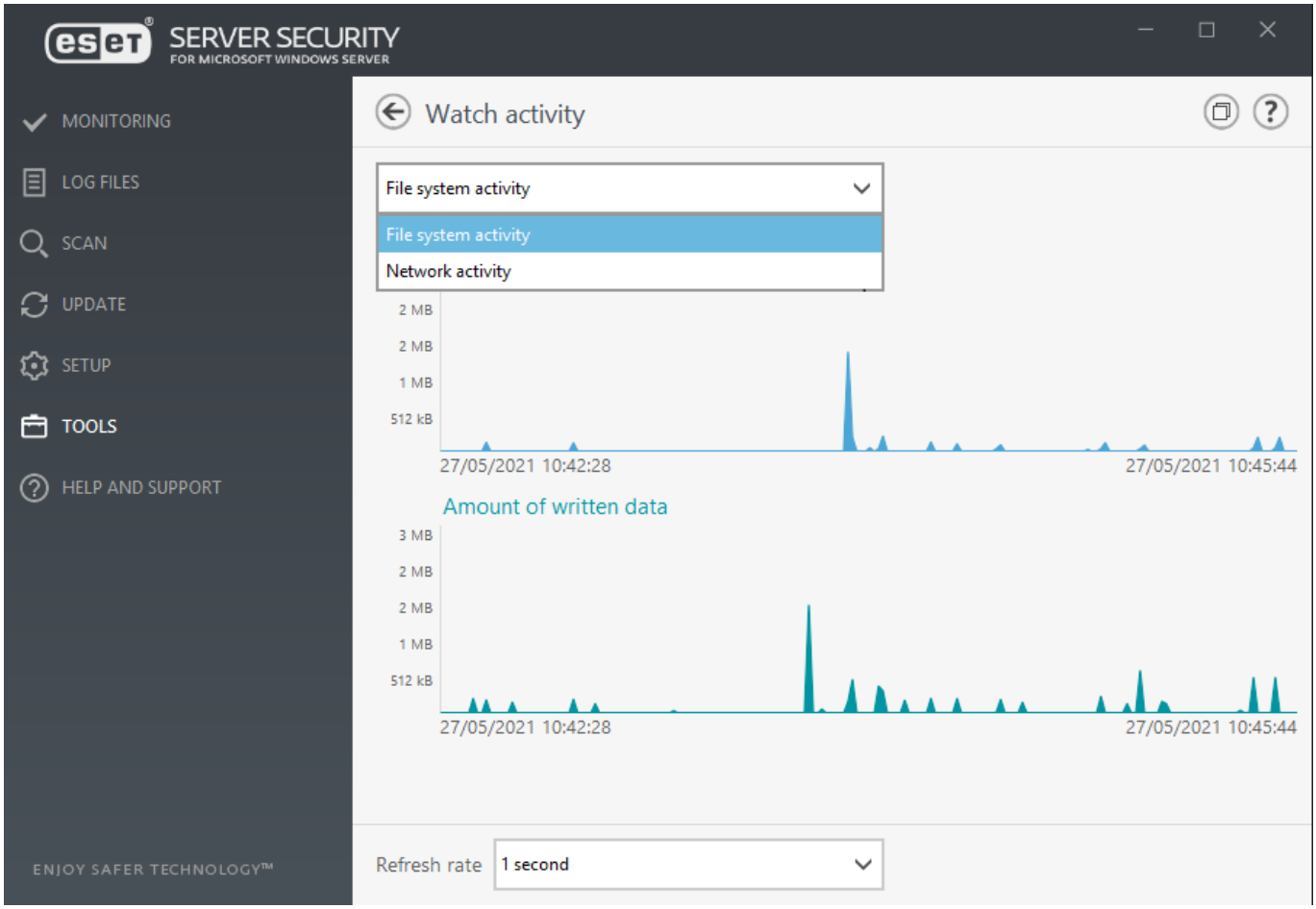
Actividad del sistema de archivos

Cantidad de datos leídos o escritos. El eje vertical del gráfico representa los datos leídos (azul) y los datos escritos (verde).

Actividad de red

Cantidad de datos recibidos o enviados. El eje vertical del gráfico representa los datos recibidos (azul) y los datos enviados (verde).

En la parte inferior del gráfico hay una línea cronológica que registra la actividad del sistema de archivos en tiempo real en el intervalo de tiempo seleccionado. Utilice el menú desplegable **Índice de actualización** para modificar la frecuencia de las actualizaciones.

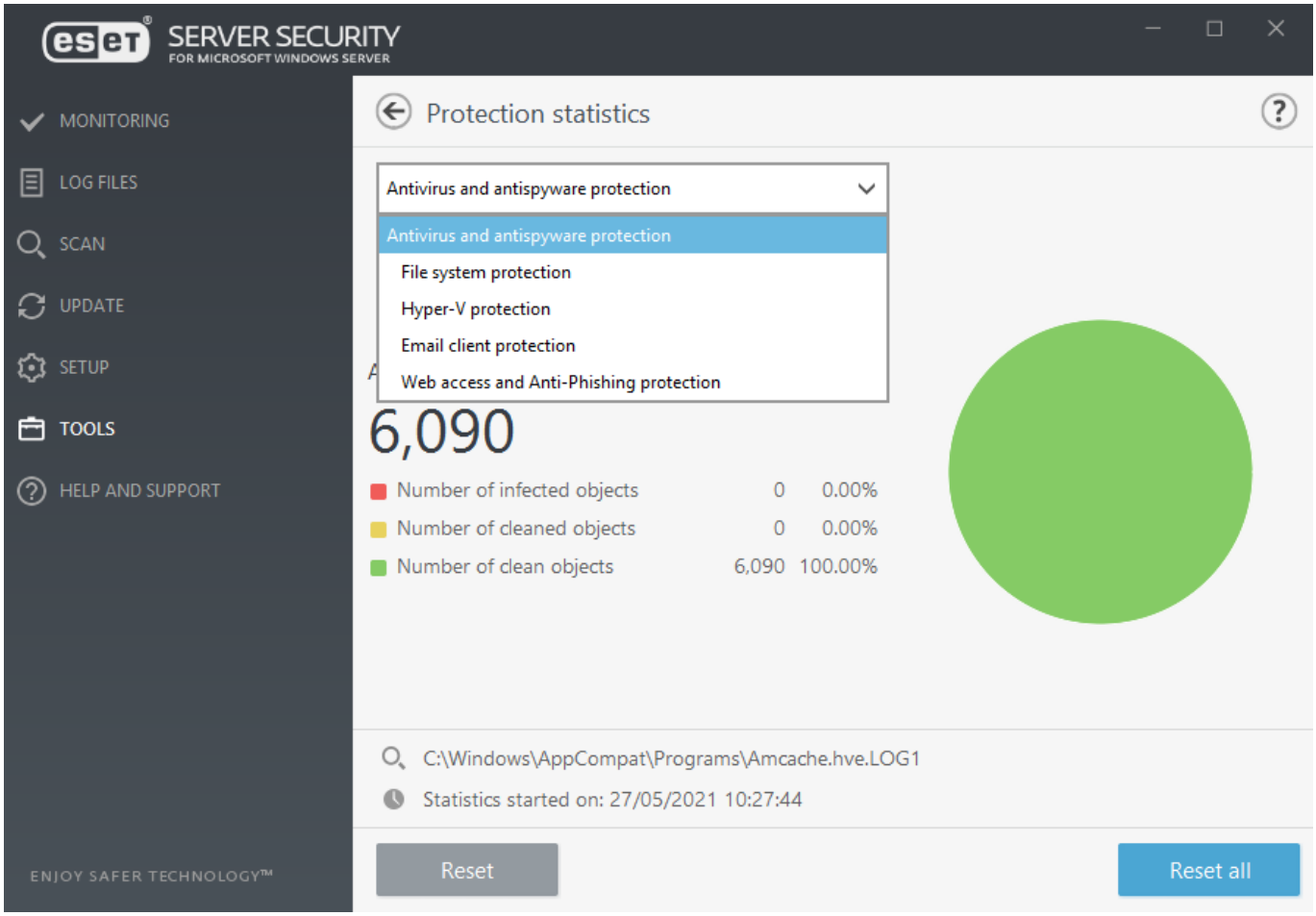


Están disponibles las opciones siguientes:

1 segundo	El gráfico se actualiza cada segundo y la línea cronológica abarca los últimos 10 minutos.
1 minuto (últimas 24 horas)	El gráfico se actualiza cada minuto y la línea cronológica abarca las últimas 24 horas.
1 hora (último mes)	El gráfico se actualiza cada hora y la línea cronológica abarca el último mes.
1 hora (mes seleccionado)	El gráfico se actualiza cada hora y la línea cronológica abarca el mes seleccionado. Seleccione un mes (y un año) en el menú desplegable para ver la actividad. Haga clic en **Cambiar**.

Estadísticas de protección

Para ver datos estadísticos de los módulos de protección de ESET Server Security, seleccione el módulo de protección en cuestión en el menú desplegable. Entre las estadísticas se incluye información como el número de objetos analizados, el número de objetos infectados, el número de objetos desinfectados y el número de objetos sin amenazas. Coloque el cursor del ratón junto a un objeto situado junto al gráfico y solo se mostrarán en el gráfico los datos correspondientes a ese objeto. Para borrar las estadísticas del módulo de protección actual, haga clic en **Restablecer**. Para borrar los datos de todos los módulos, haga clic en **Restablecer todo**.



En ESET Server Security están disponibles los siguientes gráficos de estadísticas:

Protección antivirus y antispyware

Muestra el número total de objetos infectados y desinfectados.

Protección del sistema de archivos

Solo muestra objetos que se leyeron o escribieron en el sistema de archivos.

Protección de Hyper-V

Muestra el número total de objetos infectados, desinfectados y sin amenazas (solo en sistemas con Hyper-V).

Protección del cliente de correo electrónico

Solo muestra objetos que se enviaron o recibieron a través de clientes de correo electrónico.

Protección Anti-Phishing y del tráfico de Internet

Solo muestra objetos descargados por los navegadores web.

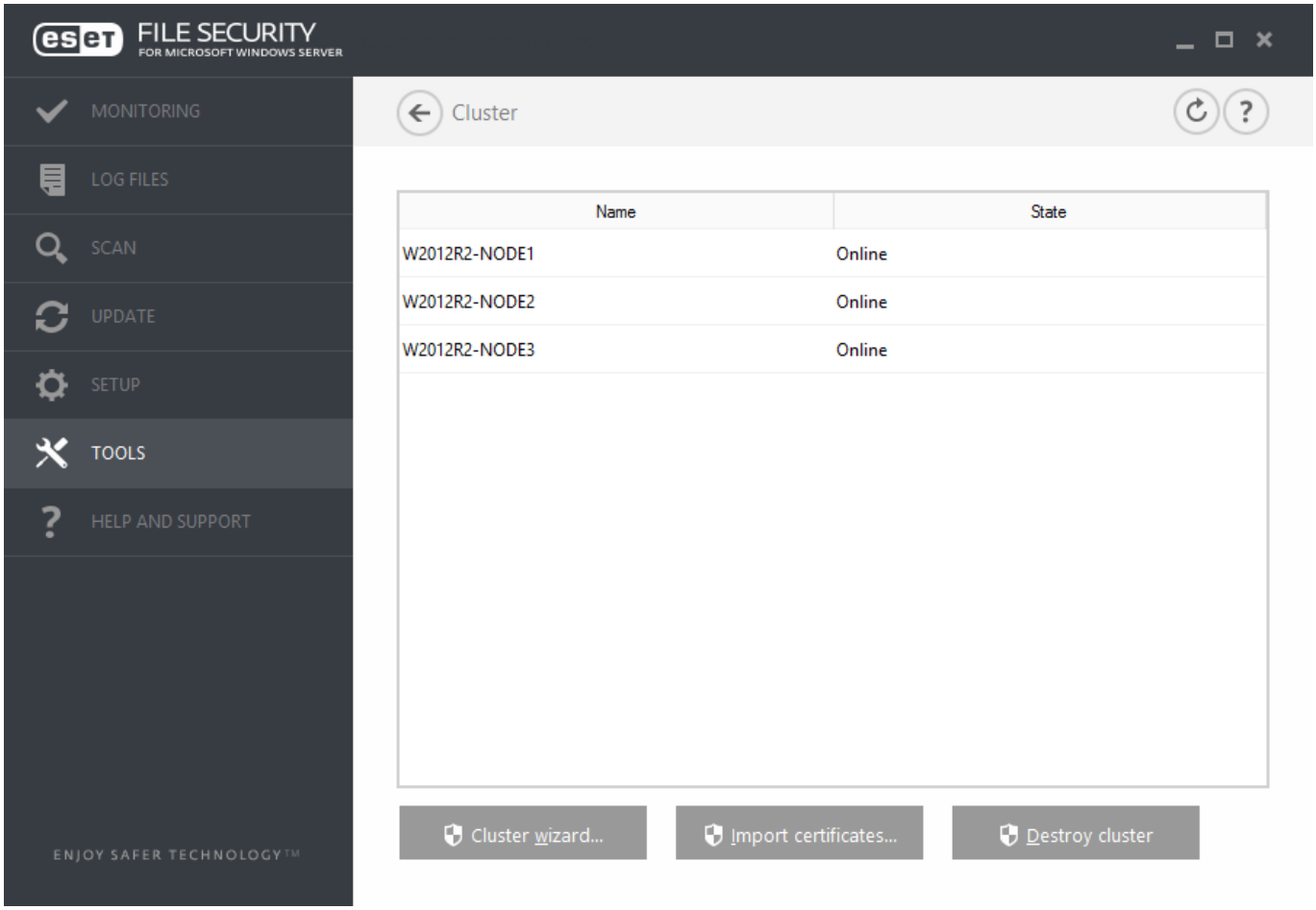
Clúster

El **Clúster de ESET** es una infraestructura de comunicación P2P de la gama de productos ESET para Microsoft Windows Server.

Esta infraestructura permite que los productos para servidor de ESET se comuniquen entre sí e intercambien datos, como configuraciones y notificaciones y pueden como sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias del producto. Un ejemplo de este tipo de grupo es un grupo de nodos de un clúster de conmutación por error de Windows o un clúster de equilibrio de carga de red (NLB) con productos de ESET instalados en el que es necesario que el producto tenga la misma configuración en todo el clúster. Clúster de ESET garantiza esta coherencia entre instancias.

NOTA
Los ajustes de la interfaz de usuario y las tareas programadas no se sincronizan entre los nodos del Clúster de ESET. Este comportamiento es intencionado.

A la página de estado de Clúster de ESET se accede desde el menú principal, con la ruta **Herramientas** > **Clúster**; cuando está correctamente configurado, la apariencia de la página de estado debe ser la siguiente:



NOTA
No es posible crear un Clúster de ESET entre ESET Server Security y ESET File Security para Linux.

Durante la configuración del Clúster de ESET, hay dos formas de agregar los nodos:

Autodetectar

Si ya tiene un clúster de conmutación por error de Windows o de equilibrio de carga de red (NLB), la función Autodetectar añadirá automáticamente sus nodos de miembros al Clúster de ESET.

Examinar

Permite agregar los nodos manualmente; para ello, escriba el nombre de los servidores (tanto miembros del mismo grupo de trabajo como miembros del mismo dominio).

NOTA
Los servidores no tienen que ser miembros de un clúster de conmutación por error de Windows o de un clúster NLB para poder usar la función Clúster de ESET. No es necesario que haya un clúster de conmutación por error de Windows ni un clúster NLB en el entorno para poder usar los Clústeres de ESET.

Tras agregar los nodos a su Clúster de ESET, el siguiente paso del proceso es instalar ESET Server Security en cada nodo. Esta tarea se realiza automáticamente durante la configuración del Clúster de ESET. Las credenciales que son necesarias para la instalación remota de ESET Server Security en otros nodos del clúster:

Entorno de dominio

Credenciales de administrador del dominio.

Entorno de grupo de trabajo

Debe asegurarse de que todos los nodos usan las credenciales de la misma cuenta de administrador local.

En un Clúster de ESET también puede usar una combinación de nodos agregados automáticamente como miembros de un clúster de conmutación por error de Windows o NLB y nodos agregados manualmente (siempre que estén en el mismo dominio).

IMPORTANTE
No es posible combinar nodos de dominio con nodos de grupo de trabajo.

Otro de los requisitos de uso del Clúster de ESET es que debe estar activada la opción **Compartir archivos e impresoras** en el Firewall de Windows antes de insertar la instalación de ESET Server Security en los nodos de Clúster de ESET.

Es posible agregar nodos nuevos a un Clúster de ESET existente en cualquier momento si se ejecuta el Asistente de clúster.

Importar certificados

Los certificados se utilizan para ofrecer una autenticación robusta a la máquina cuando se utiliza HTTPS. Hay una jerarquía independiente de certificados para cada Clúster de ESET. La jerarquía tiene un certificado raíz y un conjunto de certificados de nodo firmados por el certificado raíz. La clave privada del certificado raíz se destruye después de crear todos los certificados de nodo. Si añade un nuevo nodo al clúster, se crea una nueva jerarquía de certificado. Diríjase a la carpeta que incluye los certificados (que se generaron durante el Asistente de clúster). Seleccione el archivo de certificado y haga clic en **Abrir**.

Destruir clúster

Los Clústeres de ESET pueden desmantelarse. Cada uno de los nodos anotará una entrada en su registro de sucesos en relación a la destrucción de los Clústeres de ESET. A continuación, todas las reglas del cortafuegos de ESET se eliminan del Firewall de Windows. Los antiguos nodos recuperarán su estado anterior, y pueden usarse de nuevo en otro Clúster de ESET, si así se desea.

Asistente de clúster: Seleccionar nodos

Al configurar un Clúster de ESET, el primer paso consiste en agregar los nodos. Para ello puede usar las opciones **Detección automática** o **Examinar**. También puede escribir el nombre del servidor en el cuadro de texto y hacer clic en el botón **Agregar**.

Autodetectar

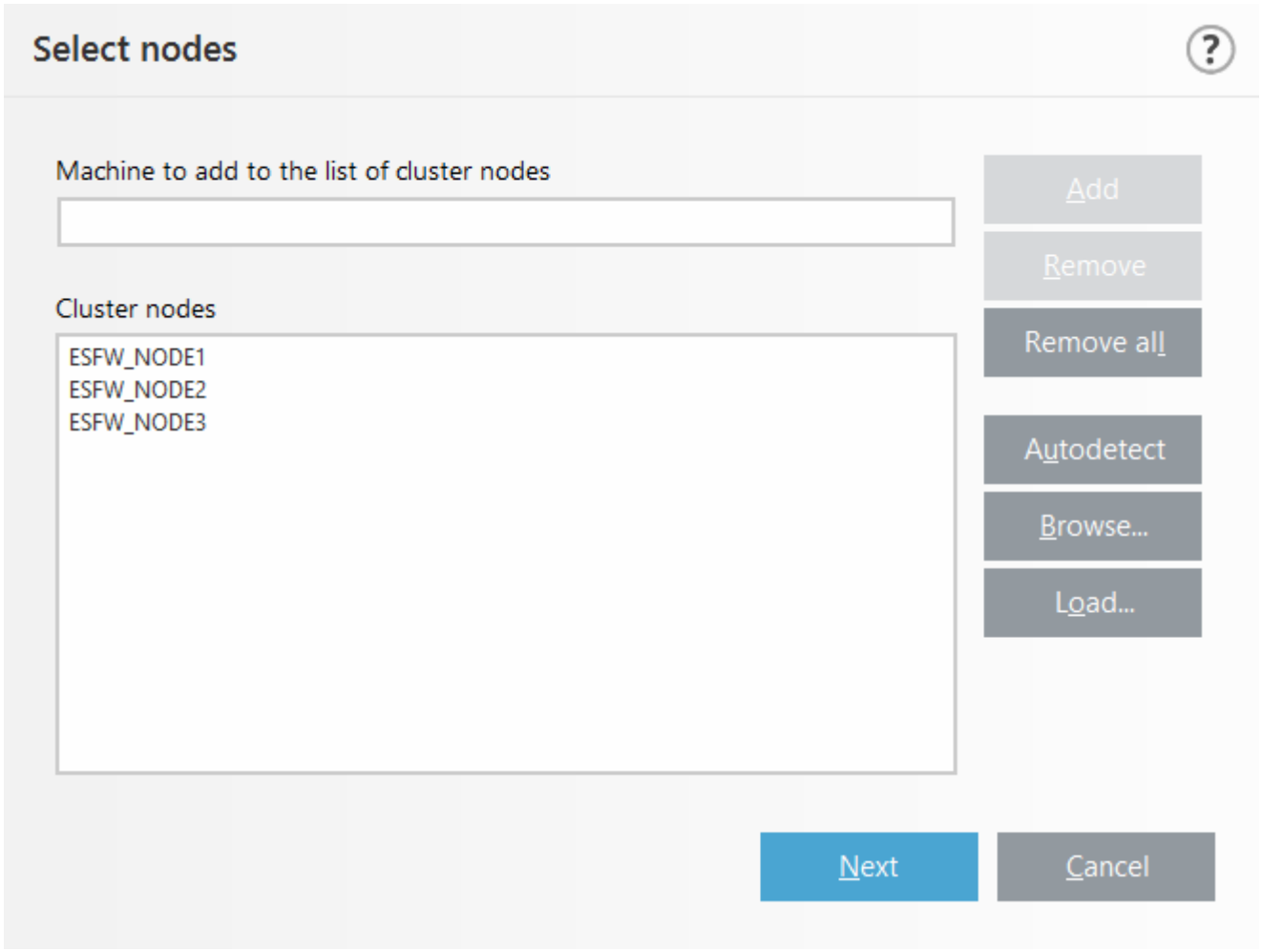
Agrega automáticamente los nodos de un Windows Failover Cluster o un Network Load Balancing (NLB) Cluster existentes. El servidor que use para crear el ESET Cluster debe ser miembro de este Windows Failover Cluster o este NLB Cluster para agregar automáticamente los nodos. El NLB Cluster debe tener activada la función **Permitir control remoto** en las propiedades del clúster para que el ESET Cluster detecte los nodos correctamente. Cuando tenga la lista de los nodos recién agregados, podrá quitar los que no desee.

Examinar

Esta opción se utiliza para encontrar y seleccionar ordenadores de un Domain o Workgroup. Este método permite agregar manualmente los nodos al Clúster de ESET. Otra de las formas de agregar nodos es escribir el nombre de host del servidor que desea agregar y hacer clic en **Agregar**.

Cargar

Se usa para importar una lista de nodos desde un archivo.



Si desea modificar los **Nodos del clúster** que aparecen en la lista, seleccione el nodo que desee quitar y haga clic en **Quitar**. Si desea borrar la lista por completo, haga clic en **Quitar todo**.

Si ya dispone de un Clúster de ESET existente, puede agregar nodos nuevos en cualquier momento. Los pasos son los mismos que los descritos anteriormente.

> NOTA
> todos los nodos que permanezcan en la lista deben estar en línea y ser accesibles. El host local se agrega a los nodos del clúster de forma predeterminada.

Asistente de clúster: Configuración del clúster

Le permite definir el nombre de clúster y las especificaciones de la red (si es necesario).

Nombre del clúster

Escriba el nombre de su clúster y haga clic en **Siguiente**.

Puerto de escucha: (el puerto predeterminado es el 9777)

Si ya utiliza el puerto 9777 en su entorno de red, especifique otro número de puerto que no se utilice.

Abrir puerto en firewall de Windows

Cuando esta opción se activa, se crea una regla en el Firewall de Windows.

Asistente de clúster: Configuración de conexión del clúster

Le permite definir el modo de distribución del certificado y si desea instalar el producto en otros nodos o no.

Distribución de certificado

- **Remoto** automático: el certificado se instalará automáticamente.
- **Manual**: haga clic en **Generar** y seleccione la carpeta en la que desea guardar los certificados. Se crearán tanto un certificado raíz como un certificado para cada nodo, incluido el que se crea para el nodo (máquina local) desde el que está configurando el Clúster de ESET. Para inscribir el certificado en la máquina local, haga clic en **Sí**.

Instalación del producto en otros nodos

- **Remoto automático**: ESET Server Security se instalará automáticamente en cada nodo (siempre que los sistemas operativos tengan la misma arquitectura).
- **Manual**: instale ESET Server Security manualmente (por ejemplo, cuando tiene arquitecturas de SO distintas en algunos nodos).

Enviar licencia a nodos sin el producto activado

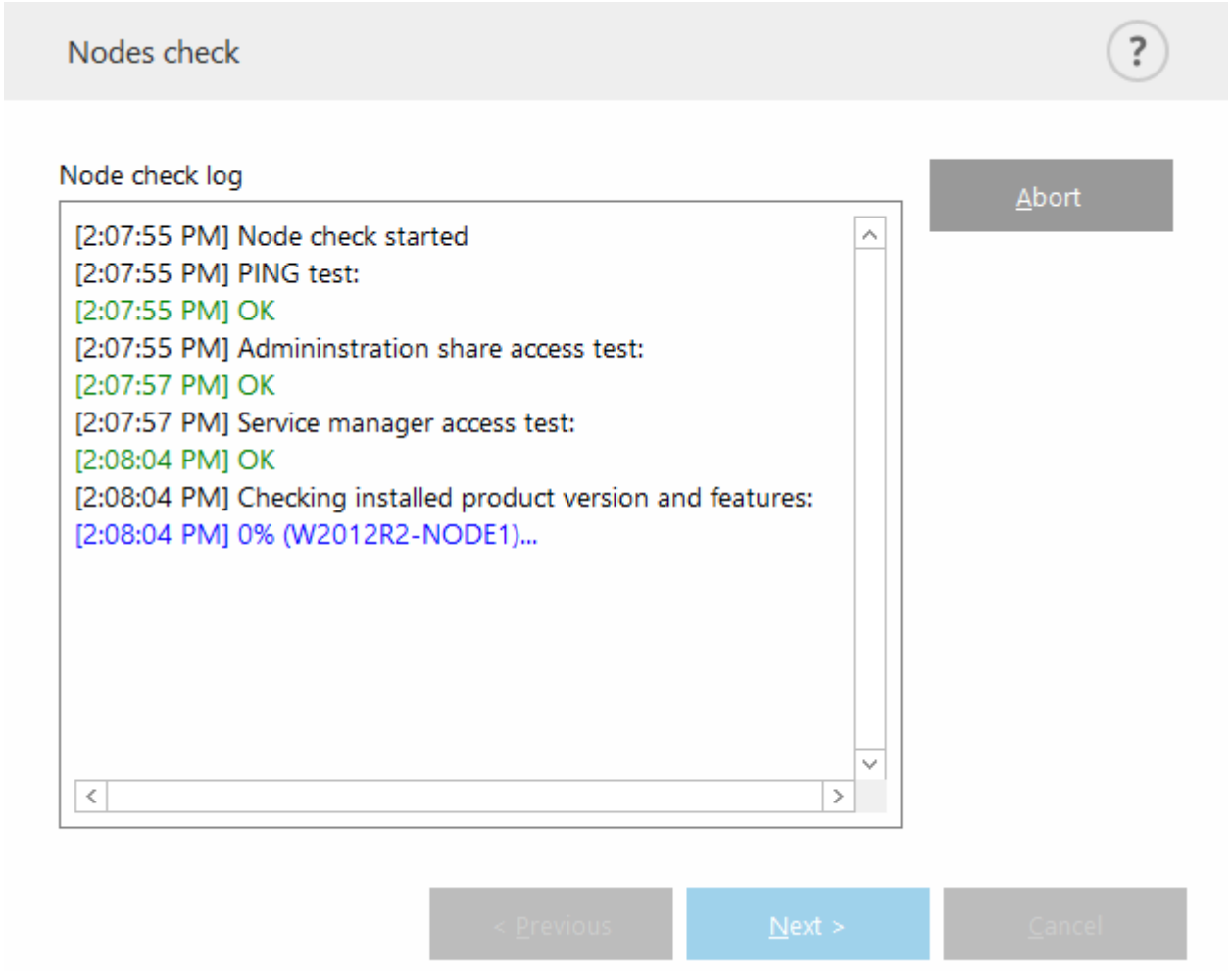
ESET Security activa automáticamente las soluciones de ESET instaladas en los nodos sin licencias.

NOTA
Para crear un Clúster de ESET con arquitecturas de sistema operativo mixtas (32 bits y 64 bits), instale ESET Server Security manualmente. Los sistemas operativos en uso se detectarán durante los próximos pasos, y verá esta información en la ventana de registro.

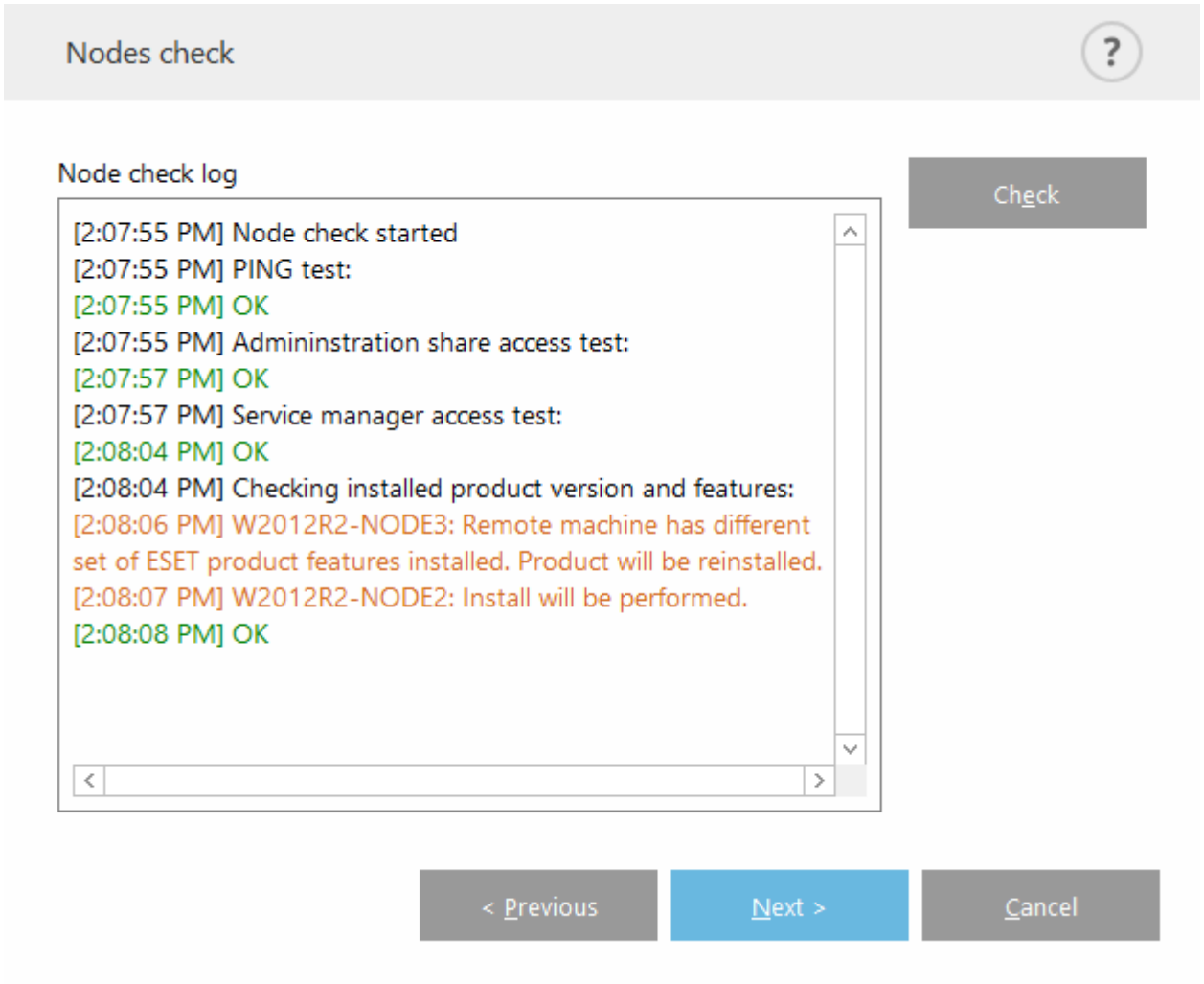
Asistente de clúster: Comprobación de nodos

Después de especificarse los detalles de la instalación se ejecuta una comprobación de nodos. La siguiente información aparecerá en el **Registro de comprobación del nodo**:

- Comprobación de que todos los nodos existentes están en línea.
- Comprobación de que puede accederse a los nodos nuevos.
- El nodo está en línea.
- Puede accederse al recurso compartido de administración.
- Es posible la ejecución remota.
- Están instaladas las versiones correctas de los productos (o no hay ningún producto instalado).
- Comprobación de que están presentes los nuevos certificados.

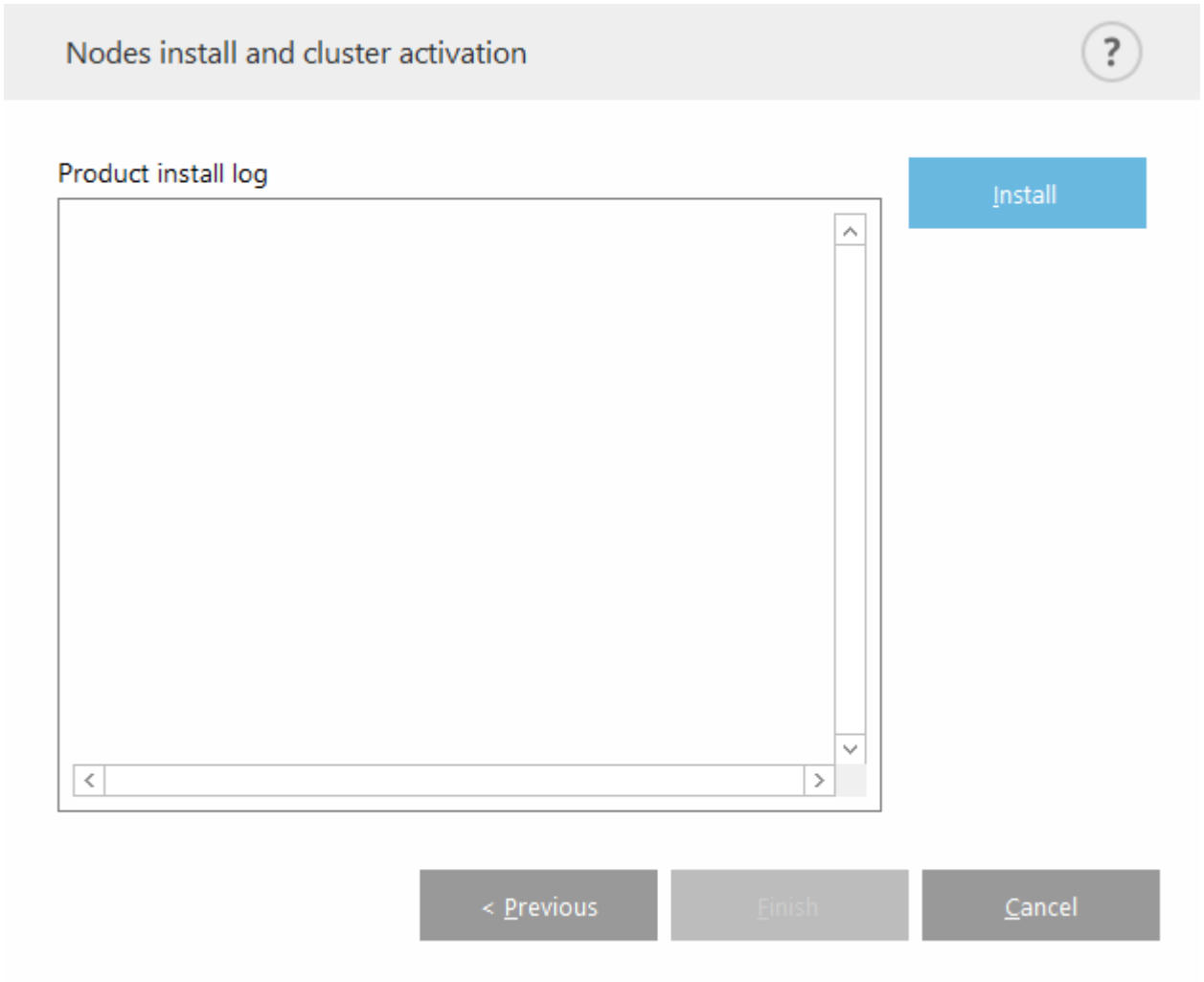


Verá el informe cuando concluya la comprobación de nodos:

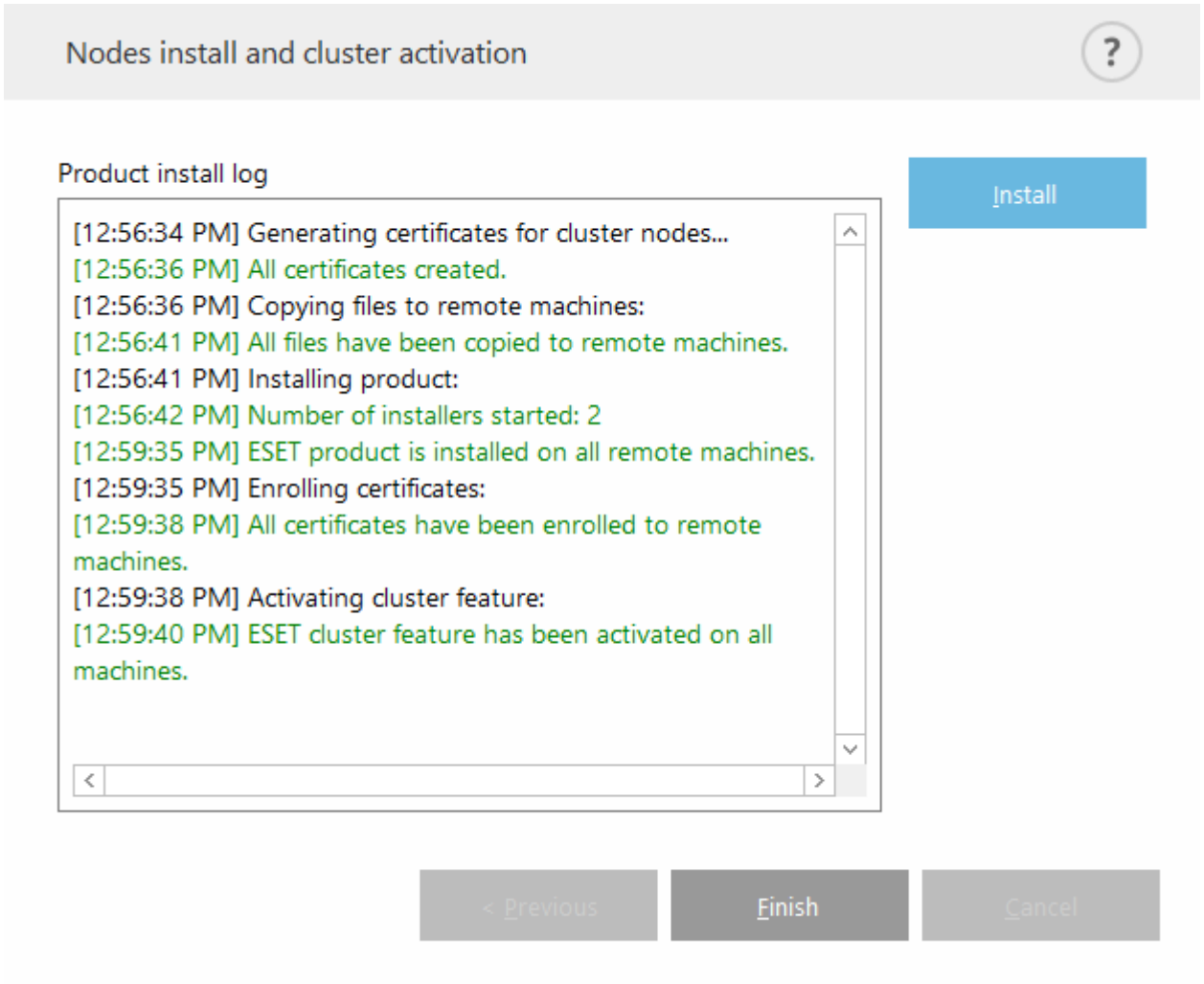


Asistente de clúster: Instalación de nodos

Al realizar la instalación en una máquina remota durante la inicialización del Clúster de ESET, el asistente intentará localizar el instalador en el directorio *%ProgramData%\ESET\ESET Security\Installer*. Si no se encuentra el paquete de instalación, deberá localizar el archivo del instalador.

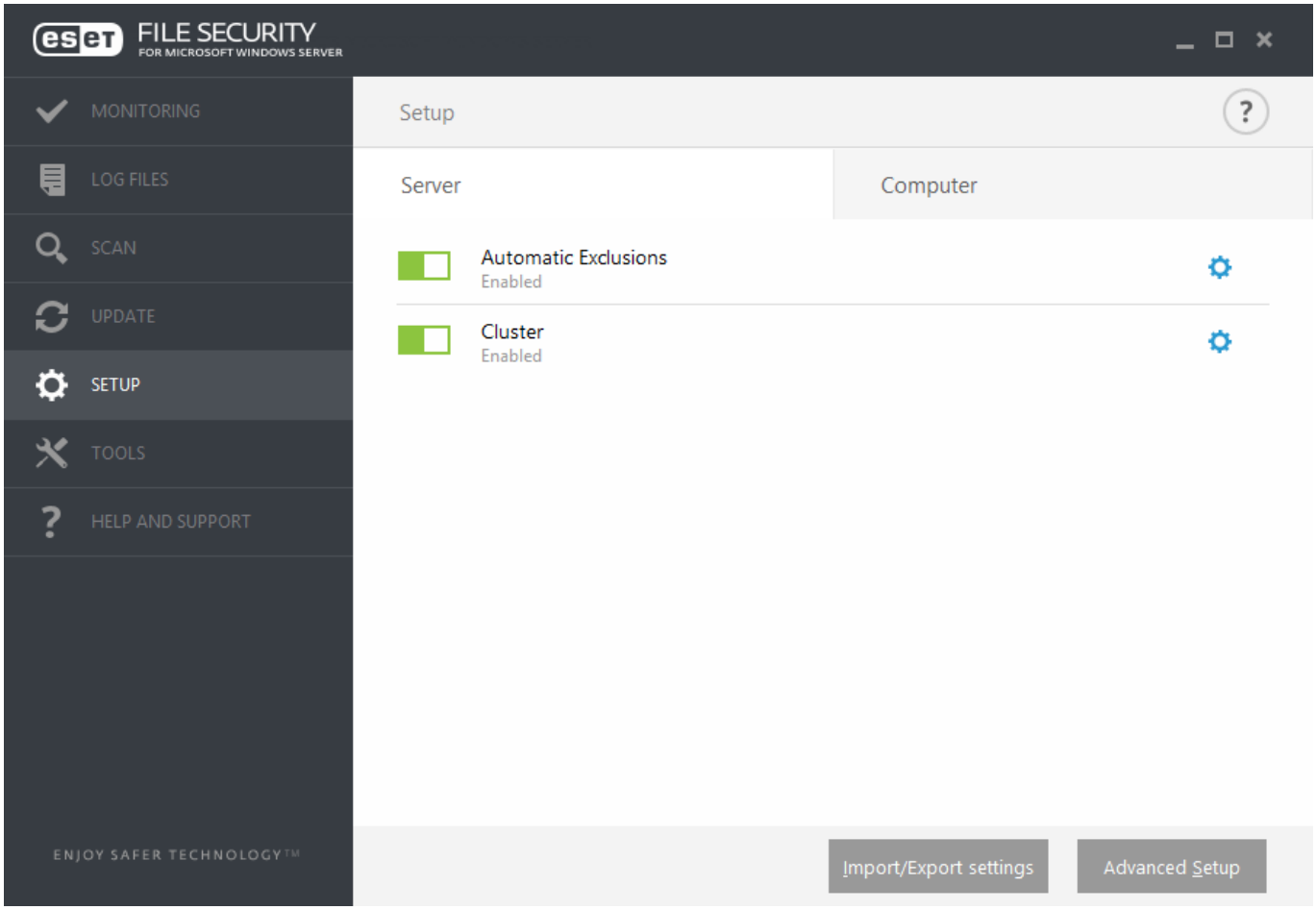


NOTA
Al intentar usar la instalación remota automática en un nodo con una arquitectura distinta (32 bits frente a 64 bits) se detectará esta situación y se le pedirá que ejecute una instalación manual.



Una vez que haya configurado correctamente el Clúster de ESET, este aparecerá en la página **Configuración** > **Servidor** como activado.

NOTA
Si ya se ha instalado una versión más antigua de ESET Server Security en algunos nodos, recibirá una notificación indicándole que estas máquinas requieren la versión más reciente. Al actualizar ESET Server Security el equipo puede reiniciarse automáticamente.



Además, puede consultar su estado en la página de estado del clúster (**Herramientas** > **Clúster**).

ESET Shell

eShell (abreviación de ESET Shell) es una interfaz de línea de comandos para ESET Server Security. Se trata de una alternativa a la interfaz gráfica de usuario (GUI). eShell tiene todas las características y opciones que suele ofrecer una interfaz gráfica de usuario; eShellademás, le permite configurar y administrar todo el programa sin necesidad de utilizar la GUI.

Además de todas las funciones y características disponibles en la GUI, también le ofrece una función de automatización mediante la ejecución de scripts para configurar, modificar una configuración o realizar una acción. eShell también puede ser de utilidad para aquellos que prefieren utilizar la línea de comandos en vez de la GUI.

> NOTA
> Recomendamos que, para esta función, abra eShell con la opción Ejecutar como administrador. La misma recomendación se aplica a la ejecución de un solo comando desde el símbolo del sistema de Windows (cmd). Abra el símbolo del sistema con Ejecutar como administrador. Si no ejecuta el símbolo del sistema como administrador, no podría ejecutar los comandos debido a la falta de permisos.

eShell se puede ejecutar en dos modos:

1. **Modo interactivo**: es útil para trabajar con eShell (no simplemente ejecutar un comando); por ejemplo, para realizar tareas como cambiar la configuración o ver los registros. También puede utilizar el modo interactivo si aún no está familiarizado con todos los comandos, ya que facilita la navegación por eShell.

En este modo, se muestran los comandos disponibles para un contexto determinado.

2. **Modo por lotes/un solo comando:** puede utilizar este modo si tan solo necesita ejecutar un comando, sin acceder al modo interactivo de eShell. Para ello, escriba eshell con los parámetros adecuados en la ventana de símbolo del sistema de Windows.

EJEMPLO
`eshell get status` o `eshell computer set real-time status disabled 1h`

Para poder ejecutar determinados comandos (como el del segundo ejemplo anterior) en el modo por lotes/de script, debe configurar primero algunos ajustes. De lo contrario, se mostrará el mensaje **Acceso denegado**. Esto se debe a cuestiones de seguridad.

NOTA
Para poder utilizar comandos eShell desde el símbolo del sistema de Windows deberá modificarse la configuración. Si desea obtener más información sobre la ejecución de archivos por lotes, haga clic aquí.

Existen dos formas de acceder al modo interactivo en eShell:

1. Desde el menú **Inicio de Windows**: Inicio > Todos los programas > ESET > ESET File Security > ESET Shell

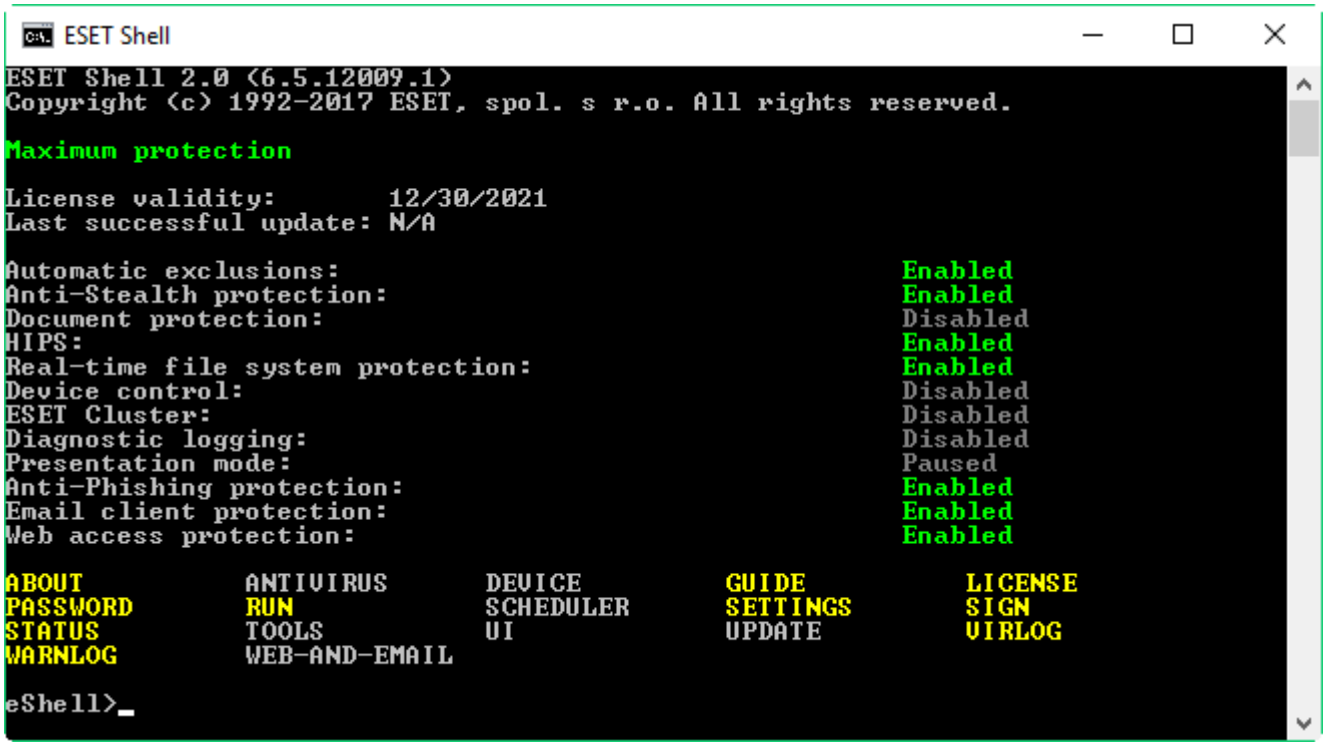
2. Desde el **símbolo del sistema de Windows**, escribiendo `eshell` y pulsando la tecla Intro.

IMPORTANTE
Si le aparece el error `'eshell' is not recognized as an internal or external command`, el motivo es que el sistema no ha cargado las nuevas variables de entorno tras la instalación de ESET Server Security. Abra un nuevo símbolo del sistema e intente iniciar eShell de nuevo. Si sigue apareciendo un error o tiene la Instalación del núcleo de ESET Server Security, inicie eShell utilizando la ruta de acceso absoluta, por ejemplo `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` (debe utilizar "" para que el comando funcione).

La primera vez que ejecute eShell en modo interactivo, se mostrará la pantalla de primera ejecución (una guía).

NOTA
Si desea ver otra vez la pantalla de primera ejecución, introduzca el comando `guide`. Muestra ejemplos básicos de cómo utilizar eShell con sintaxis, prefijos, rutas de comandos, formas abreviadas, alias, etc.

La próxima vez que ejecute eShell verá la siguiente pantalla:



> NOTA
> Los comandos no distinguen entre mayúsculas y minúsculas. Puede usar letras en mayúscula o en minúscula y el comando se ejecutará igualmente.

Personalización de eShell

Puede personalizar eShell en el contexto de `ui eshell`. Puede configurar el alias, los colores, el idioma, la política de ejecución de los scripts, la configuración de los comandos ocultos y mucho más.

Uso

Sintaxis

Los comandos deben presentar una sintaxis correcta para funcionar y pueden constar de un prefijo, contexto, argumentos, opciones, etc. Esta es la sintaxis general que se utiliza en eShell:

[<prefijo>] [<ruta del comando>] <comando> [<argumentos>]

Ejemplo (este ejemplo activa la protección de documentos):

```
SET COMPUTER SCANS DOCUMENT REGISTER ENABLED
```

- `SET` un prefijo
- `COMPUTER SCANS DOCUMENT` ruta de acceso a un comando determinado, contexto al que pertenece dicho comando
- `REGISTER` el comando propiamente dicho
- `ENABLED` argumento del comando

El uso de `?` como argumento de un comando, se mostrará la sintaxis de dicho comando. Por ejemplo, `STATUS ?` mostrará la sintaxis del comando `STATUS`:

SINTAXIS:

```
[get] status
```

OPERACIONES:

`get` Mostrar estado de todos los módulos de protección

Quizás haya observado que `[get]` está entre corchetes. Esto indica que el prefijo `get` es el predeterminado para el comando `status`. Esto quiere decir que, cuando ejecuta `status` sin especificar ningún prefijo, se utilizará el prefijo predeterminado (en este caso, `get status`). El uso de comandos sin prefijos ahorra tiempo a la hora de escribir. Normalmente, `get` es el prefijo predeterminado para la mayoría de los comandos, pero compruebe cuál es el prefijo predeterminado de un comando concreto para asegurarse de que es el que desea ejecutar.

> NOTA
> Los comandos no distinguen mayúsculas y minúsculas, por lo que el uso de unas u otras no afectará a su ejecución.

Prefijo/Operación

Un prefijo es una operación. El prefijo `GET` le proporcionará información sobre la configuración de una función determinada de ESET Server Security o le mostrará el estado (por ejemplo, `GET COMPUTER REAL-TIME STATUS` le mostrará el estado de protección actual del módulo de tiempo real). El prefijo `SET` configurará la funcionalidad o cambiará su estado (`SET COMPUTER REAL-TIME STATUS ENABLED` activará la protección en tiempo real).

Estos son los prefijos que permite utilizar eShell. No todos los comandos admiten todos los prefijos:

GET	indica la configuración o el estado actual
SET	establece un valor o estado
SELECT	selecciona un elemento
ADD	añade un elemento
REMOVE	elimina un elemento
CLEAR	quita todos los elementos o archivos
START	inicia una acción
STOP	detiene una acción
PAUSE	pone en pausa una acción
RESUME	reanuda una acción
RESTORE	restaura la configuración, el objeto o el archivo predeterminado
SEND	envía un objeto o archivo
IMPORT	importa desde un archivo
EXPORT	exporta a un archivo

> NOTA
> Los prefijos como `GET` y `SET` se utilizan con muchos comandos; y algunos comandos (como `EXIT`) no utilizan ningún prefijo.

Ruta/contexto del comando

Los comandos se colocan en contextos que conforman una estructura de árbol. El nivel superior del árbol es la raíz. Cuando ejecuta eShell, el usuario está en el nivel raíz:

```
eShell>
```

Puede ejecutar el comando desde este nivel o introducir el nombre de contexto para desplazarse por el árbol. Por ejemplo, si introduce el contexto `TOOLS`, se mostrará una lista con todos los comandos y subcontextos disponibles desde este nivel.

Los elementos amarillos son comandos que el usuario puede ejecutar y los elementos grises, subcontextos que puede especificar. U subcontexto contiene más comandos.

Si desea subir un nivel, escriba `..` (dos puntos).

> EJEMPLO
> Por ejemplo, si se encuentra aquí:
> `eShell computer real-time>`
> escriba `..` para subir un nivel a:
> `eShell computer>`

Si desea volver al nivel raíz desde `eShell computer real-time>` antivirus startup> (que está dos niveles por debajo del nivel raíz), simplemente escriba `.. ..` (dos puntos, un espacio y otros dos puntos). Así, subirá dos niveles hasta el nivel raíz, en este caso. Utilice una barra invertida `\` para volver directamente a raíz desde cualquier nivel, sea cual sea el punto del árbol contextual en el que se encuentre. Si desea acceder a un contexto determinado de niveles superiores, simplemente use el número correspondiente de comandos `..` para llegar al nivel deseado, utilizando el espacio como separador. Por ejemplo, si desea subir tres niveles, utilice `.. .. ..`

La ruta de acceso es relativa al contexto actual. Si el comando se encuentra en el contexto actual, no especifique una ruta de acceso. Por ejemplo, para ejecutar `GET COMPUTER REAL-TIME STATUS`, introduzca:

`GET COMPUTER STATUS` si se encuentra el contexto raíz (en la línea de comandos se muestra `eShell>`)
`GET STATUS` si se encuentra el contexto (en la línea de comandos se muestra `eShell computer>`)
`.. GET STATUS` si se encuentra el contexto (en la línea de comandos se muestra `eShell computer`

real-time>)

Puede utilizar un solo . (punto) en lugar de dos .. porque un punto es la abreviatura de los dos puntos.

> EJEMPLO
> . GET STATUS si se encuentra el contexto (en la línea de comandos se muestra eShell computer real-time>)

Argumento

Un argumento es una acción que se realiza para un comando determinado. Por ejemplo, el comando CLEAN-LEVEL (situado en COMPUTER REAL-TIME ENGINE) se puede utilizar con los argumentos siguientes:

rigorous Reparar la detección siempre
safe Reparar la detección si es seguro, mantener de otro modo
normal Reparar la detección si es seguro, preguntar de otro modo
none Preguntar siempre al usuario final

Otros ejemplos son los argumentos ENABLED o DISABLED, que se utilizan para activar o desactivar una función o característica determinadas.

Forma abreviada/comandos abreviados

eShell le permite acortar los contextos, comandos y argumentos (siempre que el argumento sea un modificador o una opción alternativa). Los argumentos o prefijos que sean un valor concreto, como un número, un nombre o una ruta de acceso, no se pueden acortar. Puede utilizar los números 1 y 0 en lugar de los argumentos activados o desactivados.

> EJEMPLO
> computer set real-time status enabled => com set real stat 1
> computer set real-time status disabled => com set real stat 0

Ejemplos de formas abreviadas:

> EJEMPLO
> computer set real-time status enabled => com set real stat en
> computer exclusions add detection-excludes object C:\path\file.ext => com excl add det obj C:\path\file.ext
> computer exclusions remove detection-excludes 1 => com excl rem det 1

Si dos comandos o contextos empiezan con las mismas letras (por ejemplo ADVANCED y AUTO-EXCLUSIONS, e introduce AA como comando abreviado), eShell no podrá decidir cuál de los dos comandos desea ejecutar y se mostrará un mensaje de error con los comandos que empiezan por "A" que puede elegir:

```
eShell>a

The following command is not unique: a
```

Los siguientes subcontextos están disponibles en el contexto COMPUTER:

ADVANCED

```
AUTO-EXCLUSIONS
```

Al agregar una o más letras (por ejemplo, `AD` en lugar de simplemente `A`), eShell introducirá el subcontexto `ADVANCED`, puesto que ahora es único. Lo mismo se aplica a los comandos abreviados.

> NOTA
> Cuando quiera asegurarse de que un comando se ejecute como necesita, le recomendamos que no abrevie comandos, argumentos, etc., sino que utilice la forma completa. Así, eShell ejecutará exactamente lo que necesita, y evitará errores. Esto es especialmente importante en el caso de archivos por lotes y scripts.

Finalización automática

Esta nueva función se introdujo en eShell 2.0 y es muy similar a la finalización automática del símbolo del sistema de Windows. Mientras que el símbolo del sistema de Windows finaliza rutas de acceso a archivos, eShell finaliza comandos, contexto y nombres de operaciones. La finalización de argumentos no es compatible. Cuando escriba comandos, pulse Tab para finalizarlos o ver las variaciones disponibles. Pulse Mayús + Tab para ver las variaciones en sentido inverso. No se puede mezclar la forma abreviada con la finalización automática. Utilice una o la otra. Por ejemplo, cuando escriba `computer real-time additional`, no pasará nada si pulsa Tab. En lugar de eso, escriba `com` y, a continuación, pulse Tab para finalizar `computer`, continúe escribiendo `real` y pulse Tab, `add` y pulse Tab y pulse Entrar. Escriba `on` y pulse Tab y continúe pulsando Tab para ver todas las variaciones disponibles: `on-execute-ah`, `on-execute-ah-removable`, `on-write-ah`, `on-write-archive-default`, etc.

Alias

Un alias es un nombre alternativo que se puede utilizar para ejecutar un comando (siempre que el comando tenga un alias asignado). Hay varios alias predeterminados:

`(global) close` cerrar
`(global) quit` cerrar
`(global) bye` cerrar
`warnlog` sucesos de registro de herramientas
`virlog` detecciones de registro de herramientas

"(global)" significa que el comando se puede utilizar en cualquier sitio, independientemente del contexto actual. Un comando puede tener varios alias asignados; por ejemplo, el comando `EXIT` tiene los alias `CLOSE`, `QUIT` y `BYE`. Cuando quiera cerrar eShell, puede usar el comando `EXIT` o cualquiera de sus alias. El alias `VIRLOG` es un alias para el comando `DETECTIONS`, que se encuentra en el contexto `TOOLS LOG`. De esta manera, el comando detections está disponible en el contexto `ROOT`, lo que facilita el acceso (no tiene que escribir `TOOLS` y luego el contexto `LOG` para ejecutarlo directamente desde `ROOT`).

eShell le permite definir sus propios alias. El comando `ALIAS` está disponible en el contexto `UI ESHELL`.

Configuración de la protección por contraseña

Los ajustes de ESET Server Security pueden protegerse con contraseña. Puede establecer una contraseña utilizando la GUI o eShell, con `set ui access lock-password`. A continuación, deberá introducir esta contraseña de forma interactiva para determinados comandos (como los que cambian ajustes o modifican datos). Si va a trabajar con eShell durante un periodo más largo y no desea introducir la contraseña una y otra vez, puede hacer que eShell recuerde la contraseña con el comando `set password` (ejecútelo desde `root`). A continuación, su contraseña se introducirá automáticamente con cada comando ejecutado que requiera una contraseña. Se recuerda hasta que sale de eShell, lo que significa que deberá utilizar `set password` de nuevo cuando inicie una nueva sesión y desee que eShell recuerde su contraseña.

Guía/Ayuda

Cuando ejecute los comandos `GUIDE` o `HELP`, se mostrará una pantalla de "primera ejecución" en la que se explicará cómo utilizar eShell. Este comando solo está disponible en el contexto `ROOT` (`eShell>`).

Historial de comandos

eShell guarda el historial de los comandos ejecutados. Este historial solo incluye la sesión interactiva actual de eShell, y se borrará cuando salga de eShell. Utilice las teclas de flecha arriba y abajo del teclado para desplazarse por el historial. Una vez que haya encontrando el comando que buscaba, puede volver a ejecutarlo o modificarlo sin necesidad de escribir el comando completo desde el principio.

CLS/Borrar pantalla

El comando `CLS` se puede utilizar para borrar la pantalla; funciona igual que la ventana de símbolo del sistema de Windows u otras interfaces de línea de comandos similares.

EXIT/CLOSE/QUIT/BYE

Para cerrar o salir de eShell, puede utilizar cualquiera de estos comandos (`EXIT`, `CLOSE`, `QUIT` o `BYE`).

Comandos

En esta sección se ofrece una lista de algunos comandos básicos de eShell con su descripción.

> NOTA
> Los comandos no distinguen mayúsculas y minúsculas, por lo que el uso de unas u otras no afectará a su ejecución.

Comandos de ejemplo (del contexto ROOT):

ABOUT

Muestra información sobre el programa. Algunos de los datos que muestra:

- Nombre del producto de seguridad de ESET instalado y su número de versión.
- Detalles del sistema operativo y del hardware básicos.
- Nombre de usuario (incluido el domino), nombre completo del ordenador (nombre de dominio completo, si el servidor es miembro de un dominio) y nombre del puesto.
- Componentes instalados del producto de seguridad de ESET, incluido el número de versión de cada componente.

RUTA DE ACCESO AL CONTEXTO:

```
root
```

CONTRASEÑA

Normalmente, para ejecutar comandos protegidos con contraseña, se le pide que escriba una contraseña por motivos de seguridad. Esto se aplica a comandos como los que desactivan la protección y los que pueden afectar

a la configuración de ESET Server Security. Se le pedirá una contraseña cada vez que ejecute un comando de este tipo. Puede definir esta contraseña para no tener que introducirla una y otra vez. eShell la recordará e introducirá automáticamente cuando se ejecute un comando protegido con contraseña.

> NOTA
> La contraseña solo sirve para la sesión interactiva actual de eShell; se borrará cuando salga de eShell. La próxima vez que inicie eShell, tendrá que definir la contraseña de nuevo.

La contraseña definida también se puede usar al ejecutar archivos o scripts por lotes no firmados. Asegúrese de establecer la Directiva de ejecución de ESET en Acceso total al ejecutar archivos por lotes no firmados. A continuación se proporciona un ejemplo de archivo por lotes:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

El comando encadenado anterior define una contraseña y desactiva la protección.

> IMPORTANTE
> Se recomienda utilizar archivos por lotes firmados siempre que resulte posible. Así evitará tener contraseñas en texto sin formato en el archivo por lotes (si utiliza el método descrito anteriormente). Consulte Archivos por lotes/Creación de scripts (sección Archivos por lotes firmados) para obtener más información.

RUTA DE ACCESO AL CONTEXTO:

```
root
```

SINTAXIS:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERACIONES:

`get` muestra la contraseña

`set` establece o borra la contraseña

`restore` borra la contraseña

ARGUMENTOS:

`plain` cambia al modo de introducción de contraseña como parámetro

`password` contraseña

EJEMPLOS:

`set password plain <yourpassword>` establece una contraseña para los comandos protegidos mediante contraseña

`restore password` borra la contraseña

EJEMPLOS:

`get password` utilice este comando para comprobar si hay una contraseña configurada (solo se muestran

asteriscos "*", no la contraseña); si no se muestra ningún asterisco, significa que no hay ninguna contraseña definida

`set password plain <sucontraseña>`: utilice este comando para establecer una contraseña definida

`restore password` este comando borra la contraseña definida

STATUS

Muestra información sobre el estado de protección en tiempo real actual de ESET Server Security, y también le permite poner en pausa o reanudar la protección (de forma similar a lo que hace la GUI).

RUTA DE ACCESO AL CONTEXTO:

```
computer real-time
```

SINTAXIS:

```
[get] status

set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]

restore status
```

OPERACIONES:

`get` devuelve el estado o la configuración actual

`set` define el valor o el estado

`restore` restaura la configuración, el objeto o el archivo predeterminado

ARGUMENTOS:

`enabled` Habilitar protección/función

`disabled` Deshabilitar protección/función

`10m` Deshabilitar durante 10 minutos

`30m` Deshabilitar durante 30 minutos

`1h` Deshabilitar durante 1 hora

`4h` Deshabilitar durante 4 horas

`temporary` Deshabilitar hasta el reinicio

> NOTA
> No es posible desactivar todas las funciones de protección con un solo comando. Puede administrar las funciones de protección y los módulos uno por uno mediante el comando `status`. Cada función de protección o módulo tiene su propio comando `status`.

Lista de funciones con comando `status`:

Función	Contexto y comando
Exclusiones automáticas	`COMPUTER AUTO-EXCLUSIONS STATUS`
Sistema de prevención de intrusiones del host (HIPS)	`COMPUTER HIPS STATUS`
Protección del sistema de archivos en tiempo real	`COMPUTER REAL-TIME STATUS`
Control del dispositivo	`DEVICE STATUS`
Protección contra botnets	`NETWORK ADVANCED STATUS-BOTNET`
Protección contra los ataques de red (IDS)	`NETWORK ADVANCED STATUS-IDS`
Aislamiento de la red	`NETWORK ADVANCED STATUS-ISOLATION`
Clúster de ESET	`TOOLS CLUSTER STATUS`
Registro de diagnóstico	`TOOLS DIAGNOSTICS STATUS`
Modo de presentación	`TOOLS PRESENTATION STATUS`
Protección Anti-Phishing	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Protección del cliente de correo electrónico	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Protección del acceso a la Web	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Este es un alias del comando `DETECTIONS`. Es útil cuando se necesita ver información sobre las amenazas detectadas.

WARNLOG

Este es un alias del comando `EVENTS`. Es útil cuando se necesita ver información sobre diversos eventos.

Archivos por lotes/Creación de scripts

Puede usar eShell como una potente herramienta de creación de scripts para la automatización de tareas. Si desea usar un archivo por lotes con eShell, créelo con eShell y especifique comandos en él.

> EJEMPLO
> `eshell get computer real-time status`

También puede encadenar comandos, tarea a veces necesaria. Por ejemplo, si quiere obtener un tipo de tarea programada determinado, introduzca lo siguiente:

```
eshell select scheduler task 4 "&" get scheduler action
```

La selección del elemento (tarea número 4 en este caso) normalmente se aplica solo a una instancia actualmente en ejecución de eShell. Si ejecutara estos dos comandos sucesivamente, el segundo comando fallaría y presentaría el error "No hay ninguna tarea seleccionada o la tarea seleccionada ya no existe".

Por motivos de seguridad, la política de ejecución está ajustada como **Scripts limitados** de forma predeterminada. Esta configuración le permite usar eShell como herramienta de supervisión, pero no le permitirá efectuar cambios en la configuración de ESET Server Security mediante la ejecución de un script. Si intenta ejecutar un script con comandos que pueden afectar a la seguridad, como aquellos que desactivan la protección, aparecerá el mensaje **Acceso denegado**. Le recomendamos que utilice archivos por lotes firmados para ejecutar comandos que realicen cambios en la configuración.

Para cambiar la configuración utilizando un solo comando introducido manualmente en el símbolo del sistema de

Windows, deberá otorgar acceso completo a eShell (no se recomienda). Para conceder acceso total, utilice el comando `ui eshell shell-execution-policy` en el modo interactivo de eShell o a través de la interfaz gráfica de usuario en la opción **Configuración avanzada** (**F5**)> **Interfaz de usuario** > Shell de ESET.

Archivos por lotes firmados

eShell le permite proteger archivos por lotes comunes (*.bat) por medio de una firma. Los scripts se firman con la misma contraseña que se usa para la protección de la configuración. Para poder firmar un script debe activar primero la protección de la configuración. Puede hacerlo a través de la interfaz gráfica de usuario o desde eShell con el comando `set ui access lock-password`. Cuando la contraseña de protección de la configuración esté configurada, puede empezar a firmar archivos por lotes.

> NOTA
> Si cambia la contraseña de protección de la configuración, tendrá que firmar todos los scripts de nuevo; de lo contrario, los scripts no se ejecutarán correctamente tras el cambio de contraseña. La contraseña introducida al firmar el script debe coincidir con la contraseña de protección de la configuración del sistema de destino.

Para firmar un archivo por lotes, ejecute `sign <script.bat>` desde el contexto raíz de eShell, donde *script.bat* es la ruta de acceso al script que desea firmar. Introduzca y confirme la contraseña que se utilizará para la firma. Esta contraseña debe coincidir con la contraseña de protección de la configuración. La firma se coloca al final del archivo por lotes en forma de comentario. Si este script ya se ha firmado, la firma se sustituirá por una nueva.

> NOTA
> Si se modifica un archivo por lotes previamente firmado, tendrá que firmarlo de nuevo.

Para ejecutar un archivo por lotes firmado desde el símbolo del sistema de Windows o como tarea programada, utilice el siguiente comando:

```
eshell run <script.bat>
```

Donde script.bat es la ruta de acceso al archivo por lotes.

> EJEMPLO
> `eshell run d:\myeshellscript.bat`

ESET SysInspector

ESET SysInspector es una aplicación que inspecciona a fondo el ordenador, recopila información detallada sobre los componentes del sistema (como los controladores y aplicaciones instalados, las conexiones de red o las entradas importantes del registro) y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa de un comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de código malicioso.

Haga clic en **Crear** y escriba un breve **Comentario** que describa el registro que se creará. Espere hasta que el registro de ESET SysInspector se haya generado (el estado aparecerá como Creado). La creación del registro podría llevar cierto tiempo, en función de la configuración de hardware y de los datos del sistema.

En la ventana de ESET SysInspector se muestra la siguiente información de los registros creados:

- **Fecha y hora**: fecha y hora de creación del registro.
- **Comentario**: breve comentario.
- **Usuario**: nombre del usuario que creó el registro.
- **Estado**: estado de la creación del registro.

Están disponibles las siguientes acciones:

- **Mostrar**: abre el registro creado. También puede hacer clic con el botón derecho del ratón sobre un registro y seleccionar Mostrar en el menú contextual.
- **Comparar**: compara dos registros existentes.
- **Crear**: crea un archivo de registro nuevo. Escriba un comentario breve en el que se describa el registro que se va a crear y haga clic en Crear. Espere a que la creación del archivo de registro de ESET SysInspector finalice (se mostrará el estado Creado).
- **Eliminar**: elimina de la lista los registros seleccionados.

Al hacer clic con el botón derecho del ratón en uno o varios de los registros seleccionados se mostrarán las siguientes opciones del menú contextual:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).
- **Comparar**: compara dos registros existentes.
- **Crear:** crea un archivo de registro nuevo. Escriba un comentario breve en el que se describa el registro que se va a crear y haga clic en **Crear**. Espere a que la creación del archivo de registro de ESET SysInspector finalice (se mostrará el **estado** Creado).
- **Eliminar**: elimina de la lista los registros seleccionados.
- **Eliminar todos**: elimina todos los registros.
- **Exportar**: exporta el registro a un archivo .xml o .xml comprimido.

ESET SysRescue Live

ESET SysRescue Live es una utilidad gratuita que le permite crear una unidad de CD/DVD o USB de rescate de inicio. Puede iniciar un ordenador infectado desde su soporte de rescate y, a continuación, realizar un análisis en busca de malware y desinfectar archivos infectados.

La principal ventaja de ESET SysRescue Live es que la solución ESET Security se puede ejecutar de forma independiente del sistema operativo host, pero tiene acceso directo al disco y a todo el sistema de archivos. Gracias a esto, es posible eliminar las amenazas que normalmente no se podrían suprimir como, por ejemplo, cuando el sistema operativo se está ejecutando.

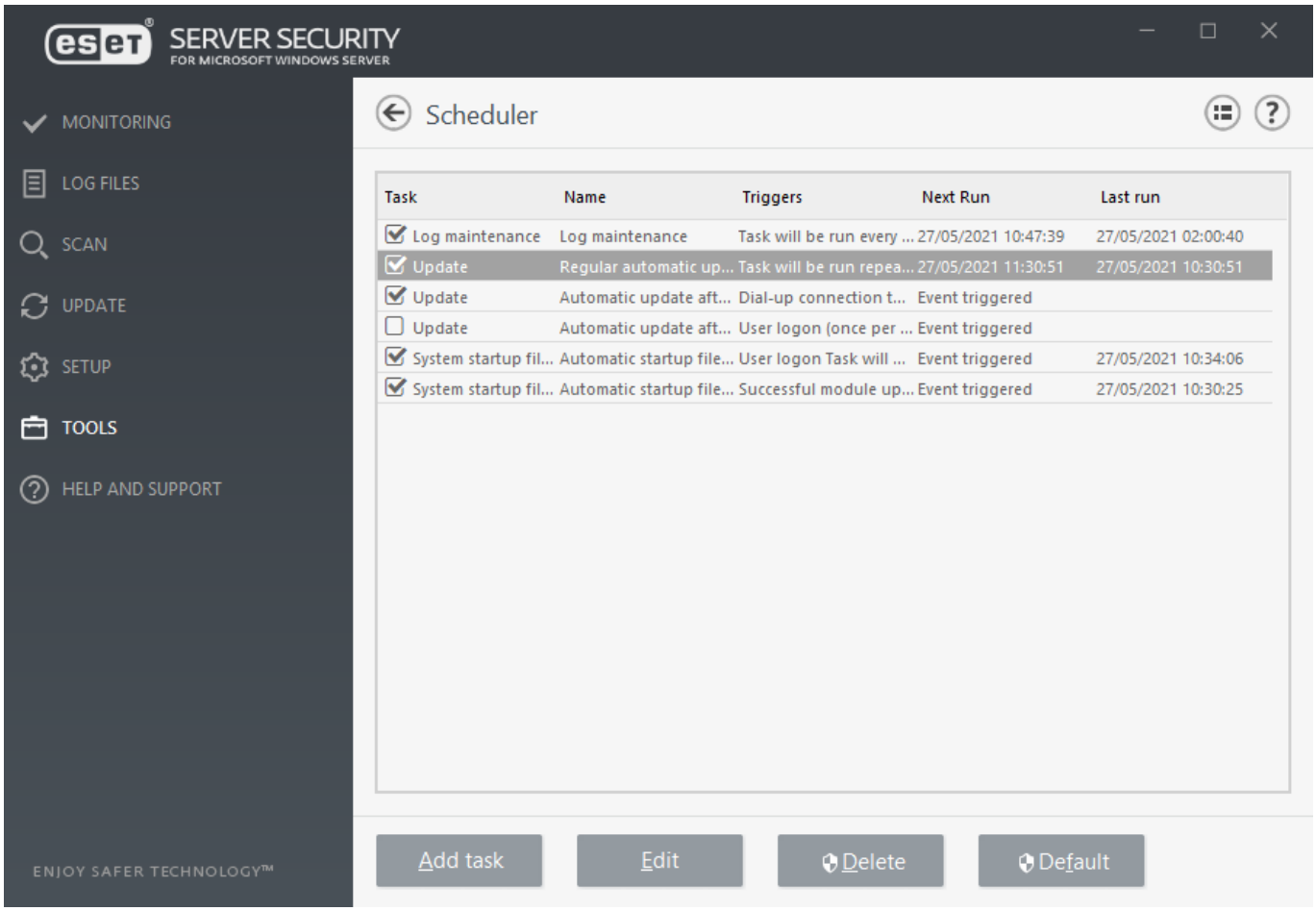
Planificador de tareas

La opción Tareas programadas gestiona e inicia las tareas programadas según los parámetros definidos. Puede ver una lista de todas las tareas programadas en forma de una tabla en la que se muestran sus parámetros, como el tipo y nombre de la tarea, la hora de ejecución y la última vez que se ejecutó. También puede hacer clic en Agregar tarea para crear nuevas tareas programadas. Para editar la configuración de una tarea programada, haga clic en el botón **Editar**. Para recuperar la configuración predeterminada de la lista de tareas programadas, haga clic en **Predeterminado** y, a continuación, en **Restaurar predeterminados**. Los cambios realizados se perderán y esta acción no se puede deshacer.

Hay una serie de tareas predeterminadas predefinidas:

- Mantenimiento de registros
- Actualización automática de rutina (utilice esta tarea para frecuencia de actualización)
- Actualización automática tras conexión de acceso telefónico
- Actualización automática tras el inicio de sesión del usuario
- Verificación automática de los archivos de inicio (tras inicio de sesión del usuario)
- Verificación automática de los archivos de inicio (tras actualización de los módulos)

NOTA
Marque las casillas de verificación pertinentes para activar o desactivar las tareas.



Para realizar las siguientes acciones, haga clic con el botón derecho del ratón en una tarea:

Mostrar detalles de la tarea	Muestra información detallada sobre una tarea programada cuando hace doble clic con el botón derecho en la tarea programada.
Ejecutar ahora	Ejecuta una tarea seleccionada de Tareas programadas y realiza la tarea inmediatamente.
Agregar...	Abre un asistente que le ayudará a crear una nueva tarea de Tareas programadas.
Editar...	Cambia la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario).
Eliminar	Elimina una tarea existente.

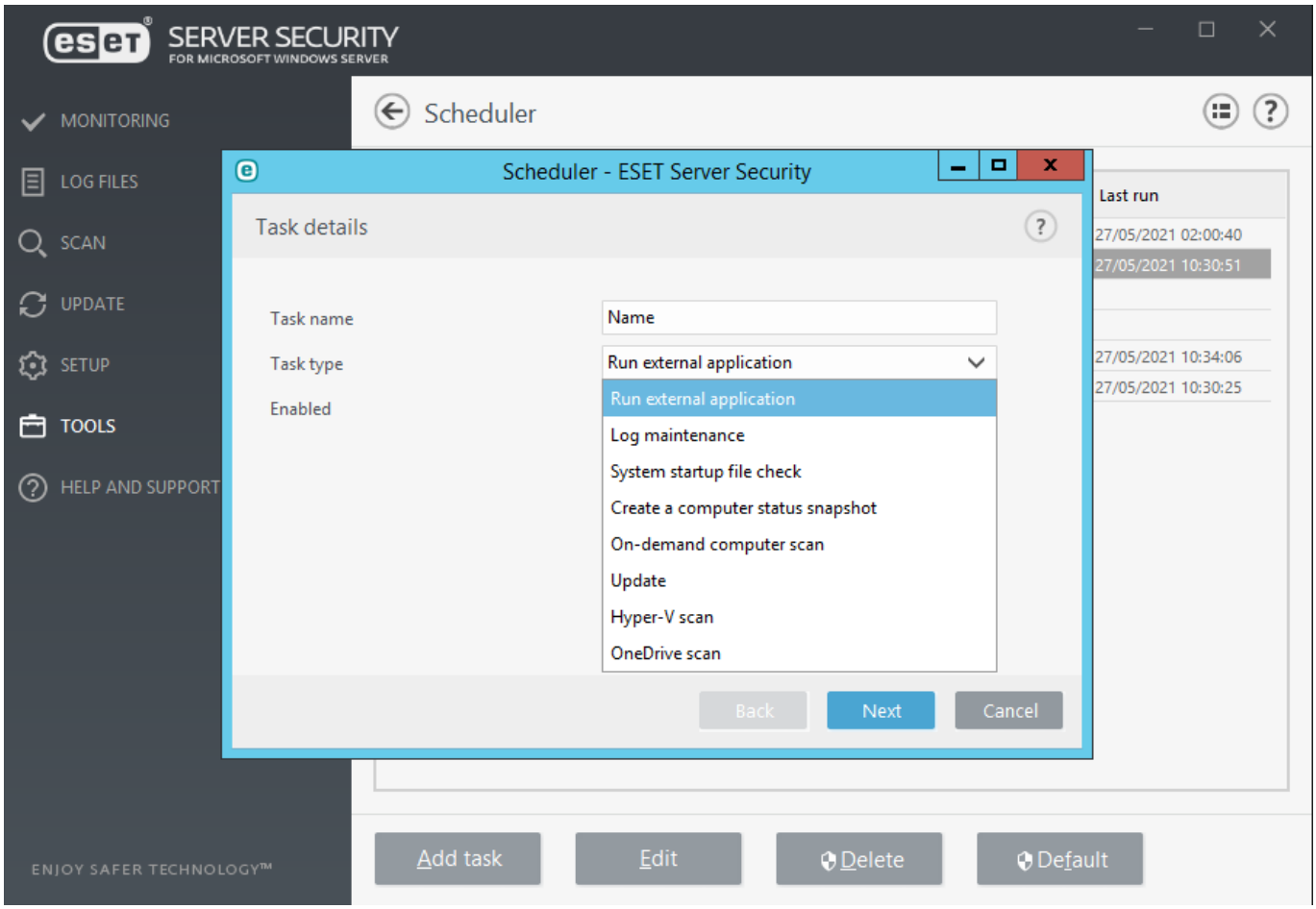
Tareas programadas: Agregar tarea

Para crear una nueva tarea programada:

1.Haga clic en **Agregar tarea**.

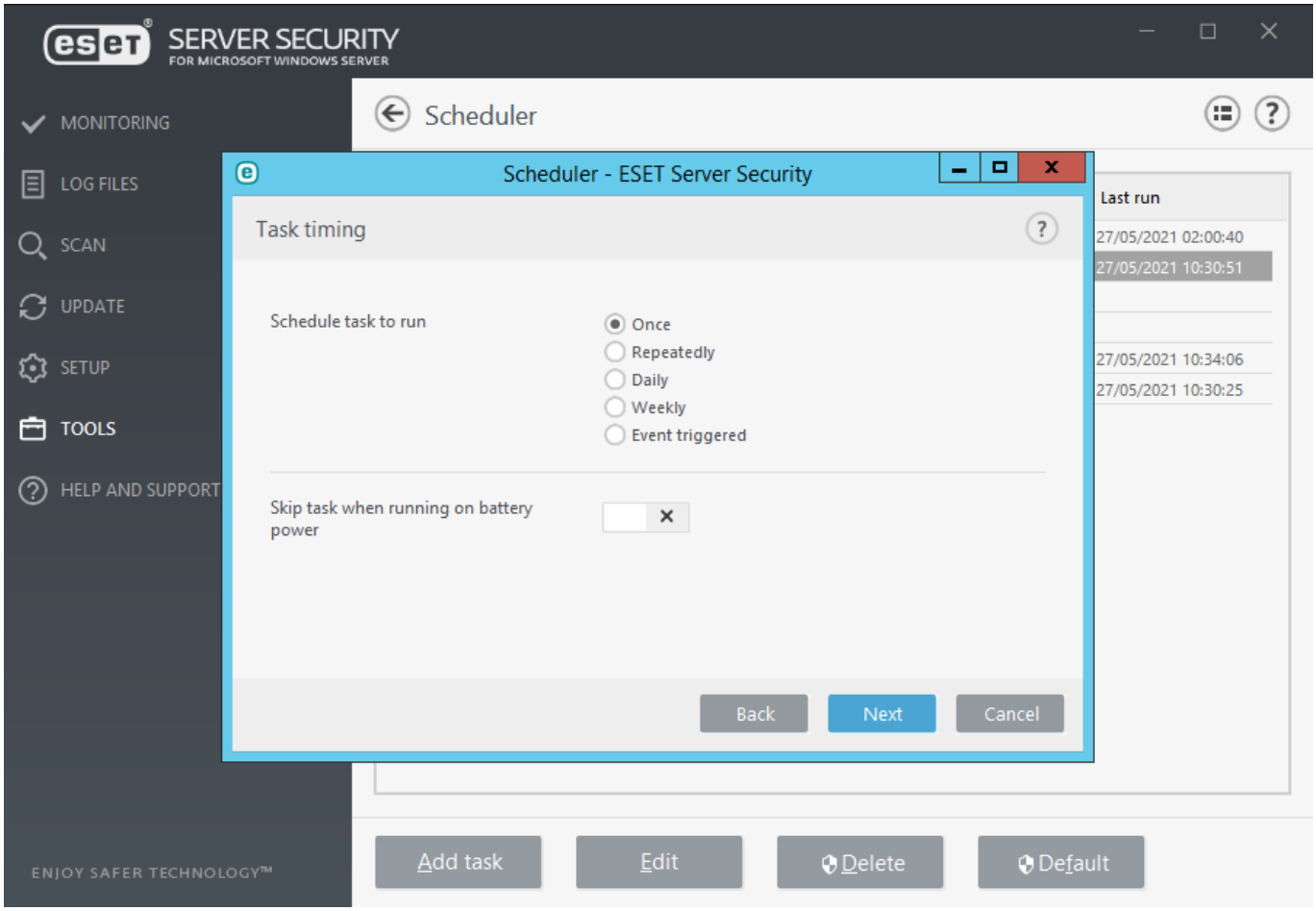
2.Escriba el **Nombre de la tarea** y configure la tarea programada personalizada.

3. Tipo de tarea: seleccione el **Tipo de tarea** correspondiente en el menú desplegable.

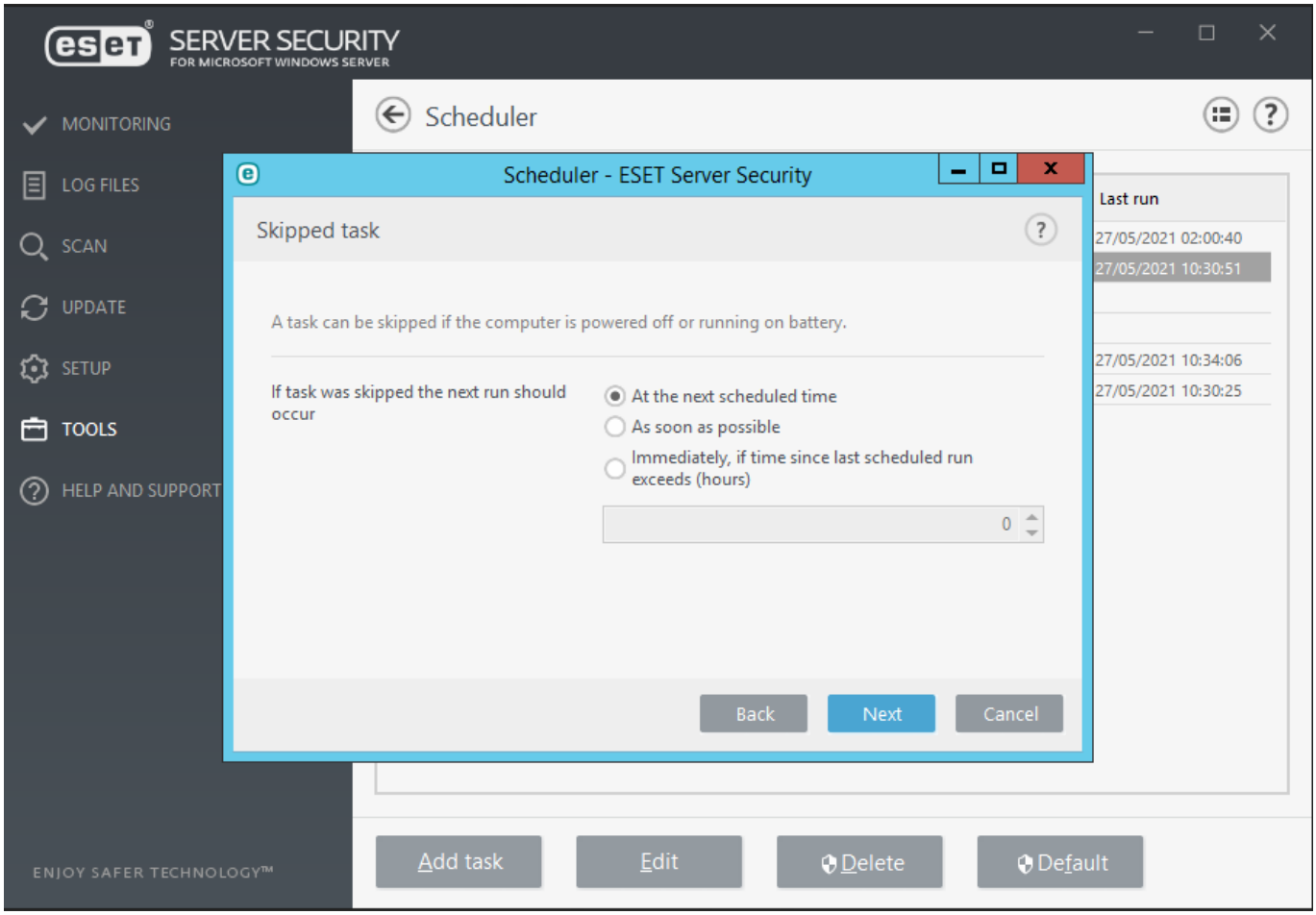


NOTA
Para desactivar una tarea, haga clic en la barra deslizante situada junto a **Activado**. Para activar la tarea más tarde, utilice la casilla de la vista de Tareas programadas.

4. Repetición de la tarea: seleccione una de las opciones para definir cuándo desea que la tarea se ejecute. En función de su elección, se le pedirá que elija una hora, una fecha, un intervalo o un suceso concretos.



5. Tarea omitida: si la tarea no se pudo ejecutar en el momento predefinido, puede especificar cuándo se ejecutará.



6. Ejecutar aplicación: si la tarea está programada para ejecutar una aplicación externa, elija un archivo ejecutable en el árbol de directorios.

7.Si necesita realizar cambios, haga clic en **Atrás** para volver a los pasos anteriores y modificar los parámetros.

8.Haga clic en **Finalizar** para crear la tarea o aplicar cambios.

La nueva tarea programada aparecerá en la vista de Tareas programadas.

Tipo de tarea

El asistente de configuración es distinto para cada **Tipo de tarea** de una tarea programada. Introduzca el **Nombre de la tarea** y seleccione el **Tipo de tarea** que desee en el menú desplegable:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos cuya ejecución se permite al encender el sistema o iniciar sesión en él.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector, recopila información detallada sobre los componentes del sistema (por ejemplo controladores,

aplicaciones) y evalúa el nivel de riesgo de cada componente.

- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.

- **Actualizar**: programa una tarea de actualización para actualizar el motor de detección y los módulos del programa.

- **Análisis Hyper-V**: programa un análisis de los discos virtuales de Hyper-V.

- **Análisis de OneDrive**: programa un análisis de los archivos almacenados en OneDrive.

Para desactivar una tarea después de crearla, haga clic en el conmutador situado junto a **Activado**. Para activar la tarea más tarde, haga clic en la casilla de la vista de Tareas programadas. Haga clic en **Siguiente** para ir al siguiente paso.

Repetición de la tarea

Seleccione una de las siguientes opciones de repetición:

- **Una vez**: la tarea se realizará solo una vez, en la fecha y a la hora especificadas. Para ejecutar la tarea solo una vez en un momento concreto, especifique la fecha y hora de inicio para una instancia en **Ejecución de la tarea**.

- **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado (en minutos). Especifique la hora a la que se ejecutará la tarea todos los días en **Ejecución de la tarea**.

- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.

- **Semanalmente**: la tarea se ejecutará una o varias veces a la semana, en los días y a la hora seleccionados. Para ejecutar la tarea reiteradamente solo días de la semana concretos, comenzando el día y la hora especificados, especifique la hora de inicio en Horario de ejecución de la tarea. Seleccione el día o los días de la semana en los que se debe ejecutar la tarea.

- Desencadenada por un suceso - La tarea se ejecutará tras un suceso especificado.

Si activa **No ejecutar la tarea si está funcionando con batería**, la tarea no se iniciará si el ordenador está funcionando con batería en el momento en que está programado el inicio de la tarea. Por ejemplo, para ordenadores que funcionan con un SAI.

Desencadenada por un suceso

Cuando se programa una tarea desencadenada por un suceso, se puede especificar el intervalo mínimo entre dos finalizaciones de la tarea.

La tarea se puede desencadenar cuando se produzca cualquiera de los sucesos siguientes:

- **Cada vez que se inicie el ordenador.**

- **La primera vez que se inicie el ordenador en el día**

- **Conexión por módem a Internet/VPN**

- **Actualización de módulo correcta**
- **Actualización de producto correcta**
- **Inicio de sesión del usuario**: la tarea se implementará cuando el usuario inicie sesión en el sistema. Si inicia sesión en su ordenador varias veces al día, seleccione 24 horas para realizar la tarea solo en el primer inicio de sesión del día y, después, al día siguiente.
- **Detección de amenazas**

Ejecutar aplicación

En esta tarea se programa la ejecución de una aplicación externa.

- **Archivo ejecutable**: seleccione un archivo ejecutable en el árbol de directorios y haga clic en la opción **Examinar (...)** o introduzca la ruta manualmente.
- **Carpeta de trabajo**: defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **archivo ejecutable** seleccionado se crearán en este directorio.
- **Parámetros**: parámetros de la línea de comandos de la aplicación (opcional).

Tarea omitida

Si la tarea no se pudo ejecutar en el momento predefinido, puede especificar cuándo se ejecutará:

- **En la siguiente hora programada**: la tarea se ejecutará a la hora especificada (por ejemplo, cuando hayan transcurrido 24 horas).
- **Lo antes posible**: la tarea se ejecutará lo antes posible, cuando las acciones que impidan la ejecución de la tarea ya no sean válidas.
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado - Tiempo desde la última ejecución (horas)**: cuando haya seleccionado esta opción, la tarea se repetirá siempre tras el período de tiempo especificado (en horas).

Resumen general de tareas programadas

Este cuadro de diálogo muestra información detallada sobre una tarea programada cuando hace doble clic en la tarea en la vista **Planificador de tareas** o hace clic con el botón derecho en la tarea programada y selecciona **Mostrar detalles de la tarea**.

Enviar muestras para su análisis

El cuadro de diálogo de envío de muestras le permite enviar un archivo o un sitio a ESET para que lo analice. Si encuentra un archivo en su ordenador que se comporta de manera sospechosa o un sitio sospechoso en Internet, envíelo al laboratorio de virus de ESET para su análisis. Si resulta que el archivo es una aplicación o un sitio web malicioso, la detección se agregará a una actualización futura.

Para enviar el archivo por correo electrónico, comprima los archivos con un programa como WinRAR o WinZip, proteja el archivo comprimido con la contraseña *infected* y envíelo a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el archivo (por ejemplo, el sitio web del que lo descargó).

Antes de enviar una muestra a ESET, asegúrese de que cumple uno o ambos de los siguientes criterios:

- El archivo o sitio web no se detecta en absoluto.
- El archivo o sitio web se detecta como una amenaza, pero no lo es.

Si no se cumple al menos uno de los anteriores requisitos, no recibirá ninguna respuesta hasta que se proporcione información adicional.

Seleccione la descripción en el menú desplegable **Motivo de envío de la muestra** que mejor se ajuste a su mensaje:

- Archivo sospechoso
- Sitio web sospechoso (sitio web que está infectado por código malicioso)
- Archivo de falso positivo (archivo que se detecta como infectado, pero no lo está)
- Sitio de falso positivo
- Otros

Archivo/Sitio

La ruta al archivo o sitio web que quiere enviar.

Correo electrónico de contacto

Esta dirección de correo electrónico de contacto se envía a ESET junto con los archivos sospechosos, y se puede utilizar para ponernos en contacto con usted en caso de que sea necesario enviar más información para poder realizar el análisis. No es obligatorio introducir una dirección de correo electrónico de contacto. No obtendrá ninguna respuesta de ESET a menos que sea necesario enviar información adicional, ya que cada día nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.

Enviar de forma anónima

Utilice la casilla junto a **Enviar de forma anónima** para enviar un archivo o sitio web sospechoso sin introducir su dirección de correo electrónico.

Archivo sospechoso

Signos y síntomas observados de la infección por código malicioso

Introduzca una descripción del comportamiento del archivo sospechoso que ha observado en el ordenador.

Origen del archivo (dirección URL o proveedor)

Especifique el origen del archivo (fuente) y cómo llegó a él.

Notas e información adicional

Aquí puede especificar más información o una descripción que le ayude con el proceso de identificación del archivo sospechoso.

> NOTA
> El primer parámetro (**Signos y síntomas observados de la infección por código malicioso**) es necesario; la información adicional que proporcione será de gran utilidad para nuestros laboratorios en el proceso de identificación de muestras.

Sitio web sospechoso

Seleccione una de las opciones siguientes en el menú desplegable **Problema del sitio**:

Número de objetos infectados

Sitio web que contiene virus u otro malware distribuido por diversos métodos.

Phishing

Su objetivo suele ser acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre este tipo de ataque en el glosario.

Estafa

Sitio web fraudulento o de estafas.

Otros

Utilice esta opción si ninguna de las opciones anteriores se aplica al sitio que va a enviar.

Notas e información adicional

Puede especificar más información o una descripción que ayude a analizar el sitio web sospechoso.

Archivo de falso positivo

Le rogamos que nos envíe los archivos que se detectan como infección, pero no están infectados, para mejorar nuestro motor de detección y ayudar a proteger a otras personas. Los falsos positivos (FP) pueden generarse cuando un patrón de un archivo coincide con el mismo patrón que contiene un motor de detección.

> NOTA
> **los** tres primeros parámetros son necesarios para identificar las aplicaciones legítimas y distinguirlas del código malicioso. La información adicional que proporcione será de gran ayuda para los procesos de identificación y procesamiento de muestras en nuestros laboratorios.

Nombre y versión de la aplicación

Título y versión del programa (por ejemplo, número, alias o nombre en código).

Origen del archivo (dirección URL o proveedor)

Especifique un origen del archivo (fuente) y anote cómo llegó a este archivo.

Objetivo de la aplicación

La descripción general de la aplicación, tipo de aplicación (por ejemplo, navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional

Aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

Sitio de falso positivo

Le rogamos que nos envíe los sitios que se detectan como sitios infectados, de estafas o de phishing, pero no lo son. Los falsos positivos (FP) pueden generarse cuando un patrón de un sitio coincide con el mismo patrón que contiene un motor de detección. Proporcione este sitio web para mejorar nuestro motor de detección y ayudar a proteger a otras personas.

Notas e información adicional

Aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

Otros

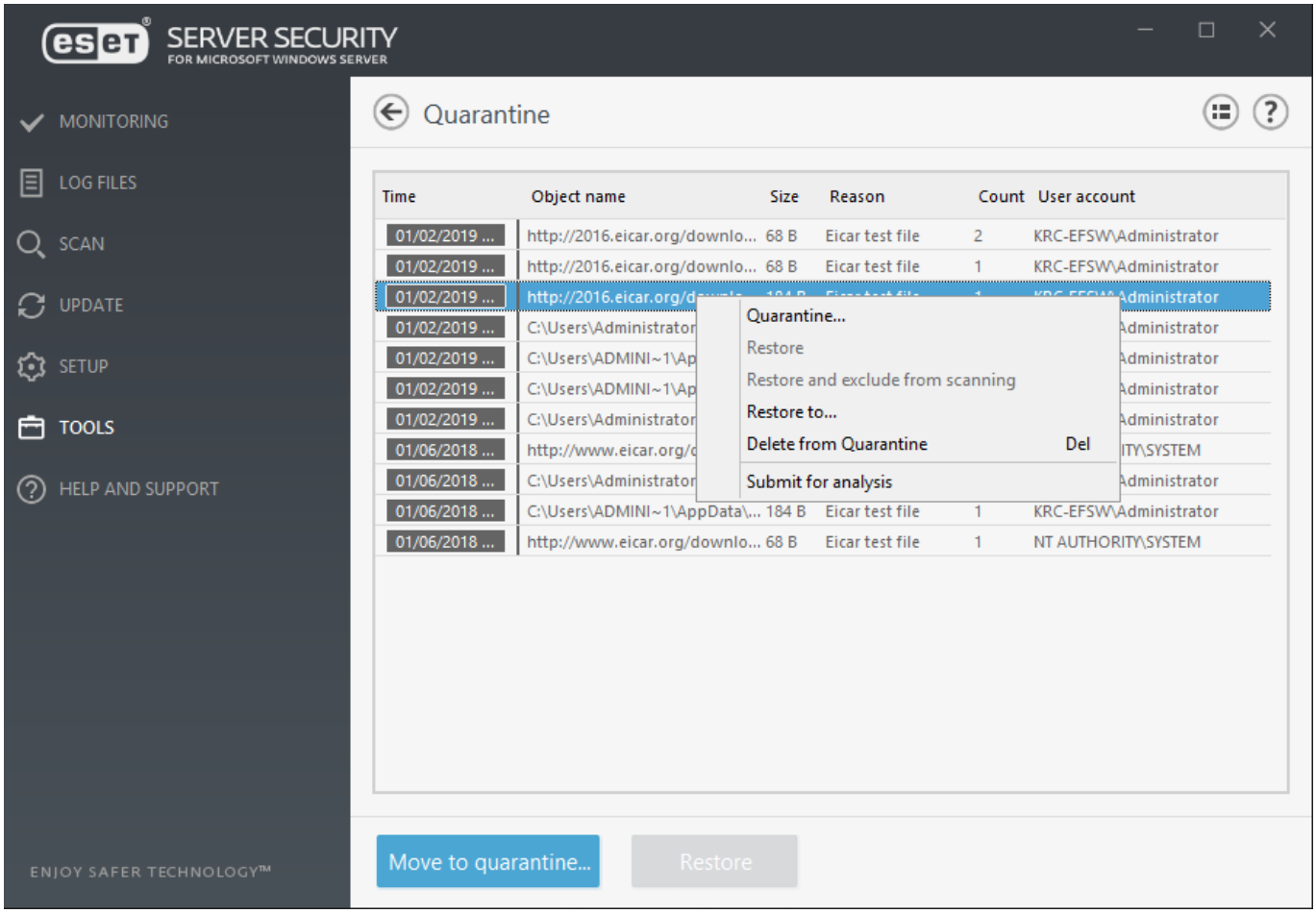
Utilice este formulario si el archivo no se puede categorizar como un **Archivo sospechoso** o un **Falso positivo**.

Motivo de envío del archivo

Introduzca una descripción detallada y el motivo por el que envía el archivo.

Cuarentena

La función principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro o aconsejable eliminarlos o si los detecta incorrectamente ESET Server Security. Puede poner en cuarentena cualquier archivo. Esto es recomendable si un archivo tiene un comportamiento sospechoso, pero el análisis de malware no lo detecta. Los archivos en cuarentena pueden enviarse al laboratorio de virus de ESET para que los analicen.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, por ejemplo) y el número de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias amenazas).

Si los objetos del mensaje de correo electrónico se colocan en la cuarentena de archivos, se mostrará información en forma de ruta al buzón de correo, la carpeta o el nombre del archivo.

Copiar archivos en cuarentena

ESET Server Security pone los archivos eliminados en cuarentena automáticamente (si no ha desactivado esta opción en la ventana de alerta). Para poner en cuarentena cualquier archivo sospechoso de forma manual, haga clic en el botón **Poner en cuarentena**. Los archivos que se pongan en cuarentena se quitarán de su ubicación original. El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Para ello, utilice la función **Restaurar**, disponible en el menú contextual que se abre al hacer clic con el botón derecho del ratón en la ventana Cuarentena. Si el archivo está marcado como aplicación potencialmente indeseable, también estará disponible la opción **Restaurar y excluir del análisis**. El menú contextual también ofrece la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

NOTA
Si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha determinado incorrectamente que un archivo está infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, se ha copiado a cuarentena, envíe el archivo al laboratorio de virus de ESET. Para enviar un archivo de cuarentena, haga clic con el botón derecho del ratón en el archivo y seleccione Enviar para su análisis en el menú contextual.

Eliminación de la cuarentena

Haga clic con el botón derecho del ratón en un elemento y seleccione **Eliminar de la cuarentena**, o seleccione los elementos que desee y pulse la tecla **Suprimir** del teclado.

Configuración del análisis de OneDrive

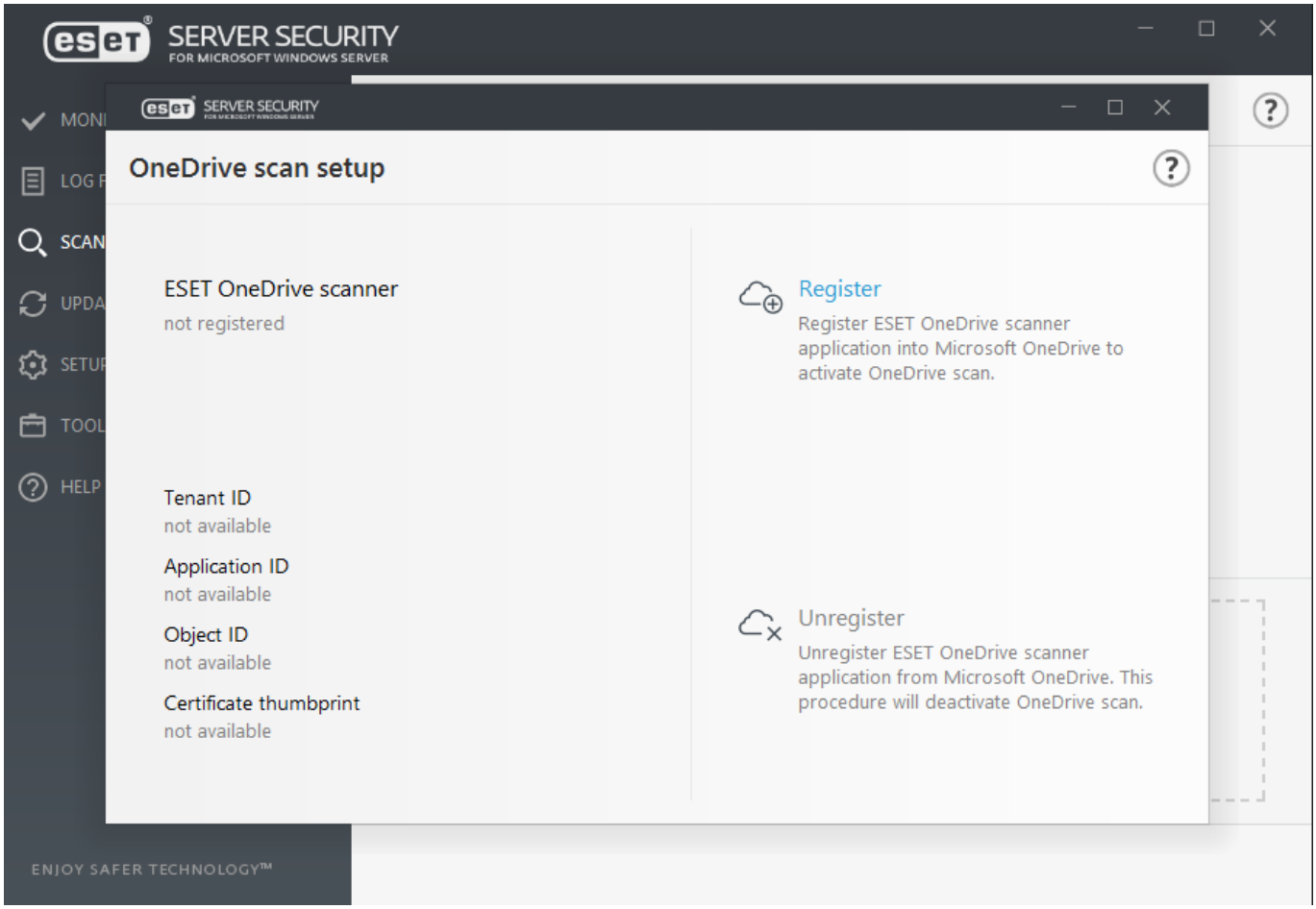
Abrir ESET Server Security
Haga clic en Configuración > Servidor > Configuración del análisis de OneDrive 

Esta función le permite analizar archivos almacenados en el almacenamiento en la nube Microsoft OneDrive para la Empresa. El análisis de ESET Server Security OneDrive solo procesa carpetas y archivos, no analiza otros tipos de datos, tales como correos electrónicos, archivos de SharePoint, contactos o calendarios.

Vínculos rápidos:

Registrar ESET OneDrive Scanner
Anular el registro de ESET OneDrive Scanner

Para comenzar a utilizar el análisis de ESET Server Security OneDrive, debe registrar la aplicación ESET OneDrive Scanner en Microsoft OneDrive/Microsoft Office 365/Microsoft Azure. La página de configuración de análisis de OneDrive le muestra el estado del registro, si ya se hubiera registrado, y los detalles del registro (ID de inquilino, ID de la aplicación, ID del objeto y huella digital del certificado). Puede registrar o anular el registro de ESET OneDrive Scanner.



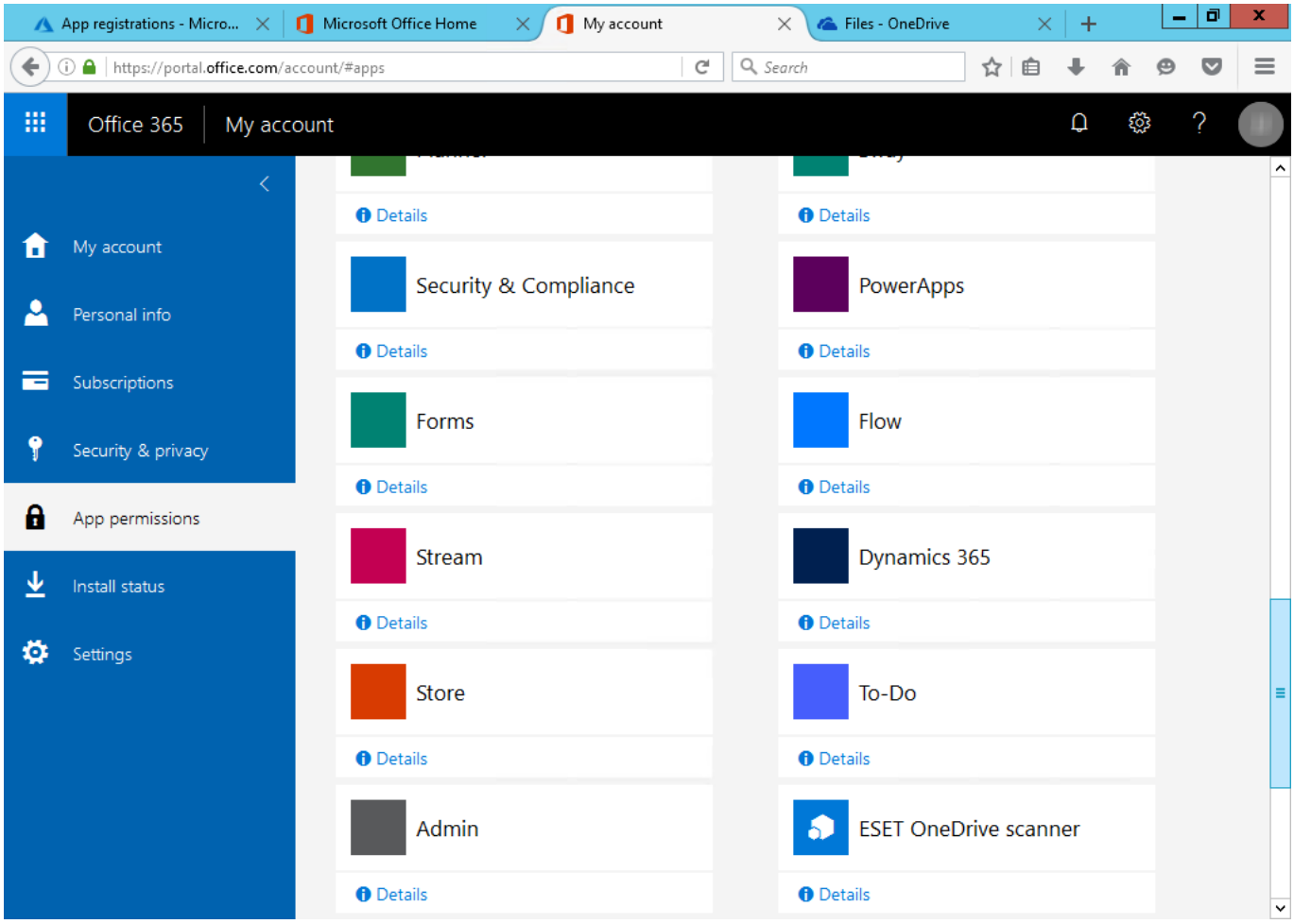
Después de realizar un registro correcto, el análisis de OneDrive estará disponible en el menú Análisis y mostrará una lista de usuarios con sus estructuras de carpetas y archivos que pueden seleccionarse para su análisis. El análisis de ESET Server Security OneDrive puede analizar archivos almacenados por usuarios en OneDrive para la Empresa.

NOTA
El análisis de ESET Server Security OneDrive descarga archivos desde el almacenamiento en la nube OneDrive para la Empresa y realiza un análisis a nivel local. Una vez realizado el análisis, los archivos descargados se eliminan. La descarga de una gran cantidad de datos desde OneDrive afectará al trafico de red.

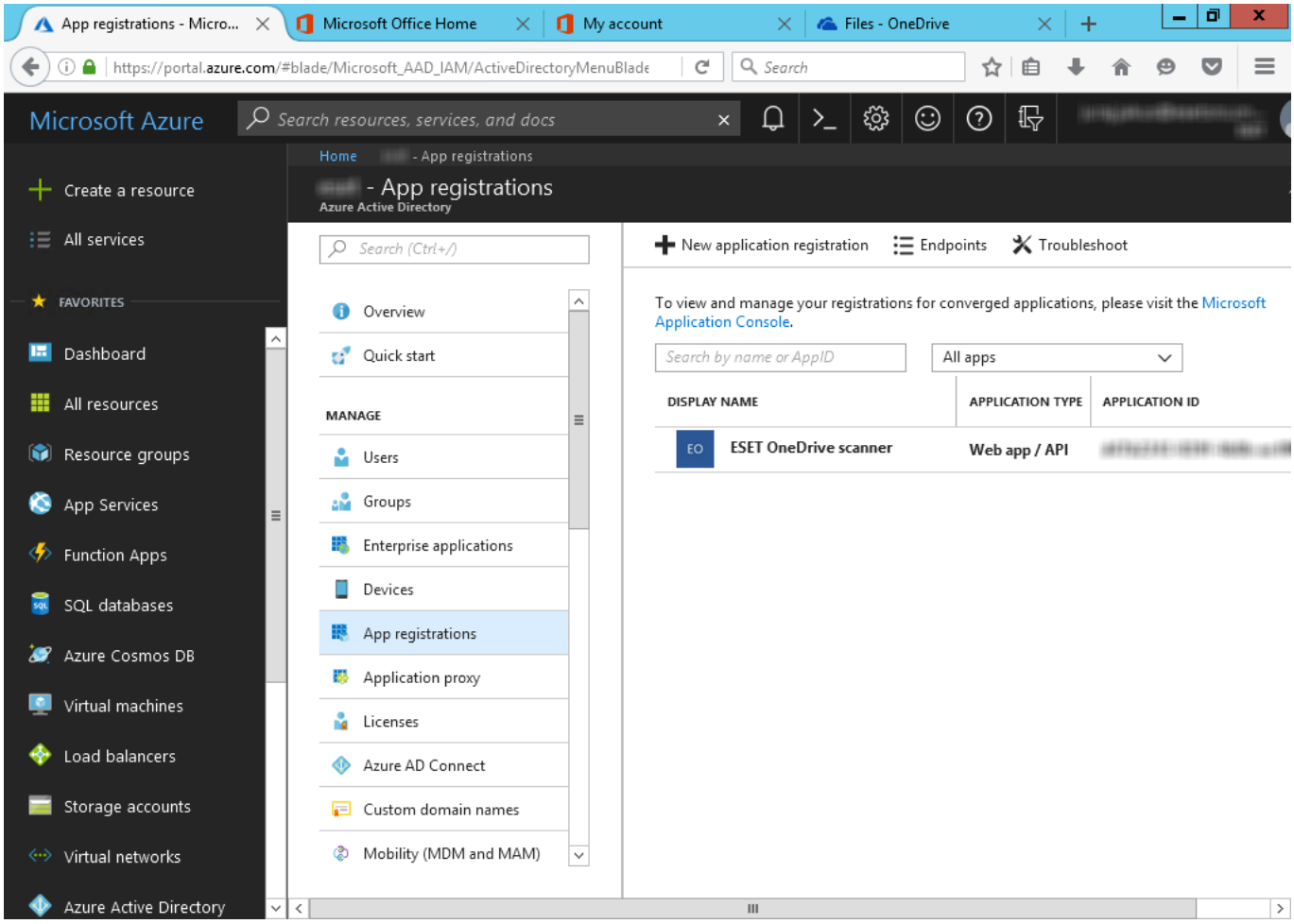
NOTA
Registrarse de nuevo con otra cuenta: si desea registrar ESET Server Security OneDrive Scanner con una cuenta nueva de Microsoft OneDrive para la Empresa u Office 365, debe Anular el registro de ESET OneDrive Scanner que utilizaba con su cuenta anterior y realizar el registro con la nueva cuenta de administrador de Microsoft OneDrive para la Empresa u Office 365.

Podrá ver que ESET OneDrive Scanner se ha registrado como aplicación en Office 365 y Azure:

Portal de Office 365: haga clic en **Permisos de aplicación** en la página Mi cuenta y aparecerá la aplicación ESET OneDrive Scanner en la lista.



Azure: vaya a **Azure Active Directory** > **Registros de aplicaciones**, haga clic en **Ver todas las aplicaciones** y aparecerá la aplicación ESET OneDrive Scanner en la lista. Haga clic en la aplicación para ver los detalles.

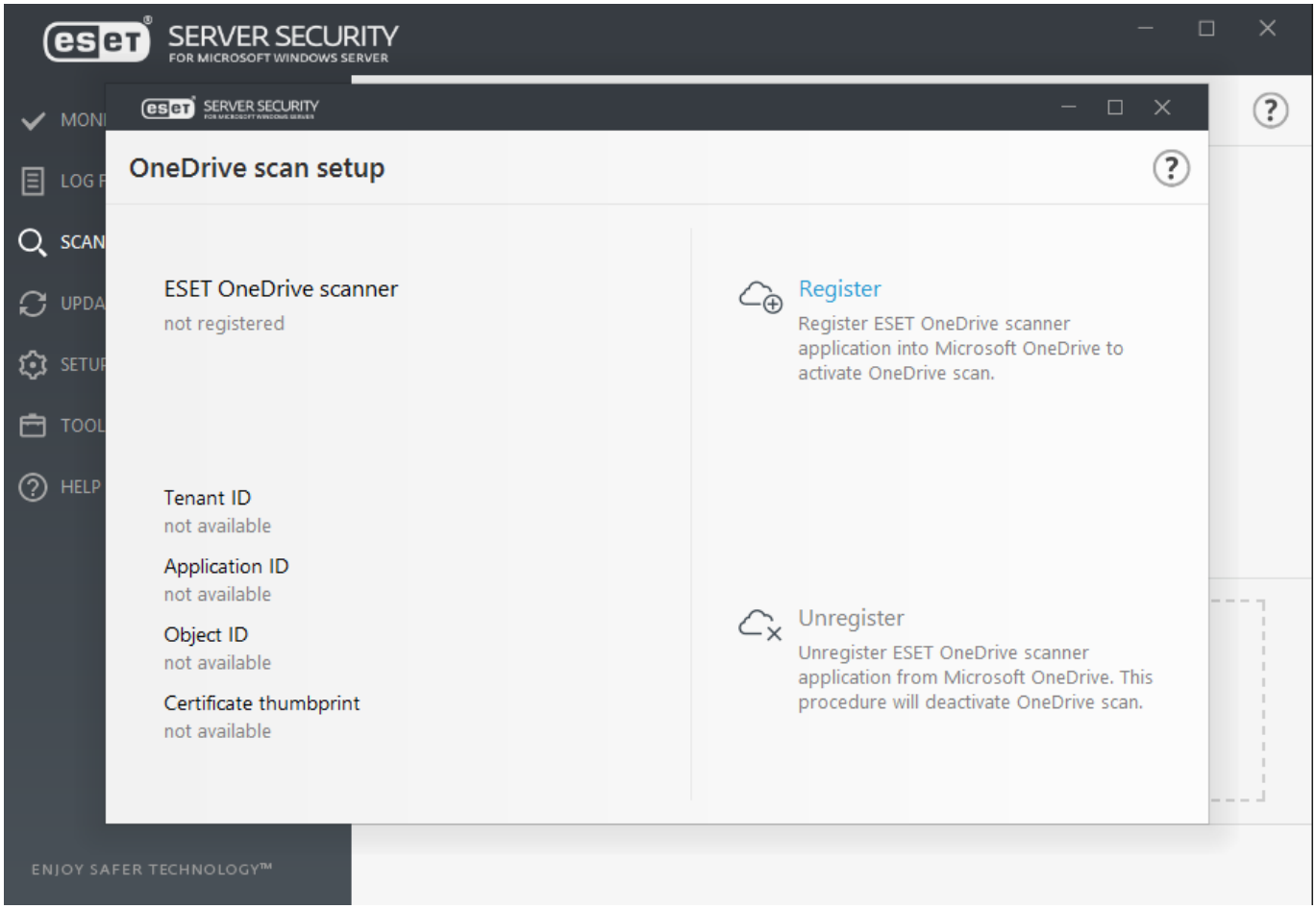


Registrar ESET OneDrive Scanner

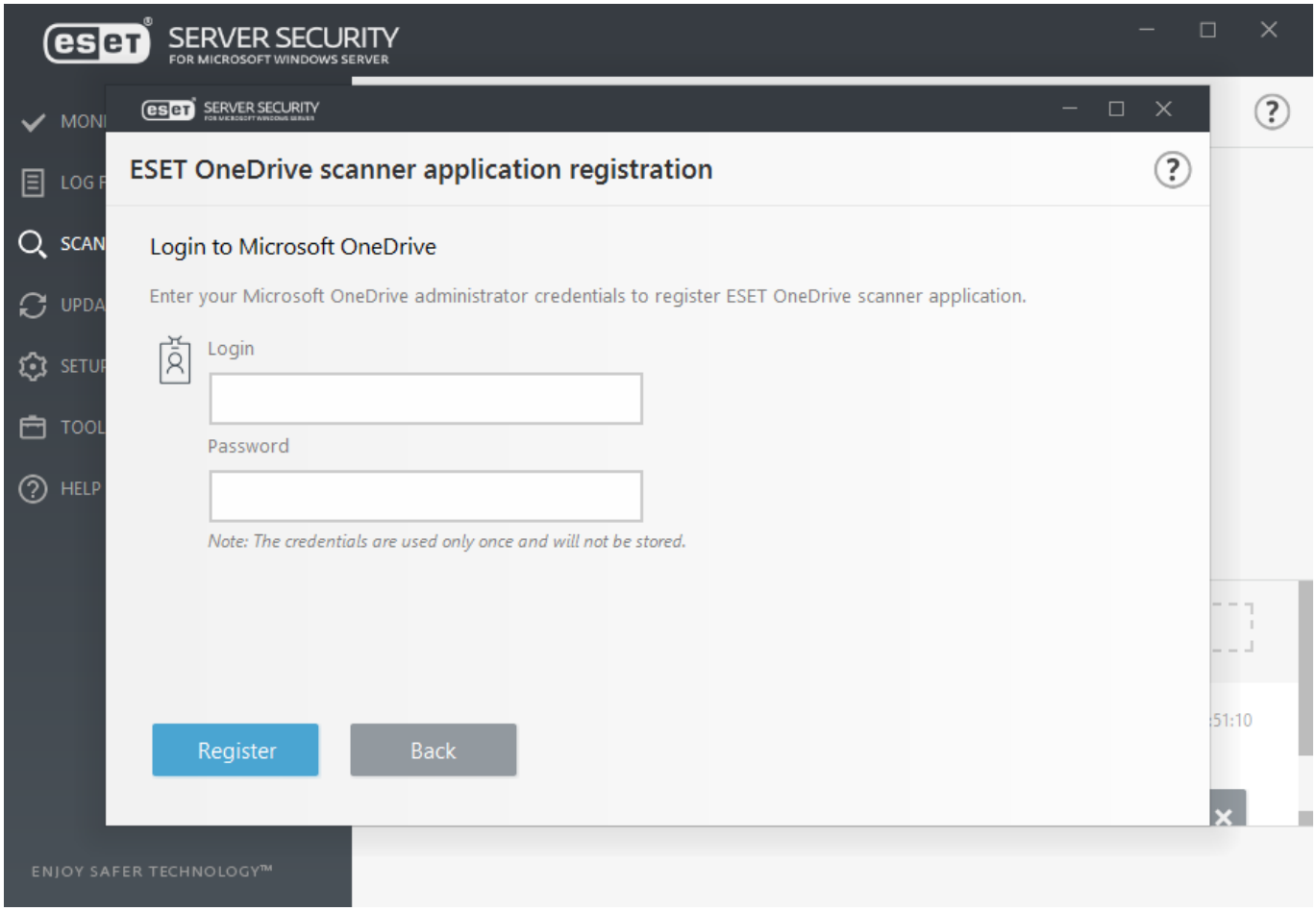
Abrir ESET Server Security
Haga clic en Configuración > Servidor > Configuración del análisis de OneDrive > Registrar. 

A continuación se indica el proceso de registro de la aplicación ESET OneDrive Scanner en Microsoft OneDrive/Office 365/Azure:

- Haga clic en **Registrar** para comenzar el registro de ESET OneDrive Scanner; se abrirá un asistente de registro.

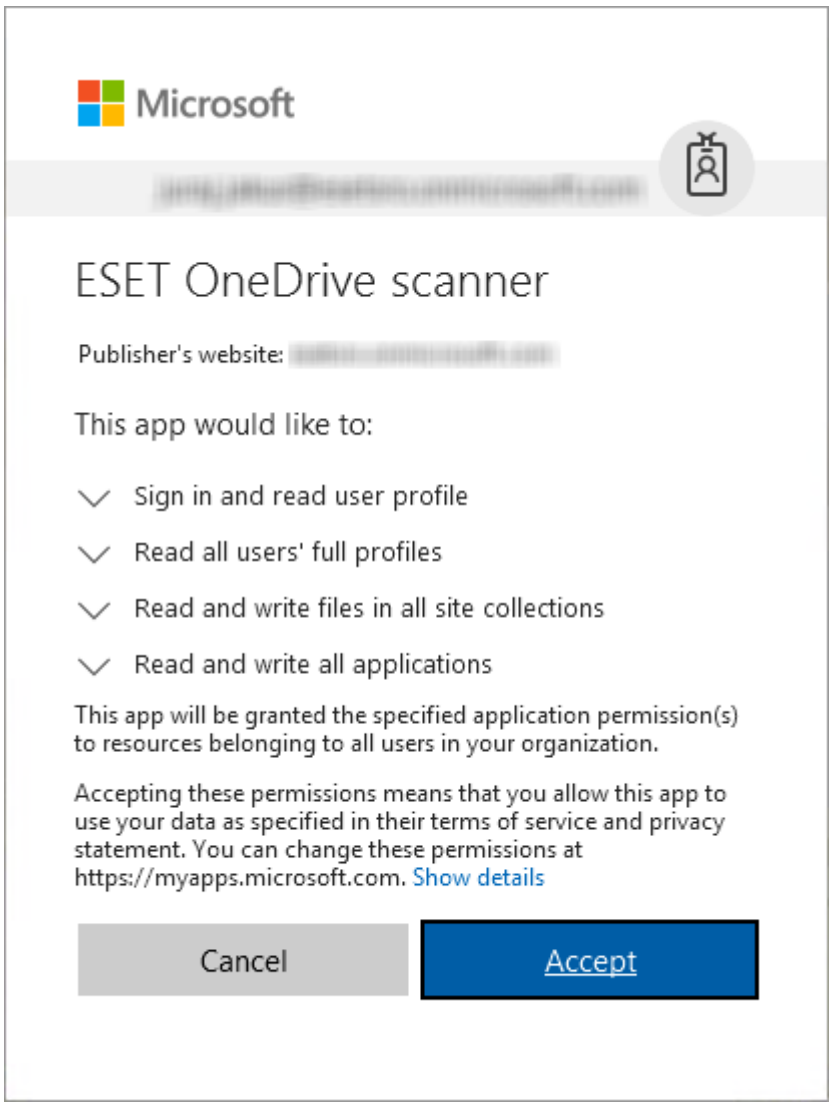


• Introduzca las credenciales de la cuenta de administrador de Microsoft OneDrive/Office 365. Espere hasta que se complete el registro de la aplicación en Microsoft OneDrive.



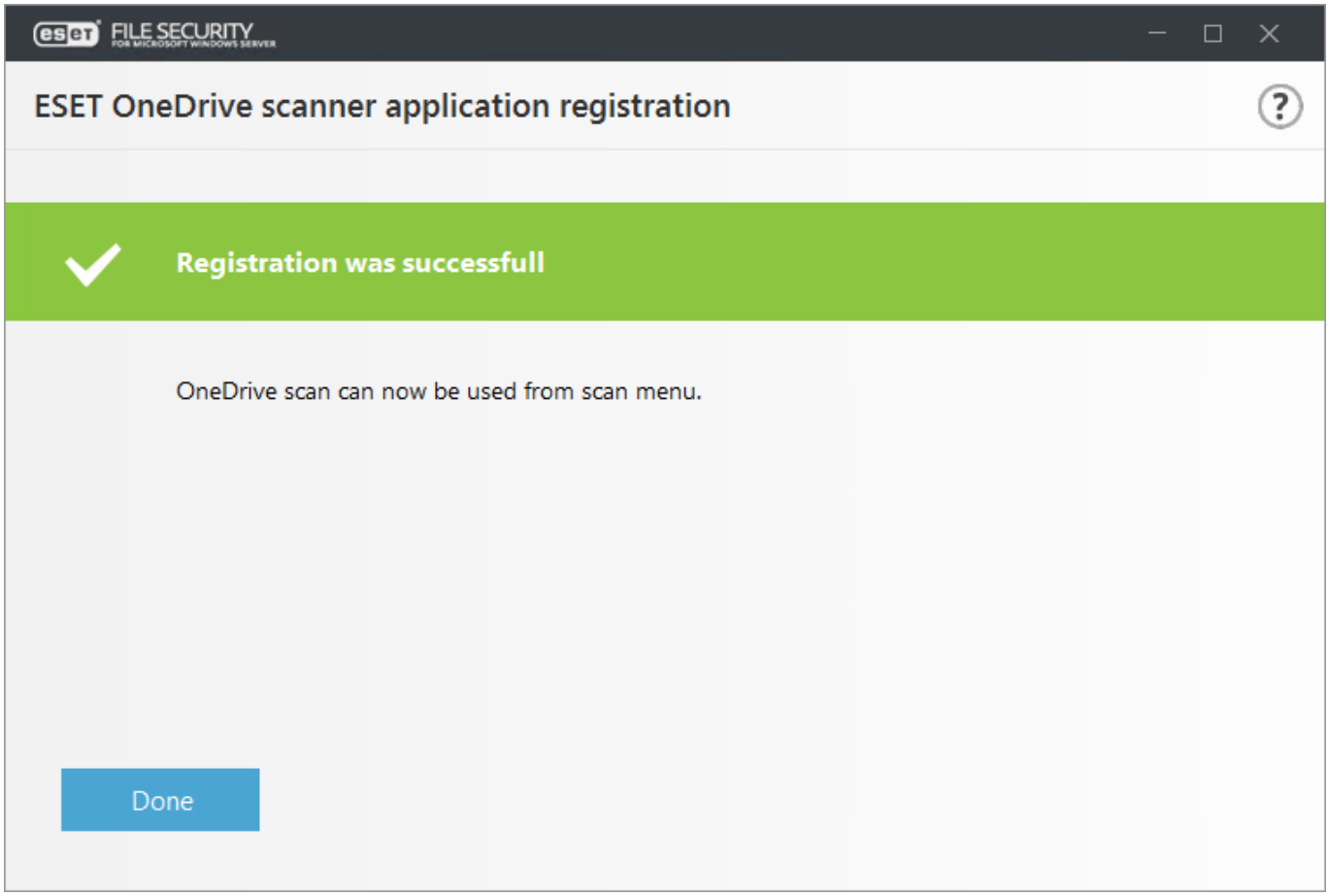
• Se abrirá un navegador web con la página **Elegir una cuenta** de Microsoft. Haga clic en la cuenta que esté utilizando, si estuviera disponible, o introduzca las credenciales de la cuenta de administrador de Microsoft OneDrive/Office 365 y haga clic en **Iniciar sesión**.

• La aplicación ESET OneDrive Scanner necesita los cuatro tipos de permisos indicados en el mensaje de aceptación. Haga clic en **Aceptar** para permitir que ESET Server Security OneDrive Scanner acceda a los datos ubicados en el almacenamiento en la nube OneDrive.



• Haga clic en **Continuar** si el navegador web le solicita enviar esta información (solo se envía al host local para permitir que ESET Server Security sepa que el registro de la aplicación se ha realizado correctamente).

• Una vez que cierre el navegador web, el asistente de registro de ESET OneDrive Scanner muestra el mensaje de que el registro se ha realizado correctamente; haga clic en **Listo**.



NOTA
El proceso de registro de ESET OneDrive Scanner puede diferir en determinadas circunstancias, en función de si ha iniciado sesión o no en alguno de los portales de Microsoft (OneDrive, Office 365, Azure, etc.) con las credenciales de la cuenta de administrador. Siga las instrucciones que aparecen en pantalla y los mensajes de la ventana del asistente de registro.

Si aparece alguno de los siguientes mensajes de error durante el registro de ESET OneDrive Scanner, consulte los detalles del mensaje de error para encontrar una sugerencia de solución:

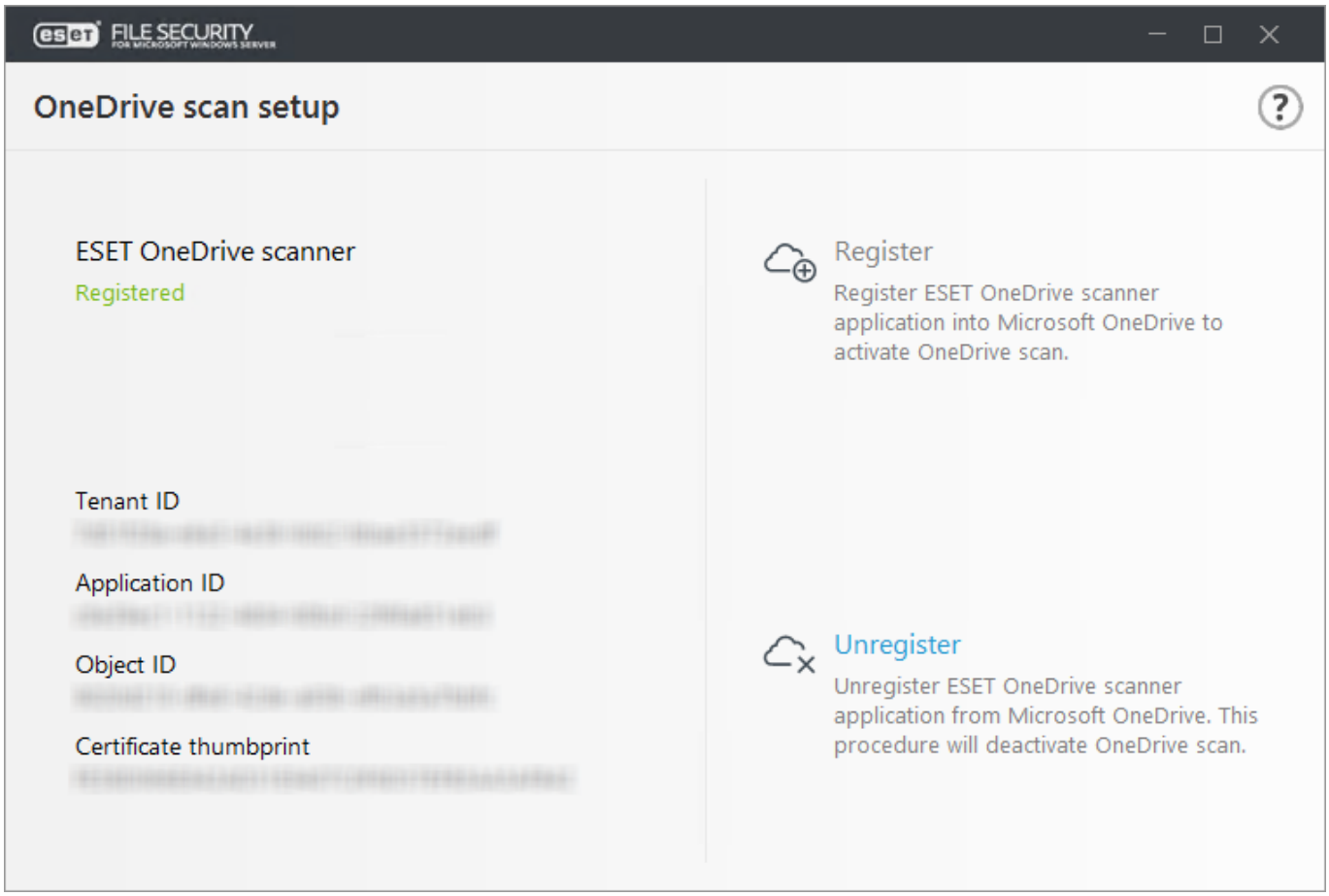
Mensaje de error	Detalles del mensaje de error
Se ha producido un error inesperado.	Podría haber un problema con ESET Server Security. Pruebe a ejecutar ESET OneDrive Scanner de nuevo más adelante. Si el problema persiste, póngase en contacto con el soporte técnico de ESET.
No ha sido posible conectar con Microsoft OneDrive.	Compruebe su conexión a Internet o a la red y vuelva a ejecutar ESET OneDrive Scanner.
Se ha recibido un error inesperado de Microsoft OneDrive.	Se ha devuelto un error HTTP 4xx sin respuesta en el mensaje de error. Si el problema persiste, póngase en contacto con el soporte técnico de ESET.
Se ha recibido el siguiente error de Microsoft OneDrive.	El servidor de Microsoft OneDrive ha devuelto un error con un código/nombre de error específico, haga clic en **Mostrar error**.
Se ha excedido el tiempo de espera de la tarea de configuración.	La tarea de configuración de registro de ESET OneDrive Scanner tarda mucho tiempo. Pruebe a ejecutar el registro de ESET OneDrive Scanner de nuevo más adelante.
Se ha cancelado la tarea de configuración.	Ha cancelado una tarea de registro en curso. Ejecute el registro de ESET OneDrive Scanner de nuevo si desea completar el registro.
Otra tarea de configuración ya está en curso.	Ya hay una tarea de registro en curso. Espere hasta que se complete el primer proceso de registro.

Anular el registro de ESET OneDrive Scanner

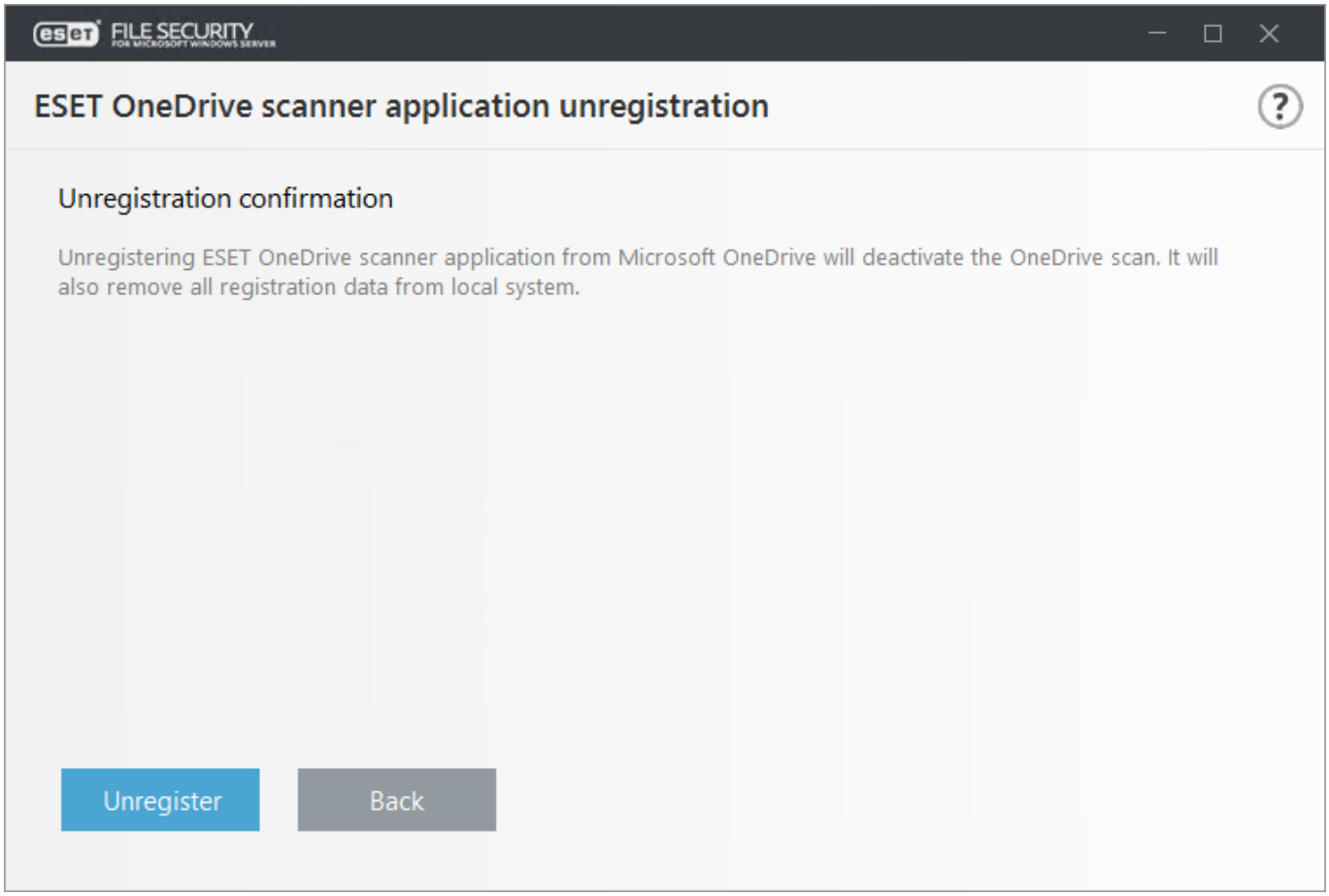
Abrir ESET Server Security
Haga clic en Configuración > Servidor > Configuración del análisis de OneDrive > Anular registro

El proceso de anulación de registro le permite eliminar el certificado y la aplicación ESET OneDrive Scanner de Microsoft OneDrive/Office 365/Azure. Este proceso también elimina las dependencias locales y hace que la opción Registrar esté disponible de nuevo.

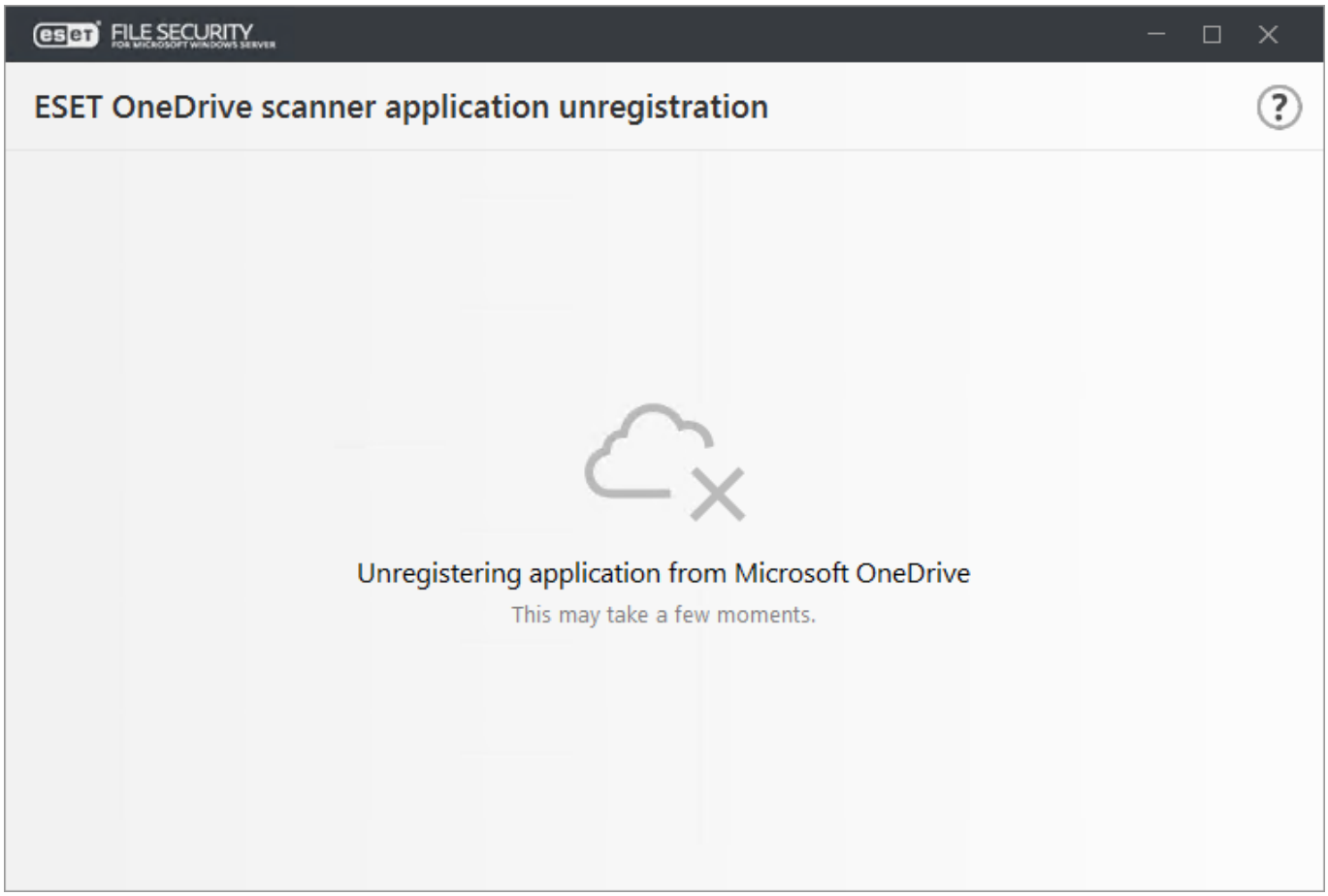
- Haga clic en **Anular registro** para comenzar el proceso de anulación/eliminación de registro de ESET OneDrive Scanner; se abrirá un asistente de anulación de registro.



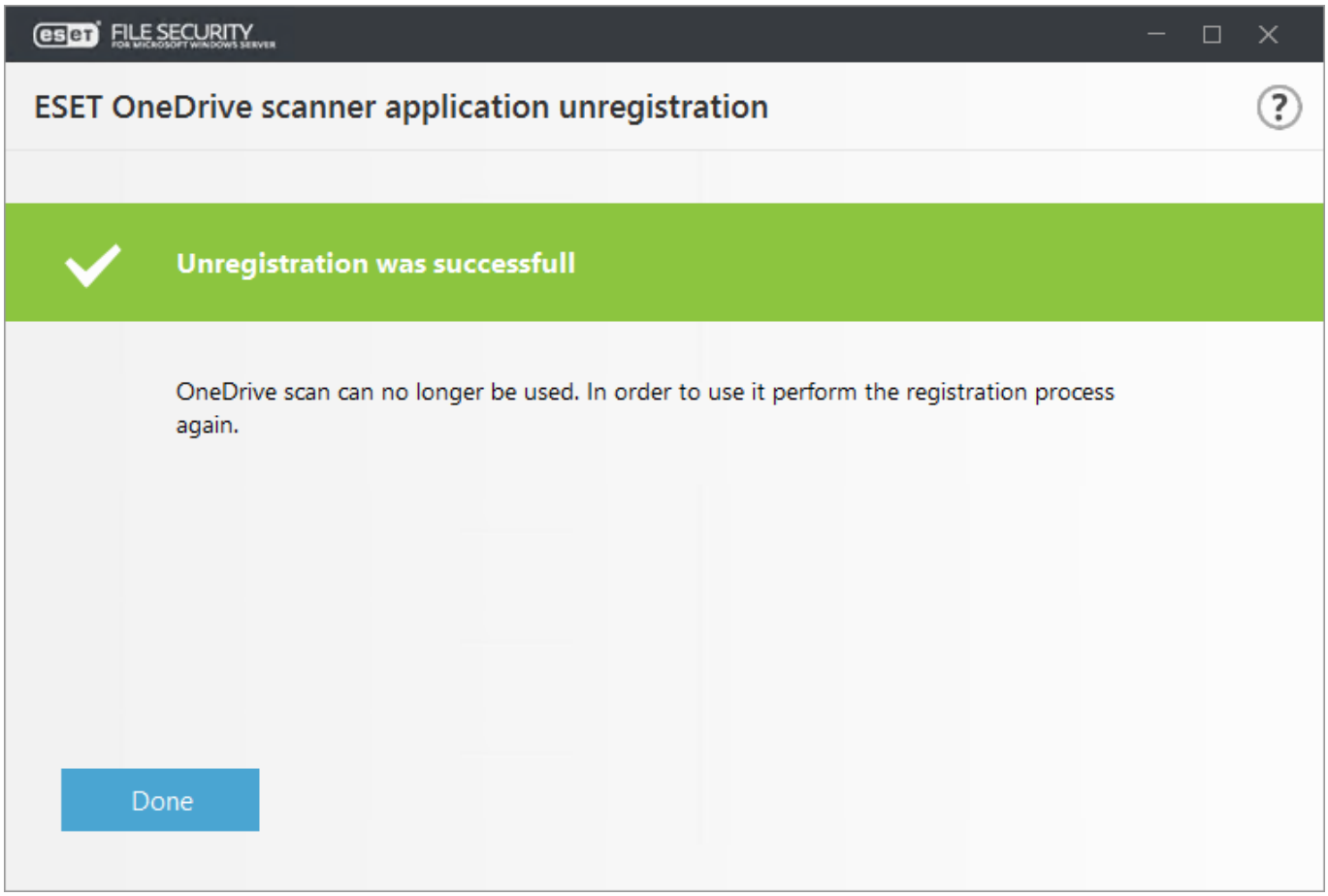
- Haga clic en **Anular registro** para confirmar que desea eliminar ESET OneDrive Scanner.



- Espere a que se complete el proceso de anulación de registro de Microsoft OneDrive.



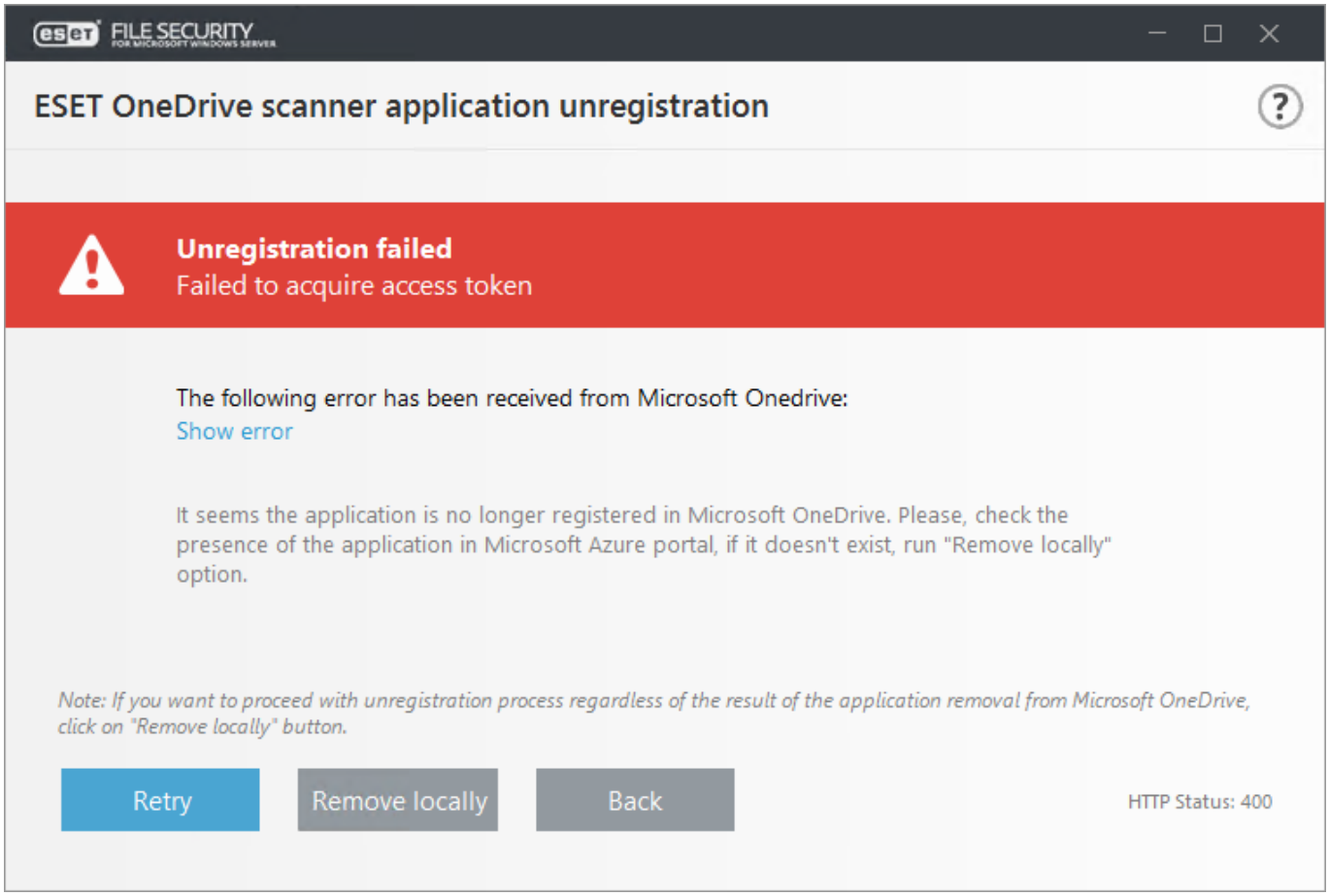
• Si el proceso de anulación de registro se realiza correctamente, el asistente de anulación de registro mostrará el correspondiente mensaje.



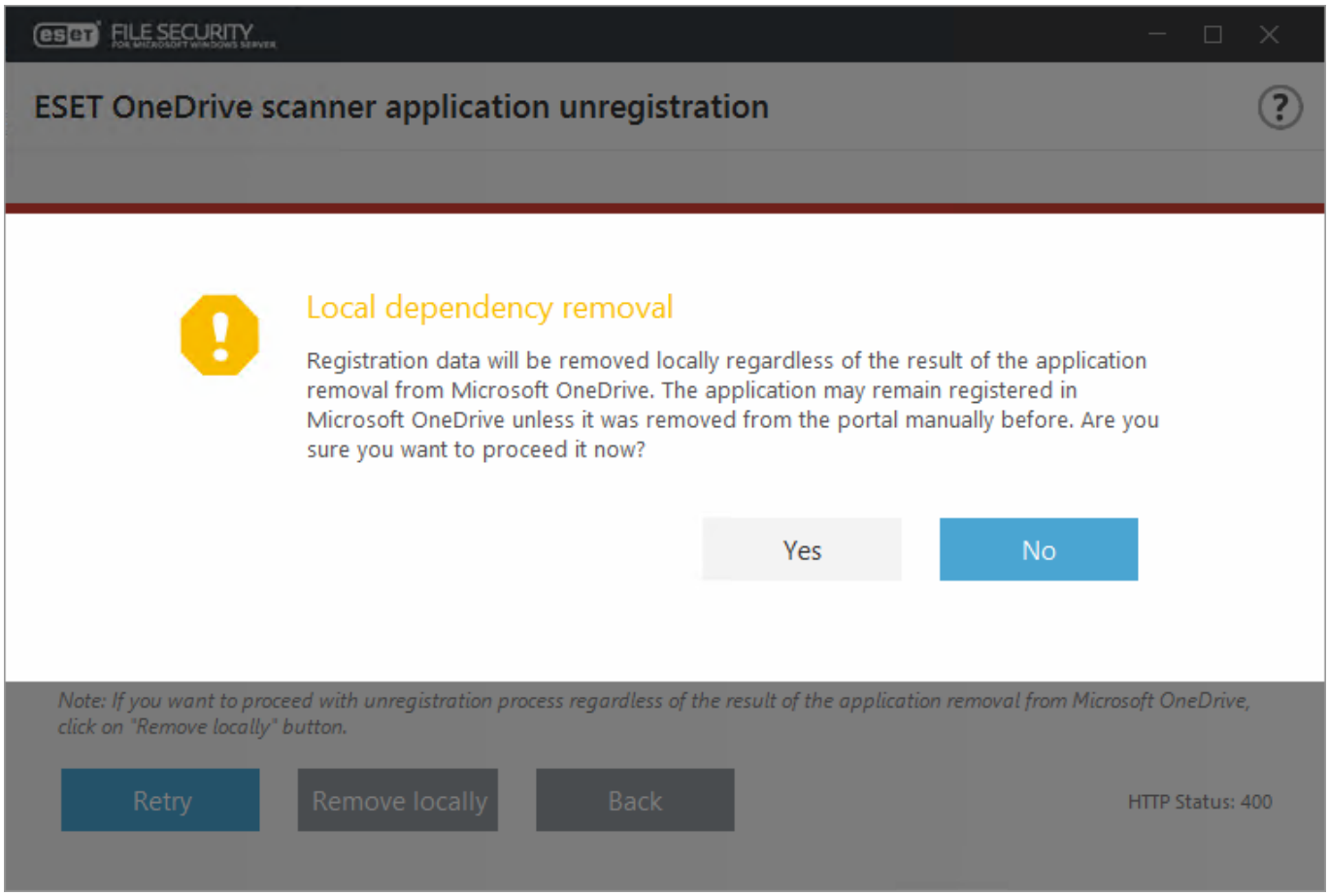
NOTA
Si recibe un mensaje de error, como, por ejemplo, Error al anular el registro, podría haber diversas razones para ello, entre ellas, por ejemplo, problemas genéricos de conexión a la red o a Internet con los servidores de Microsoft OneDrive, o que la aplicación ESET OneDrive Scanner ya no esté registrada en Microsoft OneDrive. Consulte la tabla que aparece a continuación que incluye la lista de mensajes de error y cómo solucionarlos.

Algunos cuadros de diálogo de error le ofrecen la opción de eliminar dependencias locales (problemas de conexión, aplicación no existente en Microsoft OneDrive, etc.). Para quitar ESET OneDrive Scanner a nivel local, realice lo siguiente:

• Si el botón **Reintentar** no funciona y el problema persiste, haga clic en **Quitar localmente** para continuar con el proceso de anulación de registro que eliminará las dependencias locales de ESET OneDrive Scanner.



• Haga clic en **Sí** para continuar con la eliminación local de ESET OneDrive Scanner. El análisis de ESET OneDrive ya no estará disponible y tendrá que volver a ejecutar el proceso de registro.



IMPORTANTE
La eliminación de dependencias locales no realizará ningún cambio en los registros de aplicaciones del portal de Azure ni tampoco en los permisos de aplicaciones del portal de Office 365. Si ha eliminado ESET OneDrive Scanner a nivel local debido a problemas de red o de conexión con los servidores de Microsoft OneDrive, tendrá que eliminar manualmente la aplicación ESET OneDrive Scanner de los registros de aplicaciones de Azure. Consulte Configuración del análisis de OneDrive para descubrir cómo encontrar y eliminar ESET OneDrive Scanner manualmente en el portal de Azure.

Si aparece alguno de los siguientes mensajes de error durante la anulación de registro de ESET OneDrive Scanner, consulte los detalles del mensaje de error para encontrar una sugerencia de solución:

Mensaje de error	Detalles del mensaje de error
La conexión a la aplicación de Azure no se ha realizado correctamente. No hay conexión a Internet.	Compruebe su conexión a Internet o a la red y vuelva a ejecutar la anulación de registro. Si desea continuar con el proceso de anulación de registro sin eliminar la aplicación ESET OneDrive Scanner de Microsoft OneDrive, haga clic en **Quitar localmente**.
Error al adquirir el token de acceso. Se ha recibido un error inesperado de Microsoft OneDrive.	Parece que la aplicación ESET OneDrive Scanner ya no está registrada en Microsoft OneDrive. La aplicación ESET OneDrive Scanner podría haberse eliminado manualmente del portal de Azure. Compruebe la presencia de la aplicación ESET OneDrive Scanner en el portal de Azure o en Microsoft OneDrive. Si la aplicación no aparece en la lista, haga clic en **Quitar localmente** para continuar con el proceso de anulación de registro.
Error al adquirir el token de acceso. Se ha recibido un error de servidor de Microsoft OneDrive.	Microsoft OneDrive ha devuelto el error HTTP 5xx. En este momento, no es posible completar la tarea de anulación de registro; intente ejecutarla más tarde.
Se ha recibido el siguiente error de Microsoft OneDrive.	El servidor de Microsoft OneDrive ha devuelto un error con un código/nombre de error específico, haga clic en **Mostrar error**.
Otra tarea de configuración ya está en curso.	Ya hay una tarea de anulación de registro en curso. Espere hasta que se complete el primer proceso de anulación de registro.

Configuración general

Puede establecer la configuración general y las opciones según sus necesidades. El menú de la izquierda incluye las siguientes categorías:

Motor de detección

Active o desactive la detección de aplicaciones potencialmente no deseadas, inseguras o sospechosas y la protección Anti-Stealth. Especifique exclusiones de procesos o archivos y carpetas. Configure la protección del sistema de archivos en tiempo real, los parámetros de ThreatSense, la protección en la nube (ESET LiveGrid®), análisis de malware (análisis del ordenador a petición y otras opciones de análisis), HIPS y análisis Hyper-V.

Actualización

Configure opciones de actualización, tales como perfiles, antigüedad del motor de detección, instantáneas de reversión del módulo, tipo de actualización, servidor de actualización personalizado, servidor de conexión /proxy, mirror de actualización, acceso a los archivos de actualización, servidor HTTP, detalles de la cuenta de usuario para la conexión de red, etc.

Web y correo electrónico

Le permite configurar el filtrado de protocolos y las exclusiones (direcciones IP y aplicaciones excluidas), las opciones de filtrado de protocolos SSL/TLS, la protección del cliente de correo electrónico (integración, protocolos de correo electrónico, alertas y notificaciones), protección de acceso a la Web (gestión de direcciones URL y protocolos web HTPP/HTTPS) y protección Antiphishing de cliente de correo electrónico.

Control del dispositivo

Active la integración y configure reglas y grupos de control de dispositivos.

Configuración de las herramientas

Le permite personalizar herramientas como ESET CMD, ESET RMM, proveedor WMI, objetivos de análisis de ESET PROTECT, notificaciones de Windows Update, archivos de registro, servidor proxy, notificaciones por correo electrónico, diagnóstico, clúster, etc.

Interfaz de usuario

Configure el comportamiento de la interfaz gráfica de usuario (GUI) del programa, los estados, la información de la licencia, las alertas y notificaciones, la protección por contraseña, la política de ejecución de eShell, etc.

Motor de detección

El motor de detección protege contra ataques maliciosos al sistema mediante el análisis de los archivos, los correos electrónicos y la comunicación de red. Si se detecta un objeto clasificado como malware, se iniciará la corrección. El motor de detección puede eliminarlo bloqueándolo primero y, a continuación, tomando medidas como la desinfección, la eliminación o la puesta en cuarentena.

Protección en tiempo real y de aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección gracias al aprendizaje automático. Puede obtener más información sobre este tipo de protección en el glosario. Puede configurar los niveles de informe y protección de las siguientes categorías:

Malware

Un virus informático es un fragmento de código malicioso que antecede o sigue a los archivos existentes en el ordenador. Sin embargo, el término "virus" suele utilizarse de forma inadecuada. "Malware" (software malicioso) es un término más exacto. La detección de malware la realiza el módulo del motor de detección en combinación con el componente de aprendizaje automático. Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente indeseables (PUA)

Una aplicación potencialmente no deseada es un software con una intención que no es inequívocamente malintencionada, pero que puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital, realizar actividades no aprobadas o esperadas por el usuario, o que tiene otros objetivos que no son claros.
En esta categoría se incluyen el software de visualización de publicidad, los contenedores de descarga, diversas herramientas barras de herramientas para el navegador, software con comportamiento engañoso, software agrupado, software de seguimiento, etc.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente sospechosas

Es un software comprimido con empaquetadores o protectores que normalmente se utilizan para impedir la ingeniería inversa u ocultar el contenido del archivo ejecutable (por ejemplo para ocultar la presencia de malware) con métodos privados de compresión o cifrado.
En esta categoría se incluyen todas las aplicaciones desconocidas comprimidas con un empaquetador o protector que se suelen usar para comprimir malware.

Aplicaciones potencialmente peligrosas

Esta clasificación se ofrece para programas de software comercial legítimo que pueden utilizarse con fines maliciosos. Una aplicación peligrosa hace referencia a un programa de software comercial legítimo que tiene el potencial de usarse con fines maliciosos.
En esta categoría se incluyen herramientas de descifrado, generadores de claves de licencia, herramientas de ataques informáticos, herramientas de control o acceso remoto aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran todas las teclas que pulsa un usuario). Esta opción está desactivada de forma predeterminada.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe o protección:

Informe

Los informes los realizan el motor de detección y el componente de aprendizaje automático. Puede establecer el umbral de elaboración de informes como mejor se adapte a su entorno y a sus necesidades. No hay una sola configuración correcta. Por ello, le recomendamos que supervise el comportamiento de su entorno y decida si es más adecuada otra configuración de los informes.

Los informes no llevan a cabo acciones con los objetos: transfieren información a la capa de protección correspondiente y la capa de protección lleva a cabo la acción adecuada.

Agresivo	**Informe configurado con la máxima sensibilidad. Se informa de más detecciones. Aunque el ajuste Agresivo puede parecer el más seguro, suele ser demasiado sensible, lo que puede ser contraproducente.** NOTA El ajuste Agresivo puede identificar erróneamente objetos como maliciosos, y se realizará una acción con dichos objetos (en función de la configuración de la protección).
Equilibrado	Este ajuste tiene un equilibrio óptimo entre rendimiento, precisión de la detección y número de falsos positivos.
Precavido	Informe configurado para reducir al mínimo los falsos positivos a la vez que se mantiene un nivel de protección suficiente. Solo se informa de los objetos cuando la probabilidad es evidente y coincide con el comportamiento del malware.
Desactivado	El informe no está activo. Las detecciones no se encuentran, no se informa de ellas o no se desinfectan. NOTA Los informes de malware no se pueden desactivar; por lo tanto, el ajuste **Desactivado** no está disponible para el malware.

Si desea restaurar los ajustes predeterminados de esta sección, haga clic en la flecha en "U" situada junto al encabezado de la sección. Se perderán todos los cambios realizados en esta sección.

Cuando se informa de un objeto en función de la configuración anterior y los resultados del aprendizaje automático, se bloquea y se realiza una acción (el objeto se desinfecta, se elimina o se pone en cuarentena).

Agresivo	**Se bloquean las detecciones de nivel agresivo (o inferior) y se inicia la corrección automática (es decir, la desinfección).**
Equilibrado	Se bloquean las detecciones de nivel equilibrado (o inferior) y se inicia la corrección automática (es decir, la desinfección).
Precavido	Se bloquean las detecciones de nivel precavido y se inicia la corrección automática (es decir, la desinfección).
Desactivado	Los informes no están activos y las detecciones no se encuentran, no se informa de ellas o no se desinfectan. NOTA Los informes de malware no se pueden desactivar, por lo que el ajuste **Desactivado** no está disponible para el malware.

Si desea restaurar los ajustes predeterminados de esta sección, haga clic en la flecha en "U" situada junto al encabezado de la sección. Se perderán todos los cambios realizados en esta sección.

NOTA
De forma predeterminada, la configuración de la protección de aprendizaje automático anterior se aplica también al análisis del ordenador a petición. Si es necesario, puede configurar los ajustes de **Protección a petición y de aprendizaje automático** por separado. Haga clic en el icono del conmutador para desactivar **Usar ajustes de protección en tiempo real** y continuar con la configuración.

Detección de aprendizaje automático

El motor de detección protege contra ataques maliciosos al sistema mediante el análisis de los archivos, los correos electrónicos y la comunicación de red. Si se detecta un objeto clasificado como malware, se iniciará la corrección. El motor de detección puede eliminarlo bloqueándolo primero y, a continuación, tomando medidas como la desinfección, la eliminación o la puesta en cuarentena.

Protección en tiempo real y de aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección gracias al aprendizaje automático. Puede obtener más información sobre este tipo de protección en el glosario. Puede configurar los niveles de informe y protección de las siguientes categorías:

Malware

Un virus informático es un fragmento de código malicioso que antecede o sigue a los archivos existentes en el ordenador. Sin embargo, el término "virus" suele utilizarse de forma inadecuada. "Malware" (software malicioso) es un término más exacto. La detección de malware la realiza el módulo del motor de detección en combinación con el componente de aprendizaje automático. Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente indeseables (PUA)

Una aplicación potencialmente no deseada es un software con una intención que no es inequívocamente malintencionada, pero que puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital, realizar actividades no aprobadas o esperadas por el usuario, o que tiene otros objetivos que no son claros.
En esta categoría se incluyen el software de visualización de publicidad, los contenedores de descarga, diversas herramientas barras de herramientas para el navegador, software con comportamiento engañoso, software agrupado, software de seguimiento, etc.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente sospechosas

Es un software comprimido con empaquetadores o protectores que normalmente se utilizan para impedir la ingeniería inversa u ocultar el contenido del archivo ejecutable (por ejemplo para ocultar la presencia de malware) con métodos privados de compresión o cifrado.
En esta categoría se incluyen todas las aplicaciones desconocidas comprimidas con un empaquetador o protector que se suelen usar para comprimir malware.

Aplicaciones potencialmente peligrosas

Esta clasificación se ofrece para programas de software comercial legítimo que pueden utilizarse con fines maliciosos. Una aplicación peligrosa hace referencia a un programa de software comercial legítimo que tiene el potencial de usarse con fines maliciosos.
En esta categoría se incluyen herramientas de descifrado, generadores de claves de licencia, herramientas de ataques informáticos, herramientas de control o acceso remoto aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran todas las teclas que pulsa un usuario). Esta opción está desactivada de forma predeterminada.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe o protección:

Informe

Los informes los realizan el motor de detección y el componente de aprendizaje automático. Puede establecer el umbral de elaboración de informes como mejor se adapte a su entorno y a sus necesidades. No hay una sola configuración correcta. Por ello, le recomendamos que supervise el comportamiento de su entorno y decida si es más adecuada otra configuración de los informes.

Los informes no llevan a cabo acciones con los objetos: transfieren información a la capa de protección correspondiente y la capa de protección lleva a cabo la acción adecuada.

Agresivo	**Informe configurado con la máxima sensibilidad. Se informa de más detecciones. Aunque el ajuste Agresivo puede parecer el más seguro, suele ser demasiado sensible, lo que puede ser contraproducente.** NOTA El ajuste Agresivo puede identificar erróneamente objetos como maliciosos, y se realizará una acción con dichos objetos (en función de la configuración de la protección).
Equilibrado	Este ajuste tiene un equilibrio óptimo entre rendimiento, precisión de la detección y número de falsos positivos.
Precavido	Informe configurado para reducir al mínimo los falsos positivos a la vez que se mantiene un nivel de protección suficiente. Solo se informa de los objetos cuando la probabilidad es evidente y coincide con el comportamiento del malware.

Agresivo	**Informe configurado con la máxima sensibilidad. Se informa de más detecciones. Aunque el ajuste Agresivo puede parecer el más seguro, suele ser demasiado sensible, lo que puede ser contraproducente.** NOTA El ajuste Agresivo puede identificar erróneamente objetos como maliciosos, y se realizará una acción con dichos objetos (en función de la configuración de la protección).
Desactivado	El informe no está activo. Las detecciones no se encuentran, no se informa de ellas o no se desinfectan. NOTA Los informes de malware no se pueden desactivar; por lo tanto, el ajuste **Desactivado** no está disponible para el malware.

Si desea restaurar los ajustes predeterminados de esta sección, haga clic en la flecha en "U" situada junto al encabezado de la sección. Se perderán todos los cambios realizados en esta sección.

Protección de OneDrive y aprendizaje automático

Creación de informes

Los informes los realizan el motor de detección y el componente de aprendizaje automático. Los informes no realizan ninguna acción con los objetos (esto lo hace la capa de protección correspondiente).

Protección

Configure los parámetros de la sección OneDrive para modificar la acción que se lleva a cabo con los objetos de los que se informa.

Si desea restaurar los ajustes predeterminados de esta sección, haga clic en la flecha en "U" situada junto al encabezado de la sección. Se perderán todos los cambios realizados en esta sección.

Configure la protección de aprendizaje automático con eShell. El nombre de contexto de eShell es **MLP**. Abra eShell en el modo interactivo y vaya a MLP:

```
computer onedrive mlp
```

Consulte cuál es la configuración actual de informes para aplicaciones sospechosas:

```
get suspicious-reporting
```

Si desea informes menos rigurosos, cambie el ajuste a Precavido:

```
set suspicious-reporting cautious
```

Exclusiones

Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario.

Puede que haya situaciones en las que necesite excluir un objeto, como durante el análisis de entradas de una base de datos grande que ralentice el servidor o software que entre en conflicto con el análisis (por ejemplo, software de copia de seguridad).

ADVERTENCIA
No deben confundirse con las extensiones excluidas, las exclusiones de procesos ni el filtro de exclusión.

NOTA
el módulo de protección del sistema de archivos en tiempo real o de análisis del ordenador no detectará las amenazas que contenga un archivo si este cumple los criterios de exclusión del análisis.

Seleccione el tipo de exclusiones y haga clic en **Editar** para agregar una nueva o modificar una existente:

- Exclusiones de rendimiento: excluya archivos y carpetas del análisis.
- Exclusiones de detección: excluya objetos del análisis con criterios específicos, como ruta de acceso, hash del archivo o nombre de la detección.

Exclusiones de rendimiento

Esta función le permite excluir archivos y carpetas del análisis. Las exclusiones de rendimiento son útiles para excluir el análisis a nivel de archivo de aplicaciones importantes o cuando el análisis provoca un comportamiento anómalo del sistema o reduce el rendimiento.

Ruta de acceso

Excluye una ruta de acceso específica (archivo o directorio) para este ordenador. No utilice comodines - asterisco (*) en medio de una ruta de acceso. Consulte el artículo de la Base de conocimiento para obtener más información.

NOTA
Excluir contenido de carpetas, no olvide agregar el asterisco (*) al final de la ruta de acceso (*C:\Tools**). *C:\Tools* no se excluirá porque, desde la perspectiva del análisis, *Herramientas* también puede ser un nombre de archivo.

Comentario

Agregue un **Comentario** opcional para reconocer fácilmente la exclusión en el futuro.

EJEMPLO
Exclusiones de ruta de acceso usando un asterisco:
*C:\Tools**: la ruta de acceso debe terminar con la barra invertida (\) y el asterisco (*) para indicar que es una carpeta y todo el contenido de dicha carpeta (archivos y subcarpetas) se excluirá.
C:\Tools.**: el mismo comportamiento que *C:\Tools**, lo que significa que funciona de forma recursiva.
C:\Tools.dat*: excluirá los archivos *dat* de la carpeta Herramientas.
C:\Tools\sg.dat: excluirá este archivo particular en la ruta exacta.

EJEMPLO
Para excluir todos los archivos de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara *.*
• Para excluir solo archivos .doc, utilice la máscara *.doc
• Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato:
D????.exe (los signos de interrogación sustituyen a los caracteres que faltan o son desconocidos)

EJEMPLO
Utilice variables del sistema como *%PROGRAMFILES%* para definir las exclusiones del análisis.
• Para excluir la carpeta Program Files con esta variable del sistema, utilice la ruta de acceso *%PROGRAMFILES%* (asegúrese de añadir la barra invertida al final de la ruta de acceso al agregarla a las exclusiones).
• Si desea excluir todos los archivos del subdirectorio *%HOMEDRIVE%*, utilice la ruta de acceso *%HOMEDRIVE%\Excluded_Directory*.*.
Las siguientes variables pueden usarse en el formato de exclusión de la ruta de acceso:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
No se admiten variables del sistema específicas de usuarios (como *%TEMP%* o *%USERPROFILE%*), ni variables del entorno (como *%PATH%*).

Exclusiones de detección

Este es otro método para excluir objetos del análisis, con el nombre de la detección, la ruta de acceso o su hash. Las exclusiones de detección no excluyen archivos y carpetas del análisis (como las exclusiones de rendimiento). Las exclusiones de detección solo excluyen objetos cuando los detecta el motor de detección y existe una regla apropiada en la lista de exclusiones.

La forma más sencilla de crear una exclusión basada en la detección es usar una detección existente de **Archivos de registro** > Detecciones. Haga clic con el botón derecho del ratón en un registro (detección) y haga clic en **Crear exclusión**. Se abrirá el Asistente de exclusiones con los criterios predefinidos.

Para crear una exclusión de detección manualmente, haga clic en **Editar** > **Agregar** (o en **Editar** para modificar una existente) y especifique uno o más de los siguientes criterios (se pueden combinar):

Ruta de acceso

Excluye una ruta de acceso específica (archivo o directorio). Puede buscar una ubicación o un archivo específicos o introducir la cadena manualmente. No utilice comodines - asterisco (*) en medio de una ruta de acceso. Consulte el artículo de la base de conocimiento que se indica a continuación para obtener más información.

NOTA
Excluir contenido de carpetas, no olvide agregar el asterisco (*) al final de la ruta de acceso (*C:\Tools**). *C:\Tools* no se excluirá porque, desde la perspectiva del análisis, *Herramientas* también puede ser un nombre de archivo.

Hash

Excluye un archivo según un hash especificado (SHA1), sea cual sea el tipo de archivo, la ubicación, el nombre o la extensión.

Nombre de la detección

Introduzca un nombre de detección (amenaza) válido. Crear una exclusión únicamente en función del nombre de la detección puede representar un riesgo para la seguridad. Le recomendamos que combine el nombre de la detección con la ruta de acceso. Estos criterios de exclusión solo pueden utilizarse para ciertos tipos de detecciones.

Comentario

Agregue un **Comentario** opcional para reconocer fácilmente la exclusión en el futuro.

ESET PROTECT incluye administración de exclusiones de detección para crear exclusiones de detección y aplicarlas a más ordenadores o grupos.

Utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (*?*) representa un carácter único variable y el asterisco (*) representa una cadena variable de cero o más caracteres.

EJEMPLO
Exclusiones de ruta de acceso usando un asterisco:
*C:\Tools**: la ruta de acceso debe terminar con la barra invertida (\) y el asterisco (*) para indicar que es una carpeta y todo el contenido de dicha carpeta (archivos y subcarpetas) se excluirá.
C:\Tools.**: el mismo comportamiento que *C:\Tools**, lo que significa que funciona de forma recursiva.
C:\Tools.dat*: excluirá los archivos *dat* de la carpeta Herramientas.
C:\Tools\sg.dat: excluirá este archivo particular en la ruta exacta.

EJEMPLO
Para excluir una amenaza, introduzca el nombre de detección válido con el siguiente formato:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

EJEMPLO
Para excluir todos los archivos de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara *.**
- Para excluir solo archivos .doc, utilice la máscara *.doc*
- Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato:
D????.exe (los signos de interrogación sustituyen a los caracteres que faltan o son desconocidos)

EJEMPLO
Utilice variables del sistema como *%PROGRAMFILES%* para definir las exclusiones del análisis.
• Para excluir la carpeta Program Files con esta variable del sistema, utilice la ruta de acceso *%PROGRAMFILES%*\ (asegúrese de añadir la barra invertida al final de la ruta de acceso al agregarla a las exclusiones).
• Si desea excluir todos los archivos del subdirectorio *%HOMEDRIVE%*, utilice la ruta de acceso *%HOMEDRIVE%**Excluded_Directory**.*.
Las siguientes variables pueden usarse en el formato de exclusión de la ruta de acceso:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
No se admiten variables del sistema específicas de usuarios (como *%TEMP%* o *%USERPROFILE%*), ni variables del entorno (como *%PATH%*).

Asistente de creación de exclusiones

La exclusión recomendada se preselecciona en función del tipo de detección, pero también puede especificar criterios de exclusión para las detecciones. Haga clic en **Cambiar criterios**:

- **Archivos exactos**: excluya cada archivo por su hash SHA-1.
- **Detección**: especifique el nombre de la detección para excluir todos los archivos que contengan dicha detección.
- **Ruta de acceso + detección**: especifique el nombre y la ruta de acceso de la detección (incluido el nombre de archivo) para excluir todos los archivos con una detección en la ubicación especificada.

Agregue un **Comentario** opcional para reconocer fácilmente la exclusión en el futuro.

Opciones avanzadas

Tecnología Anti-Stealth

Es un sofisticado sistema de detección de programas peligrosos como rootkits, que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

AMSI

Deje que la interfaz de examen antimalware de Microsoft (AMSI) analice los scripts PowerShell ejecutados por Windows Script Host.

Exclusiones automáticas

Los desarrolladores de aplicaciones de servidor y sistemas operativos recomiendan excluir conjuntos de archivos y carpetas de trabajo críticos del análisis de malware para la mayoría de sus productos. El análisis de malware puede tener una influencia negativa sobre el rendimiento de un servidor, lo que puede provocar conflictos e incluso impedir que algunas aplicaciones se ejecuten en el servidor. Las exclusiones ayudan a reducir al mínimo el riesgo de que pueda haber conflictos y a aumentar el rendimiento general del servidor cuando se ejecuta software antimalware. Consulte la lista de archivos excluidos del análisis para productos de servidor de ESET.

ESET Server Security identifica las aplicaciones de servidor y los archivos del sistema operativo del servidor esenciales y los agrega automáticamente a la lista de Exclusiones. Todas las exclusiones automáticas están activadas de forma predeterminada. Puede desactivar o activar las exclusiones de cada aplicación de servidor con la barra deslizante, con el siguiente resultado:

- Cuando están activadas, cualquiera de sus archivos y carpetas críticos se agregará a la lista de archivos excluidos del análisis. Cada vez que se reinicia el servidor, el sistema realiza una comprobación automática de las exclusiones y actualiza la lista si ha habido cambios en el sistema o las aplicaciones (por ejemplo, si se ha instalado una nueva aplicación de servidor). Esta configuración garantiza que se apliquen siempre las Exclusiones automáticas recomendadas.

- Cuando están desactivadas, los archivos y carpetas excluidos automáticamente se quitarán de la lista. Las exclusiones definidas por el usuario introducidas manualmente no se verán afectadas.

Para identificar y generar exclusiones automáticas, ESET Server Security utiliza la aplicación dedicada *eAutoExclusions.exe*, ubicada en la carpeta de instalación. No es necesaria ninguna interacción suya, pero puede utilizar la línea de comandos para mostrar las aplicaciones de servidor detectadas en su sistema ejecutando `eAutoExclusions.exe -servers`. Para mostrar la sintaxis completa, utilice `eAutoExclusions.exe -?`.

Caché local compartida

La Caché local compartida de ESET mejorará el rendimiento en entornos virtualizados al eliminar el análisis duplicado en la red. De esta manera se garantiza que cada archivo se analizará solo una vez y se almacenará en la caché compartida. Active el conmutador **Activar caché** para guardar en la caché local información sobre los análisis de archivos y carpetas de su red. Si realiza un análisis nuevo, ESET Server Security buscará los archivos analizados en la caché. Si los archivos coinciden, no se incluirán en el análisis.

La configuración de Servidor de caché contiene los campos siguientes:

- **Nombre de host**: nombre o dirección IP del ordenador donde se encuentra la caché.
- **Puerto**: número de puerto utilizado para la comunicación (el mismo que se estableció en la caché local compartida).
- **Contraseña**: especifique la contraseña de la caché local compartida, si es necesario.

Detección de una amenaza

Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Comportamiento estándar

Como ejemplo general de cómo ESET Server Security gestiona las amenazas, estas se pueden detectar mediante:

- Protección del sistema de archivos en tiempo real
- Protección del tráfico de Internet
- Protección del cliente de correo electrónico
- Análisis del ordenador

Cada uno de estos componentes utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Se muestra una ventana de notificación en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para obtener más información sobre los tipos de desinfección y el comportamiento, consulte la sección Desinfección.

Desinfección y eliminación

Si no hay que realizar ninguna acción predefinida para la protección en tiempo real, se le pedirá que seleccione una opción en la ventana de alerta. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados quedarían intactos. La única excepción es cuando está seguro de que el archivo es inofensivo y se ha detectado por error.

Aplique esta opción si un archivo ha sido infectado por un virus que le ha añadido código malicioso. Si este es el caso, intente desinfectar el archivo infectado para restaurarlo a su estado original antes de la desinfección. Si el archivo consta exclusivamente de código malicioso, se eliminará.

Si un proceso del sistema "bloquea" o está utilizando un archivo infectado, por lo general solo se eliminará cuando se haya publicado (normalmente, tras reiniciar el sistema).

Múltiples amenazas

Si durante un análisis del ordenador no se desinfectaron algunos archivos infectados (o el Nivel de desinfección se estableció en **Sin desinfección**), aparecerá una ventana de alerta solicitándole que seleccione las acciones que desea llevar a cabo en esos archivos. Seleccione una acción individualmente para cada una de las amenazas de la lista, o utilice **Seleccionar acción para todas las amenazas de la lista**, elija la acción que desea realizar en todas las amenazas de la lista y, a continuación, haga clic en **Finalizar**.

Eliminación de amenazas de archivos comprimidos

En el modo de desinfección predeterminado, solo se eliminará todo el archivo comprimido si todos los archivos que contiene están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos no infectados e inofensivos. Tenga cuidado cuando realice un análisis con desinfección exhaustiva activada, ya que un archivo comprimido se eliminará si contiene al menos un archivo infectado, sin tener en cuenta el estado de los otros archivos.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con malware en el sistema. Todos los archivos se analizan en busca de código malicioso cuando se abren, crean o ejecutan en su ordenador. De forma predeterminada, la protección del sistema de archivos en tiempo real se inicia al arrancar el sistema y proporciona análisis ininterrumpido. En casos especiales (por ejemplo, si hay un conflicto con otro análisis en tiempo real), la protección en tiempo real puede desactivarse desmarcando **Iniciar automáticamente la protección del sistema de archivos en tiempo real** en **Configuración avanzada** (**F5**) en **Protección del sistema de archivos en tiempo real** > **Básico**.

ESET Server Security es compatible con equipos que usan el agente de Azure File Sync con los niveles de nube activados. ESET Server Security reconoce archivos con el atributo *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Objetos a analizar

De forma predeterminada, se buscan posibles amenazas en todos los tipos de objetos:

- **Unidades locales**: controla todas las unidades de disco duro del sistema.
- **Medios extraíbles**: controla los discos CD y DVD, el almacenamiento USB, los dispositivos Bluetooth, etc.
- **Unidades de red**: analiza todas las unidades asignadas.

Recomendamos que esta configuración predeterminada se modifique solo en casos específicos como, por ejemplo, cuando el control de ciertos objetos ralentiza significativamente las transferencias de datos.

Analizar

De forma predeterminada, todos los archivos se analizan cuando se abren, crean o ejecutan. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador:

- **Abrir el archivo**: análisis al abrir archivos o acceder a ellos.
- **Crear el archivo**: análisis durante la creación o modificación de archivos.
- **Ejecutar el archivo**: análisis cuando se ejecutan archivos.
- **Acceso a medios extraíbles**: análisis durante el acceso a almacenamiento extraíble. Cuando el medio extraíble que contiene un sector de inicio se inserta en el dispositivo, el sector de inicio se analiza inmediatamente. Esta opción no activa el análisis de archivos en medios extraíbles. El análisis de archivos en medios extraíbles está en **Objetos a analizar** > **Medios extraíbles**. Para que el acceso al sector de inicio de medios extraíbles funcione correctamente, mantenga **Sectores de inicio/UEFI activado** en los parámetros de ThreatSense.

Exclusiones de procesos

Esta opción le permite excluir procesos concretos. Por ejemplo, en el caso de los procesos de la solución de copia de seguridad, todas las operaciones con archivos relacionadas con dicho proceso se ignoran y se consideran seguras, lo que minimiza las interferencias con el proceso de copia de seguridad.

Parámetros de ThreatSense

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y se activa con varios sucesos del sistema como, por ejemplo, cuando se accede a un archivo. La protección del sistema de archivos en tiempo real se puede configurar para que trate de forma diferente los archivos recién creados y los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se vuelven a analizar inmediatamente después de cada actualización del motor de detección. Este comportamiento se controla con la opción **Optimización inteligente**. Si la opción **Optimización inteligente** está desactivada, se analizan todos los archivos cada vez que se accede a ellos. Para modificar este ajuste, pulse **F5** para abrir **Configuración avanzada** y expanda **Motor de detección** > **Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetros de ThreatSense** > **Otros** y seleccione o anule la selección de **Activar optimización inteligente**.

Parámetros adicionales de ThreatSense

Puede modificar las opciones detalladas de **Parámetros adicionales de ThreatSense de archivos nuevos y modificados** o **Parámetros adicionales de ThreatSense de archivos ejecutados**.

Parámetros de ThreatSense

La tecnología ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina los rootkits eficazmente.

> NOTA
> para obtener más información sobre la comprobación automática de los archivos en el inicio, consulte Análisis en el inicio.

Las opciones de configuración del motor ThreatSense permiten al usuario especificar distintos parámetros de análisis:

- **Los tipos de archivos y extensiones que se deben analizar.**
- **La combinación de diferentes métodos de detección.**
- **Los niveles de desinfección, etc.**

Para acceder a la ventana de configuración, haga clic en **Configuración de los parámetros del motor ThreatSense** en la ventana **Configuración avanzada** (**F5**) de cualquier módulo que utilice la tecnología ThreatSense (consulte a continuación). Es posible que cada contexto de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Análisis Hyper-V
- Análisis de OneDrive
- Protección del sistema de archivos en tiempo real
- Análisis de malware
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían implicar la ralentización del sistema (normalmente, solo se analizan archivos recién creados mediante estos métodos). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

⊟ Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

Memoria operativa

Busca amenazas que ataquen a la memoria operativa del sistema.

Sectores de inicio/UEFI

Analiza los sectores de inicio para detectar virus en el registro de inicio principal (MBR). Si se trata de una máquina virtual Hyper-V, el MBR del disco se analiza en el modo de solo lectura.

Archivos de correo electrónico

El programa admite las extensiones: DBX (Outlook Express) y EML.

Archivos comprimidos

El programa admite las siguientes extensiones: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

Archivos comprimidos de autoextracción

Los archivos comprimidos de autoextracción (SFX) son archivos que no necesitan programas especializados (archivos comprimidos) para descomprimirse.

Empaquetadores en tiempo real

Después de su ejecución, los empaquetadores en tiempo real (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis es capaz de reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

Heurística

La heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía.

Heurística avanzada/ADN inteligentes

La heurística avanzada es un algoritmo heurístico único desarrollado por ESET, y optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que

únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

Desinfección

Las opciones de desinfección determinan el comportamiento del análisis durante la desinfección de archivos infectados. Hay 3 niveles de desinfección:

Sin desinfección

Los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción. Este nivel es adecuado para usuarios avanzados que conocen los pasos necesarios en caso de amenaza.

Desinfección normal

El programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (según el tipo de amenaza). La detección y la eliminación de un archivo infectado se marcan mediante una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección estricta

El programa desinfecta o elimina todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un archivo, se preguntará al usuario qué tipo de acción debe realizarse.

ADVERTENCIA
si un archivo comprimido contiene archivos infectados, se puede tratar de dos maneras: En el modo predeterminado **Desinfección normal**, se elimina el archivo comprimido completo si todos los archivos que contiene están infectados. En el modo **Desinfección estricta**, el archivo se elimina si contiene al menos un archivo infectado, independientemente del estado de los demás archivos.

IMPORTANTE
Si el host Hyper-V se está ejecutando en Windows Server 2008 R2 SP1, las opciones **Desinfección normal** y **Desinfección estricta** no son compatibles. El análisis de los discos de la máquina virtual se realiza en el modo de solo lectura, y no se llevará a cabo la desinfección. Sea cual sea el nivel de desinfección seleccionado, el análisis siempre se realiza en el modo de solo lectura.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En este apartado de la configuración de parámetros de ThreatSense es posible definir los tipos de archivos que se desean excluir del análisis.

Otros

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

Analizar secuencias de datos alternativas (ADS)

Las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección al hacerse pasar por secuencias de datos alternativas.

Realizar análisis en segundo plano con baja prioridad

Cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos

Si se selecciona esta opción, el archivo de registro mostrará todos los archivos analizados, incluso los que no estén infectados.

Activar la optimización inteligente

Si la opción Optimización inteligente está activada, se utiliza la configuración óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la Optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo de ThreatSense de los módulos en los que se realice el análisis.

Preservar el último acceso con su fecha y hora

Seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Usar parámetros predeterminados del objeto

Active esta opción para utilizar la configuración predeterminada (sin límite). ESET Server Security ignorará la configuración personalizada.

Tamaño máximo del objeto

Define el tamaño máximo de los objetos que se analizarán. A continuación, el módulo de protección correspondiente analizará solo objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que puedan tener motivos específicos para excluir del análisis objetos mayores. Valor predeterminado: ilimitado.

Tiempo máximo de análisis para el objeto (seg.)

Define el valor de tiempo máximo para analizar un objeto. Si aquí se ha introducido un valor definido por el usuario, el módulo de protección dejará de analizar un objeto cuando haya transcurrido ese tiempo, independientemente de si el análisis ha finalizado. Valor predeterminado: ilimitado.

Configuración del análisis de archivos comprimidos

Para modificar la configuración de análisis de archivos comprimidos, desactive la opción **Configuración predeterminada para el análisis de archivos comprimidos**.

Nivel de anidamiento de archivos

Especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10. En los objetos detectados por Protección del transporte del buzón, el nivel real de anidamiento es +1 porque adjuntar archivos comprimidos en un mensaje de correo electrónico se considera de primer nivel.

EJEMPLO
Si tiene el nivel de anidamiento configurado en 3, un archivo con nivel de anidamiento 3 solo se analizará en una capa de transporte hasta su nivel 2 real. Por lo tanto, si quiere que Protección del transporte del buzón analice los archivos hasta el nivel 3, configure el valor de **Nivel de anidamiento de archivos** en 4.

Tamaño máx. de archivo en el archivo comprimido

Esta opción le permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. Valor predeterminado: ilimitado.

NOTA
no se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

Parámetros adicionales de ThreatSense

Parámetros adicionales de ThreatSense de archivos nuevos y modificados

La probabilidad de infección en archivos modificados o recién creados es superior que en los archivos existentes, por eso el programa comprueba estos archivos con parámetros de análisis adicionales. Además de los métodos de análisis basados en firmas habituales, se utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización del módulo. El análisis se realiza también en archivos de autoextracción (.sfx) y empaquetadores en tiempo real (archivos ejecutables comprimidos internamente), no solo en los archivos nuevos. Los archivos se analizan, de forma predeterminada, hasta el décimo nivel de anidamiento; además, se analizan independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, desactive la opción **Configuración predeterminada para el análisis de archivos comprimidos**.

Parámetros adicionales de ThreatSense de archivos ejecutados

De forma predeterminada, la heurística avanzada se utiliza cuando se ejecutan archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET LiveGrid® con el fin de mitigar su repercusión en el rendimiento del sistema.

Extensiones de archivo excluidas del análisis

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo del archivo. Normalmente, todos los archivos se analizan. Sin embargo, si necesita excluir archivos con una extensión determinada, la configuración de parámetros de ThreatSense le permite excluir archivos del análisis en función de su extensión. La exclusión puede resultar útil si el análisis de determinados tipos de archivos evita que una

aplicación se ejecute de forma correcta.

EJEMPLO
Para agregar una nueva extensión a la lista, haga clic en **Agregar**. Escriba la extensión en el campo de texto (por ejemplo, `tmp`) y haga clic en **Aceptar**. Si selecciona **Introduzca múltiples valores**, puede añadir varias extensiones de archivos delimitadas por líneas, comas o punto y coma (por ejemplo, elija **Punto y coma** en el menú desplegable como separador y escriba `edb;eml;tmp`).
Se puede usar un símbolo especial ? (signo de interrogación). El signo de interrogación representa cualquier símbolo (por ejemplo, `?db`).

NOTA
Para ver la extensión (tipo de archivo) de todos los archivos en un sistema operativo Windows, tiene que desmarcar la opción **Ocultar extensiones de tipos de archivo conocidos** en **Panel de control** > **Opciones de carpeta** > **Ver**.

Exclusiones de procesos

La función de exclusiones de procesos le permite excluir procesos de aplicaciones solo del análisis Anti-Malware en el acceso. Debido al papel esencial que juegan los servidores dedicados (el servidor de aplicaciones, el servidor de almacenamiento, etc.), es obligatorio realizar copias de seguridad periódicas para recuperarse a tiempo de incidentes de cualquier tipo. Con el fin de mejorar la velocidad de la copia de seguridad, la integridad del proceso y la disponibilidad del servicio, durante la copia de seguridad se utilizan algunas técnicas que suelen entrar en conflicto con la protección contra malware a nivel de archivos. Al intentar realizar migraciones dinámicas de máquinas virtuales pueden surgir problemas similares. La única forma eficaz de evitar ambas situaciones es desactivar el software Anti-Malware. Al excluir procesos concretos (por ejemplo, los relacionados con la solución de copia de seguridad), todas las operaciones con archivos relacionadas con dicho proceso se ignoran y se consideran seguras, lo que minimiza las interferencias con el proceso de copia de seguridad. Se recomienda tener cuidado a la hora de crear exclusiones: una herramienta de copia de seguridad que se haya excluido puede acceder a archivos infectados sin desencadenar una alerta, razón por la cual los permisos ampliados solo se autorizan en el módulo de protección en tiempo real.

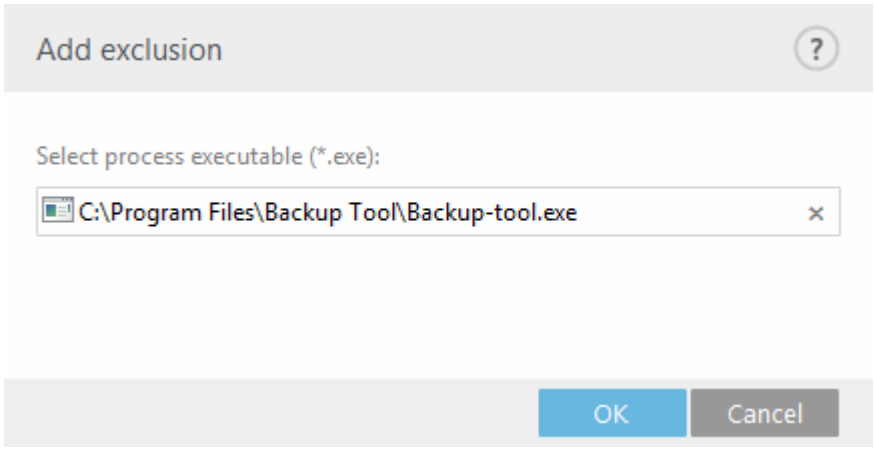
Las exclusiones de procesos ayudan a minimizar el riesgo de posibles conflictos y a mejorar el rendimiento de las aplicaciones excluidas, lo que a su vez tiene una repercusión positiva en el rendimiento y la estabilidad globales del sistema operativo. La exclusión de un proceso o aplicación es una exclusión de su archivo ejecutable (*.exe*).

Puede agregar archivos ejecutables a la lista de procesos excluidos desde **Configuración avanzada** (F5) > **Motor de detección** > **Protección del sistema de archivos en tiempo real** > **Básico** > **Exclusiones de procesos** o utilizando la lista de procesos en ejecución del menú principal **Herramientas** > **Procesos en ejecución**.

Esta función se ha diseñado para excluir herramientas de copia de seguridad. Excluir el proceso de las herramientas de copia de seguridad del análisis no solo garantiza la estabilidad del sistema, sino que, además, no afecta al rendimiento de la copia de seguridad, ya que esta no se ralentiza mientras se ejecuta.

EJEMPLO
Haga clic en **Editar** para abrir la ventana de gestión de **Exclusiones de procesos**, donde puede **Agregar** exclusiones y examinar el archivo ejecutable (por ejemplo, *Backup-tool.exe*), que se excluirá del análisis.
En cuanto el archivo *.exe* se añada a las exclusiones, ESET Server Security no supervisará la actividad de este proceso y no se realizará ningún análisis en las operaciones del archivo llevadas a cabo por este proceso.

IMPORTANTE
Si no utiliza la función de examen al seleccionar el archivo ejecutable del proceso, debe introducir manualmente una ruta de acceso completa al archivo ejecutable. De lo contrario, la exclusión no funcionará correctamente y es posible que HIPS informe de errores.



También puede **Editar** los procesos existentes o **Eliminar** dichos procesos de las exclusiones.

NOTA
La protección del acceso a la Web no tiene en cuenta esta exclusión, por lo que si excluye el archivo ejecutable de su navegador web, los archivos descargados se seguirán analizando. De esta forma pueden detectarse las amenazas. Esta situación tiene meramente fines ilustrativos, y no se recomienda crear exclusiones para los navegadores web.

Protección en la nube

ESET LiveGrid® es un sistema avanzado de alerta temprana compuesto por varias tecnologías basadas en la nube. Ayuda a detectar las amenazas emergentes según su reputación y mejora el rendimiento de análisis mediante la creación de listas blancas. La nueva información sobre la amenaza se transmite en tiempo real a la nube, lo que permite que el laboratorio de investigación de malware de ESET responda a tiempo y mantenga una protección constante en todo momento. Los usuarios pueden consultar la reputación de los archivos y procesos en ejecución directamente en el menú contextual o en la interfaz del programa; además, disponen de información adicional en ESET LiveGrid®.

Seleccione una de las siguientes opciones durante la instalación de ESET Server Security:

- La activación de ESET LiveGrid® no es obligatoria. El software no perderá funcionalidad, pero puede que ESET Server Security responda más lento a las nuevas amenazas que la actualización de la base de datos del motor de detección.

- Puede configurar ESET LiveGrid® para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso detectado. Este archivo se puede enviar a ESET para que realice un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar sus funciones de detección de amenazas.

ESET LiveGrid® recopilará información anónima del ordenador relacionada con las amenazas detectadas recientemente. Esta información puede incluir una muestra o copia del archivo donde haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la fecha y la hora, el proceso por el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

De forma predeterminada, ESET Server Security está configurado para enviar archivos sospechosos al laboratorio de virus de ESET para su análisis. Los archivos con determinadas extensiones, como *.docx* o *.xlsx*, se excluyen siempre. También puede agregar otras extensiones para excluir los archivos que usted o su empresa no deseen enviar.

Activar el sistema de reputación ESET LiveGrid® (recomendado)

El sistema de reputación ESET LiveGrid® mejora la eficiencia de las soluciones contra malware de ESET mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.

Activar el sistema de respuesta ESET LiveGrid®

Los datos se enviarán al laboratorio de investigación de ESET para su posterior análisis.

Enviar informes de bloqueo y datos de diagnóstico

Se envían datos como informes de bloqueo, datos de módulos o volcados de memoria.

Enviar estadísticas anónimas

Permita que ESET recopile información sobre nuevas amenazas detectadas (nombre de la amenaza, información sobre la fecha y hora en la que se detectó, el método de detección y los metadatos asociados), archivos analizados (hash, nombre y origen del archivo, telemetría), direcciones URL bloqueadas y sospechosas y la versión y la configuración del producto, además de información sobre el sistema.

Correo electrónico de contacto (opcional)

Su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

Envío de muestras

Envío automático de muestras infectadas

Si activa esta opción, enviará a ESET todas las muestras infectadas para que las analice y mejore la detección futura.

- Todas las muestras infectadas
- Todas las muestras excepto los documentos
- No enviar

Envío automático de muestras sospechosas

Las muestras sospechosas que por su comportamiento o características inusuales recuerdan a amenazas se envían a ESET para su análisis.

- **Ejecutable**: incluye archivos ejecutables (*.exe, .dll, .sys*)
- **Archivos comprimidos**: incluye tipos de archivos comprimidos (*.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*)

- **Scripts**: incluye tipos de archivos con script (*.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.js*, *.ps1*)
- **Otros**: incluye otros tipos de archivos (*.jar*, *.reg*, *.msi*, *.swf*, *.lnk*)
- **Correos electrónicos con posible spam**: mejora la detección global del spam.
- **Documentos**: incluye documentos de Microsoft Office o documentos PDF con contenido activo.

Exclusiones

Haga clic en la opción Editar junto a Exclusiones en ESET LiveGrid® para configurar el modo de envío de las amenazas al laboratorio de virus de ESET para su análisis.

Tamaño máximo de las muestras

Le permite definir el tamaño máximo de las muestras que se analizarán.

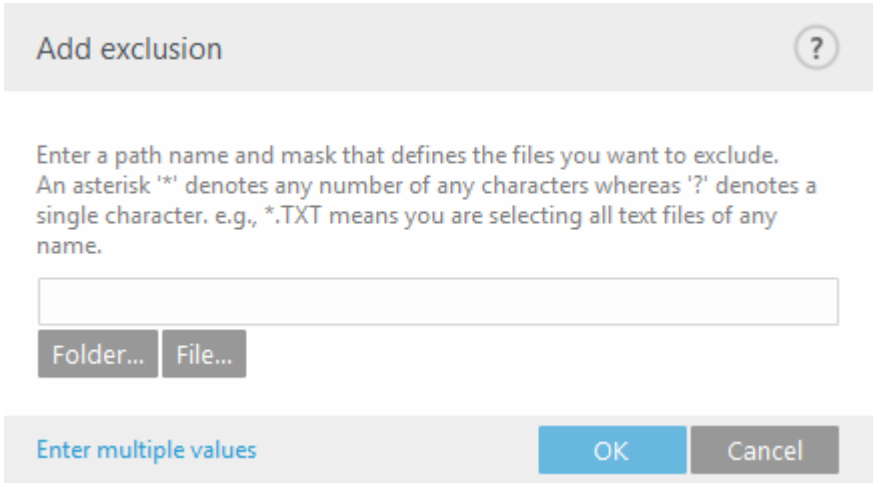
ESET Dynamic Threat Defense

Para activar el servicio ESET Dynamic Threat Defense en un equipo cliente con ESET PROTECT Web Console. En ESET PROTECT Web Console, cree una política nueva o edite una existente y asígnela a los equipos en los que quiera usar ESET Dynamic Threat Defense.

Filtro de exclusión

Esta opción le permite excluir del envío determinados archivos o carpetas (por ejemplo, puede ser útil excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivos más comunes se excluyen de manera predeterminada (*.doc*, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Si utilizó ESET LiveGrid® anteriormente pero lo desactivó, es posible que aún haya paquetes de datos pendientes de envío. Estos paquetes se enviarán a ESET incluso después de la desactivación. Una vez que se haya enviado toda la información actual, no se crearán más paquetes.



Si encuentra un archivo sospechoso, puede enviarlo a nuestros laboratorios para su análisis. Si resulta ser una

aplicación maliciosa, su detección se agregará a la siguiente actualización de módulo de detección.

Análisis de malware

En esta sección se ofrecen opciones para seleccionar parámetros de análisis.

> NOTA
> Este selector de perfiles de análisis se aplica al **Análisis a petición**, al análisis Hyper-V y al análisis OneDrive.

Perfil seleccionado

Un conjunto concreto de parámetros utilizado por el Análisis a petición. Puede utilizar uno de los perfiles de análisis predefinidos o crear uno nuevo. Los perfiles de análisis utilizan distintos parámetros del motor ThreatSense.

Lista de perfiles

Para crear uno nuevo, haga clic en **Editar**. Escriba el nombre del perfil y haga clic en **Agregar**. El nuevo perfil aparecerá en el menú desplegable **Perfil seleccionado** que muestra los perfiles de análisis existentes.

Objetos del análisis

Si desea analizar un objeto específico, puede hacer clic en **Editar** y seleccionar una opción en el menú desplegable o elegir objetos específicos de la estructura de carpetas (árbol).

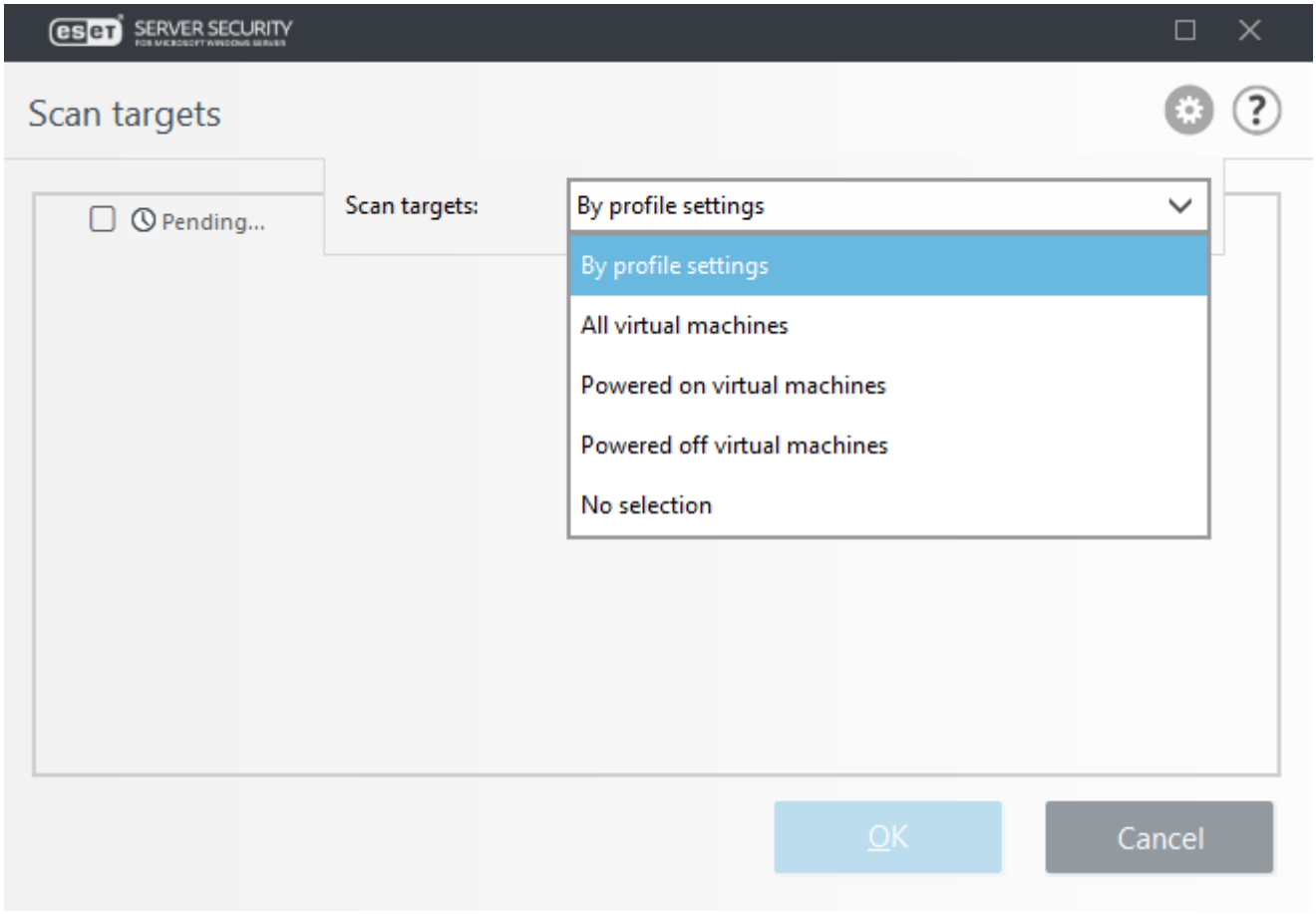
Parámetros de ThreatSense

Modifique los parámetros de análisis del Análisis a petición del ordenador.

Protección a petición y de aprendizaje automático

Los informes los realizan el motor de detección y el componente de aprendizaje automático.

La ventana emergente **Análisis Hyper-V**:



En el menú desplegable **Objetos de análisis** de **Hyper-V** puede seleccionar objetos predefinidos para el análisis:

Parámetros según perfil	Selecciona los objetos definidos en el perfil de análisis seleccionado.
Todas las máquinas virtuales	Selecciona todas las máquinas virtuales.
Máquinas virtuales encendidas	Selecciona todas las máquinas virtuales que están conectadas.
Máquinas virtuales apagadas	Selecciona todas las máquinas virtuales que están apagadas.
Sin selección	Borra todas las selecciones.

Haga clic en **Analizar** para ejecutar el análisis con los parámetros personalizados que ha definido. Una vez finalizados todos los análisis, marque **Archivos de registro** > Análisis Hyper-V.

Administrador de perfiles

El menú desplegable **Perfil de análisis** le permite seleccionar perfiles de análisis predefinidos.

- **Análisis estándar**
- **Análisis del menú contextual**
- **Análisis exhaustivo**
- **Mi perfil** (se aplica a Análisis Hyper-V, Perfiles de actualización y Análisis de OneDrive)

Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte el apartado Configuración de parámetros del motor ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

El Administrador de perfiles se usa en tres componentes de ESET Server Security.

Análisis del ordenador

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Actualización

El editor de perfil permite a los usuarios crear nuevos perfiles de actualización. Solo se deben crear perfiles de actualización personalizados si su ordenador utiliza varios métodos para conectarse a los servidores de actualización.

Análisis Hyper-V

Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**. El nuevo perfil aparecerá en el menú desplegable **Perfil seleccionado**, en el que se muestran los perfiles de análisis existentes.

Análisis de OneDrive

Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**. El nuevo perfil aparecerá en el menú desplegable **Perfil seleccionado**, en el que se muestran los perfiles de análisis existentes.

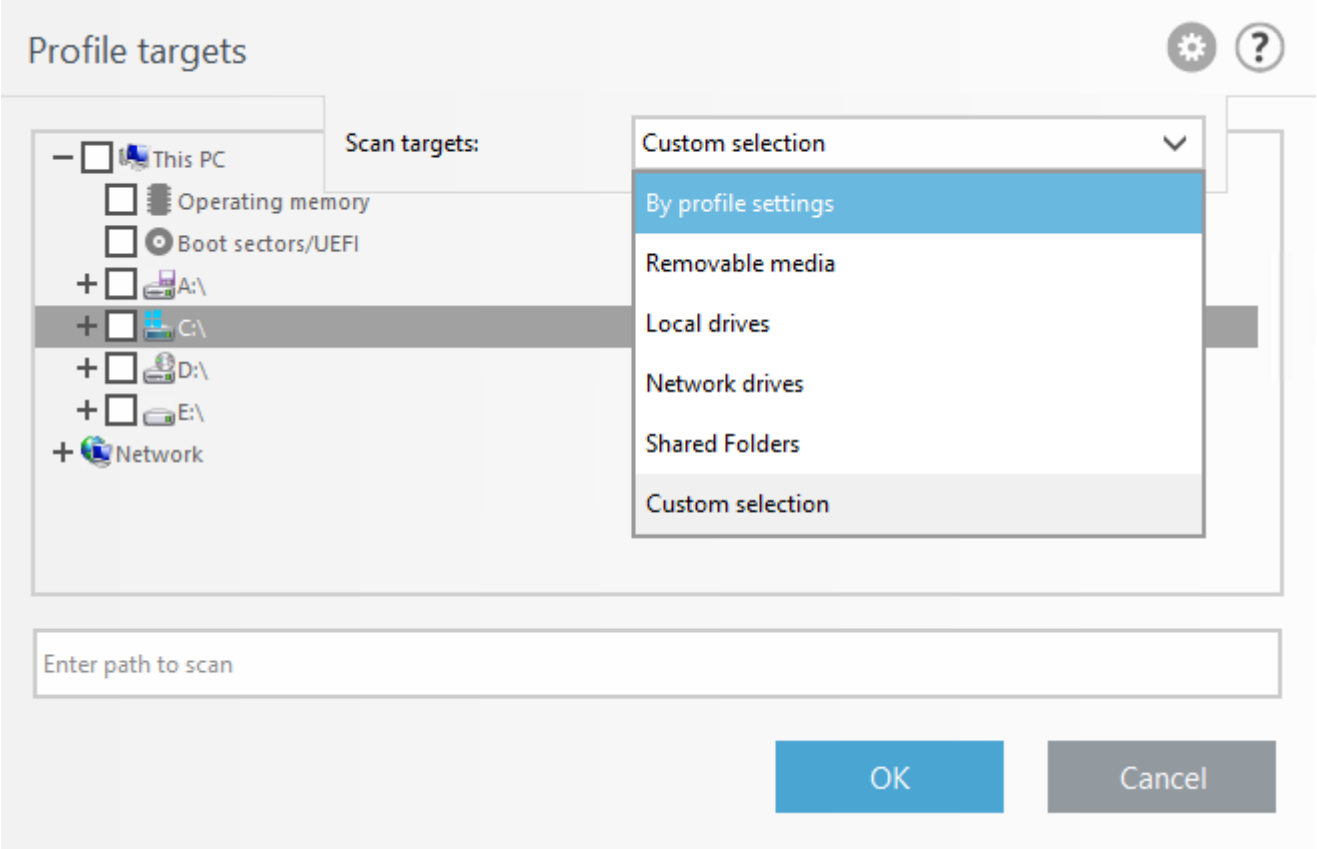
Objetos de perfil

Puede especificar qué se analizará en busca de amenazas. Elija objetos (memoria, sectores de inicio y UEFI, unidades, archivos o carpetas o red) en la estructura de árbol en la que se muestran todos los objetos disponibles en su sistema. Haga clic en el icono del engranaje situado en la esquina superior izquierda para acceder a los menús desplegables **Objetos de análisis** y **Perfil de análisis**.

> NOTA
> Este selector de perfiles de análisis se aplica al **Análisis a petición**, al análisis Hyper-V y al análisis OneDrive.

Memoria operativa	**Analiza todos los procesos y datos que utiliza en ese momento la memoria operativa.**
Sectores de inicio/UEFI	Analiza los sectores de inicio y la UEFI en busca de malware. Puede obtener más información sobre el análisis UEFI en el glosario.
Base de datos de WMI	Analiza toda la base de datos de Instrumental de administración de Windows (WMI), todos los espacios de nombres, todas las instancias de clase y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
Registro del sistema	Analiza todo el registro del sistema, todas las claves y las subclaves. Busca referencias a archivos infectados o malware incrustados como datos. Durante la desinfección de las detecciones, la referencia permanece en el registro para que no se pierda ningún dato importante.

Para ir rápidamente a un objeto de análisis o agregar una carpeta o un archivo de destino, introduzca el directorio de destino en el campo en blanco situado debajo de la lista de carpetas.



En el menú desplegable **Objetos de análisis** puede seleccionar un objetos de análisis predefinido:

Parámetros según perfil	**Selecciona los objetos definidos en el perfil de análisis seleccionado.**
Medios extraíbles	Selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
Unidades locales	Selecciona todas las unidades de disco del sistema.
Unidades de red	Selecciona todas las unidades de red asignadas.
Carpetas compartidas	Selecciona todas las carpetas compartidas del servidor local.
Selección personalizada	Borra todas las selecciones. Una vez borradas, puede realizar su selección personalizada.

Para ir rápidamente a un objeto de análisis (archivo o carpeta) e incluirlo en el análisis, especifique su ruta en el campo de texto situado debajo de la estructura de árbol. A la hora de introducir la ruta se distinguen las mayúsculas de las minúsculas.

En el menú desplegable **Perfil de análisis** puede seleccionar perfiles de análisis predefinidos:

- **Análisis estándar**
- **Análisis del menú contextual**
- **Análisis exhaustivo**

Estos perfiles de análisis emplean parámetros distintos del motor de ThreatSense.

Analizar sin desinfectar

Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Esta opción resulta útil cuando solo quiere obtener una visión general de si hay elementos infectados y obtener información detallada sobre dichas infecciones, en caso de haber alguna. Puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración** > **Parámetros de**

ThreatSense > **Desinfección**. La información sobre el análisis se guarda en un registro de análisis.

Ignorar exclusiones

Cuando selecciona **Ignorar exclusiones**, le permite realizar un análisis ignorando las exclusiones que de otro modo se aplicarían.

Objetos del análisis

Si desea analizar un objeto específico, puede elegir **Análisis personalizado** y seleccionar una opción en el menú desplegable **Objetos de análisis**, o seleccionar objetos concretos en la estructura de carpetas (árbol).

El selector de perfiles de objetos del análisis se aplica a:

- Análisis a petición
- Análisis Hyper-V
- Análisis de OneDrive

Para acceder rápidamente a un objeto de análisis o agregar una nueva carpeta o un nuevo archivo de destino, introdúzcalo en el campo en blanco disponible debajo de la lista de carpetas. Si no se ha seleccionado ningún objeto en la estructura de árbol y el menú **Objetos a analizar** está definido en **Sin selección**, no podrá hacerlo.

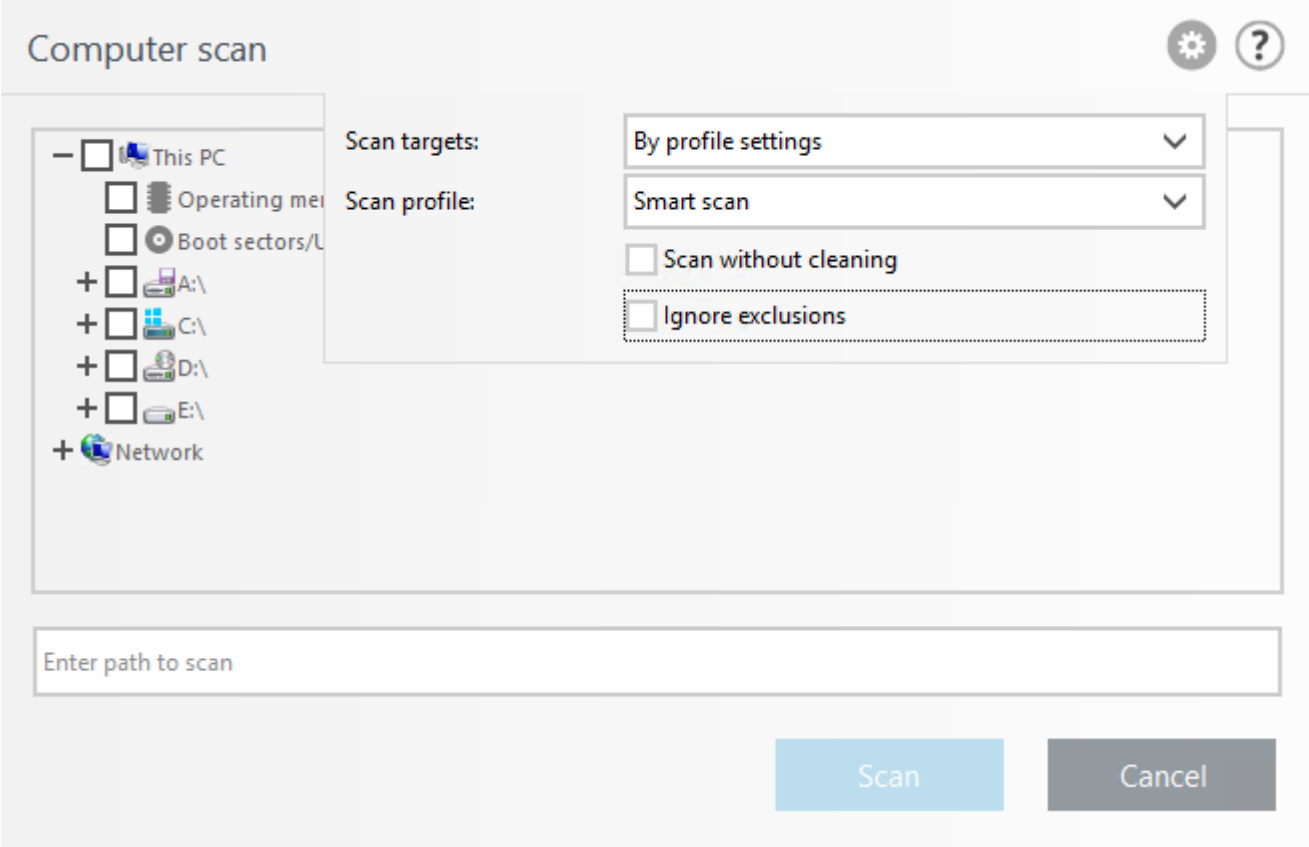
Memoria operativa	**Analiza todos los procesos y datos que utiliza en ese momento la memoria operativa.**
Sectores de inicio/UEFI	Analiza los sectores de inicio y la UEFI en busca de malware. Puede obtener más información sobre el análisis UEFI en el glosario.
Base de datos de WMI	Analiza toda la base de datos de Instrumental de administración de Windows (WMI), todos los espacios de nombres, todas las instancias de clase y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
Registro del sistema	Analiza todo el registro del sistema, todas las claves y las subclaves. Busca referencias a archivos infectados o malware incrustados como datos. Durante la desinfección de las detecciones, la referencia permanece en el registro para que no se pierda ningún dato importante.

En el menú desplegable **Objetos de análisis** puede seleccionar objetos predefinidos para el análisis.

Parámetros según perfil	**Selecciona los objetos definidos en el perfil de análisis seleccionado.**
Medios extraíbles	Selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
Unidades locales	Selecciona todas las unidades de disco del sistema.
Unidades de red	Selecciona todas las unidades de red asignadas.
Carpetas compartidas	Selecciona todas las carpetas compartidas del servidor local.
Selección personalizada	Borra todas las selecciones. Una vez borradas, puede realizar su selección personalizada.

Puede elegir un perfil en el menú desplegable **Perfil** de análisis para usarlo para el análisis de los objetos de análisis elegidos. El perfil predeterminado es el **Análisis inteligente**. Hay dos perfiles de análisis predefinidos más, denominados **Análisis exhaustivo** y **Análisis del menú contextual**. Estos perfiles de análisis usan parámetros distintos del motor de ThreatSense.

La ventana emergente **Análisis personalizado**:



Analizar sin desinfectar

Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Esta opción resulta útil cuando solo quiere obtener una visión general de si hay elementos infectados y obtener información detallada sobre dichas infecciones, en caso de haber alguna. Puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración** > **Parámetros de ThreatSense** > **Desinfección**. La información sobre el análisis se guarda en un registro de análisis.

Ignorar exclusiones

Puede realizar un análisis ignorando las exclusiones que de otro modo se aplicarían.

Analizar

Para ejecutar el análisis con los parámetros personalizados que ha definido.

Analizar como administrador

Le permite ejecutar el análisis con la cuenta de administrador. Haga clic en esta opción si el usuario actual no tiene privilegios para acceder a los archivos que se deben analizar. Observe que este botón no está disponible si el usuario actual no puede realizar operaciones de UAC como administrador.

Análisis en estado inactivo

Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis del ordenador silencioso de todos los discos locales. La **detección de estado inactivo** se ejecutará cuando el ordenador se encuentre en uno de los estados siguientes:

- **Pantalla apagada o con protector de pantalla**
- **Bloqueo de equipo**
- **Cierre de sesión de usuario**

Ejecutar aunque el ordenador esté funcionando con la batería

De forma predeterminada, el análisis de estado inactivo no se ejecutará si el ordenador (portátil) está funcionando con batería.

Activar el registro de sucesos

Para guardar un informe del análisis del ordenador en la sección Archivos de registro (en la ventana principal del programa, haga clic en Archivos de registro y seleccione el tipo de registro Análisis del ordenador en el menú desplegable).

Parámetros de ThreatSense

Le permite modificar los parámetros de análisis del análisis en estado inactivo.

Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema (inicio de sesión del usuario) o después de una actualización de módulo correcta. Este análisis se controla mediante la Configuración y las tareas de Tareas programadas.

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos en el inicio del sistema** de Tareas programadas.

Para modificar la configuración del análisis en el inicio, seleccione **Herramientas** > **Tareas programadas**, seleccione la tarea denominada **Verificación automática de los archivos de inicio** (inicio de sesión del usuario o actualización de módulo) y haga clic en **Editar**. Si hace clic en el asistente y en el último paso, puede modificar las opciones detalladas de la Verificación automática de los archivos de inicio.

Verificación automática de los archivos de inicio

Al crear una tarea programada de comprobación de archivos en el inicio del sistema tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable Objetos a analizar especifica la profundidad del análisis para los archivos que se ejecutan al iniciar el sistema. Los archivos se organizan en orden ascendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrados** (se analiza el mayor número de archivos)
- **Archivos usados pocas veces**
- **Archivos usados ocasionalmente**
- **Archivos usados frecuentemente**
- **Solo los archivos de uso más frecuente** (se analiza el menor número de archivos)

También se incluyen dos grupos específicos de Objetos a analizar:

Archivos ejecutados antes del inicio de sesión del usuario

Contiene archivos de ubicaciones a las que se puede tener acceso sin que el usuario haya iniciado sesión (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, notificación del registro de Windows, entradas de Tareas programadas de Windows, archivos dll conocidos, etc.).

Archivos ejecutados tras el inicio de sesión del usuario

Contiene archivos de ubicaciones a las que solo se puede tener acceso cuando el usuario inicia sesión (incluye archivos que solo ejecuta un usuario concreto, generalmente los archivos de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se analizan son fijas para cada uno de los grupos anteriores.

Prioridad del análisis

El nivel de prioridad empleado para determinar cuándo se iniciará un análisis:

- **Normal**: con carga media del sistema.
- **Baja**: con poca carga del sistema.
- **Muy baja**: cuando la carga del sistema es la más baja posible.
- **Cuando se encuentra inactivo**: la tarea se ejecutará solo cuando el sistema esté inactivo.

Medios extraíbles

ESET Server Security permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática. Este módulo le permite analizar un medio insertado. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Acción a realizar después de insertar medios extraíbles

Seleccione la acción que se realizará cuando se inserte un dispositivo multimedia extraíble en el ordenador (CD/DVD/USB).

- **No analizar**: no se realizará ninguna acción y se cerrará la ventana **Nuevo dispositivo detectado**.
- **Análisis automático del dispositivo**: se realizará un análisis del ordenador a petición del medio extraíble insertado.
- **Mostrar las opciones de análisis**: abre la sección de configuración de medios extraíbles.

Cuando se inserta un medio extraíble aparece la siguiente ventana:

- **Analizar ahora** : activa el análisis del medio extraíble.
- **Analizar más adelante**: el análisis del medio extraíble se pospone.
- **Configuración**: abre la configuración avanzada.
- **Utilizar siempre la opción seleccionada**: cuando se seleccione esta opción, se realizará la misma acción la próxima vez que se introduzca un medio extraíble.

Además, ESET Server Security presenta funciones de control de dispositivos, lo que le permite definir reglas para el uso de dispositivos externos en un ordenador concreto. Encontrará más detalles sobre el control de dispositivos en la sección Control del dispositivo.

Protección de documentos

La característica de protección de documentos analiza los documentos de Microsoft Office antes de que se abran y los archivos descargados automáticamente con Internet Explorer como, por ejemplo, elementos de Microsoft ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección en tiempo real del sistema de archivos, y se puede desactivar para mejorar el rendimiento en sistemas que no están expuestos a un volumen elevado de documentos de Microsoft Office.

Integrar en el sistema

Esta opción mejora la protección de documentos de Microsoft Office (en circunstancias normales no es necesaria).

Parámetros de ThreatSense

Le permite modificar los parámetros de la protección de documentos.

> NOTA
> Esta función se activa mediante aplicaciones que utilizan la Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y superior, o Microsoft Internet Explorer 5.0 y superior).

Análisis Hyper-V

La versión actual del análisis Hyper-V permite el análisis de sistemas virtuales en línea o desconectados en Hyper-V. A continuación se indican los tipos de análisis admitidos según el sistema Hyper-V de Windows alojado y el estado del sistema virtual:

Sistemas virtuales con función Hyper-V	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
Máquina virtual en línea	Sin análisis	Solo lectura	Solo lectura	Solo lectura	Solo lectura
Máquina virtual desconectada	Solo lectura/desinfección	Solo lectura/desinfección	Solo lectura/desinfección	Solo lectura/desinfección	Solo lectura/desinfección

Requisitos de hardware

El servidor no debería experimentar ningún problema de rendimiento durante la ejecución de máquinas virtuales. La actividad de análisis utiliza principalmente recursos de la CPU. Para analizar máquinas virtuales en línea se necesita espacio libre en el disco. El espacio del disco debe ser como mínimo el doble del espacio utilizado por los puntos de comprobación o instantáneas y los discos virtuales.

Limitaciones concretas

- El análisis en almacenamiento RAID, volúmenes distribuidos y discos dinámicos no se admite debido a la naturaleza de los discos dinámicos. Por ello, le recomendamos que, siempre que sea posible, evite utilizar el tipo de disco dinámico en sus máquinas virtuales.

- El análisis se realiza siempre en la máquina virtual actual y no afecta a puntos de comprobación ni instantáneas.
- Actualmente, ESET Server Security no es compatible con Hyper-V en ejecución en un host de un clúster.
- Las máquinas virtuales de un host Hyper-V que se ejecutan en Windows Server 2008 R2 SP1 solo se pueden analizar en el modo de solo lectura (Sin desinfección), sea cual sea el nivel de desinfección seleccionado en los Parámetros de ThreatSense.

NOTA
Aunque ESET Security permite el análisis del registro de inicio principal (MBR) de los discos virtuales, el análisis de solo lectura es el único método admitido para estos objetos. Este ajuste puede modificarse en **Configuración avanzada+** (**F5**) > **Motor de detección** > **Análisis Hyper-V** > Parámetros de ThreatSense > **Sectores de inicio**.

La máquina virtual a analizar está fuera de línea (desconectada)

ESET Server Security utiliza la administración de Hyper-V para detectar y conectarse a los discos virtuales. De esta forma, ESET Server Security dispone del mismo acceso al contenido de los discos virtuales que si accediera a los datos y archivos de cualquier unidad genérica.

La máquina virtual a analizar está fuera de línea: En ejecución, En pausa, Guardada

ESET Server Security utiliza la administración de Hyper-V para detectar discos virtuales. No es posible conectarse a estos discos. Por ello, ESET Server Security crea un punto de control o una instantánea de la máquina virtual, y luego se conecta al punto de control o la instantánea. El punto de control o la instantánea se eliminan una vez finalizado el análisis. Esto significa que el análisis de solo lectura se puede realizar porque las máquinas virtuales en ejecución no se ven afectadas por la actividad de análisis.

Espere un minuto para que ESET Server Security cree una instantánea o un punto de comprobación durante el análisis. Debe tener esto en cuenta a la hora de ejecutar un análisis de Hyper-V en un mayor número de máquinas virtuales.

Convención de nomenclatura

El módulo de análisis Hyper-V utiliza la siguiente convención de nomenclatura:

```
VirtualMachineName\DiskX\VolumeY
```

Donde X es el número de discos e Y es el número de volúmenes. Por ejemplo:

```
Computer\Disk0\Volume1
```

El sufijo numérico se añade en función del orden de detección, y es idéntico al orden observado en el Administrador de discos de la máquina virtual. Esta convención de nomenclatura se utiliza en la lista de objetos estructurada en árbol para analizar, en la barra de progreso y también en los archivos de registro.

Ejecución de un análisis

- A petición: haga clic en **Análisis Hyper-V** para ver una lista de máquinas virtuales y volúmenes disponibles para el análisis. Seleccione las máquinas virtuales, los discos o los volúmenes que desee analizar y haga clic en **Analizar**.
- Para crear una tarea de Tareas programadas.

- Mediante ESET PROTECT como una tarea del cliente denominada Análisis del servidor.
- La opción Análisis Hyper-V puede gestionarse e iniciarse a través de eShell.

Pueden ejecutarse varios análisis Hyper-V simultáneamente. Recibirá una notificación con un enlace a los archivos de registro cuando finalice el análisis.

Posibles problemas

- Al ejecutar el análisis de una máquina virtual conectada, debe crearse un punto de control o una instantánea de la máquina virtual específica y, durante la creación de un punto de control o una instantánea, ciertas acciones genéricas de la máquina virtual pueden estar limitadas o desactivadas.
- Si se desea analizar una máquina virtual desconectada, no puede encenderla hasta que finalice el análisis.
- El Administrador de Hyper-V permite nombrar dos máquinas virtuales diferentes de forma idéntica y esto plantea un problema al intentar diferenciar las máquinas mientras se revisan los registros de análisis.

Análisis de OneDrive

Básico

Puede configurar las acciones y la cuarentena.

Acción que debe realizarse si el archivo está infectado:

- **Sin acción**: no se aplicarán cambios al archivo.
- **Eliminar**: realiza el traslado a la cuarentena y elimina los archivos de OneDrive. No obstante, los archivos seguirán estando disponibles en la papelera de reciclaje de OneDrive.

Archivos infectados en cuarentena

Cuando esta opción está activada, los archivos que se marquen para su eliminación se trasladarán a la cuarentena. Desactive este ajuste para desactivar la cuarentena y que los archivos no se acumulen en ella.

Avanzado

Este elemento contiene información sobre el registro de análisis de OneDrive (ID de la aplicación, ID de objeto en el portal de Azure, huella digital del certificado). Puede configurar los tiempos de espera y el límite de descargas simultáneas.

Perfiles

Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**, escriba su **Nombre de perfil** y haga clic en **Agregar**. El nuevo perfil aparecerá en el menú desplegable **Perfil seleccionado** que muestra los perfiles de análisis existentes.

En el menú desplegable **Objeto de análisis** puede seleccionar un objeto de análisis predefinido:

- **Por perfil**: selecciona los objetos definidos en el perfil de análisis seleccionado.

- **Todos los usuarios**: selecciona todos los usuarios.
- **Sin selección**: borra la selección actual.

Haga clic en **Analizar** para ejecutar el análisis con los parámetros personalizados que ha definido. Una vez finalizados todos los análisis, marque **Archivos de registro** > Análisis de OneDrive.

Parámetros de ThreatSense

Le permite modificar los parámetros de análisis de OneDrive.

Análisis de OneDrive y protección de aprendizaje automático

Los informes los realizan el motor de detección y el componente de aprendizaje automático.

HIPS

El Sistema de prevención de intrusiones del host (HIPS) protege el sistema frente a código malicioso o cualquier actividad no deseada que intente menoscabar la seguridad del ordenador. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos, solo supervisa los procesos que se ejecutan dentro del sistema operativo.

> ADVERTENCIA
> Solo debe modificar la configuración de HIPS si es un usuario experimentado. Una configuración incorrecta de los parámetros de HIPS puede provocar inestabilidad en el sistema.

Activar la Autodefensa

ESET Server Security tiene tecnología de Autodefensa integrada que impide que el software malicioso dañe o desactive su protección contra el malware, de modo que puede estar seguro de que su sistema está protegido en todo momento. Los cambios de los ajustes Activar HIPS y Activar la Autodefensa se aplican después de reiniciar el sistema operativo Windows. Para desactivar todo el sistema HIPS también es necesario reiniciar el ordenador.

Activar servicio protegido

Microsoft ha introducido un concepto de servicios protegidos con Microsoft Windows Server 2012 R2. Evita que un servicio sufra ataques de malware. El núcleo de ESET Server Security se ejecuta como un servicio protegido de forma predeterminada. Esta función está disponible en Microsoft Windows Server 2012 R2 y en los sistemas operativos de servidor más recientes.

Activar Advanced Memory Scanner

Funciona conjuntamente con el Bloqueador de exploits para aumentar la protección frente a malware que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos antimalware. El Advanced Memory Scanner está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

Activar bloqueo de exploits

Se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de

Internet, los lectores de archivos pdf, los clientes de correo electrónico y los componentes de MS Office. El Bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

Activar protección contra ransomware

Para utilizar esta función, active HIPS y ESET Live Grid. Obtenga más información sobre Ransomware en el glosario.

Modo de filtrado

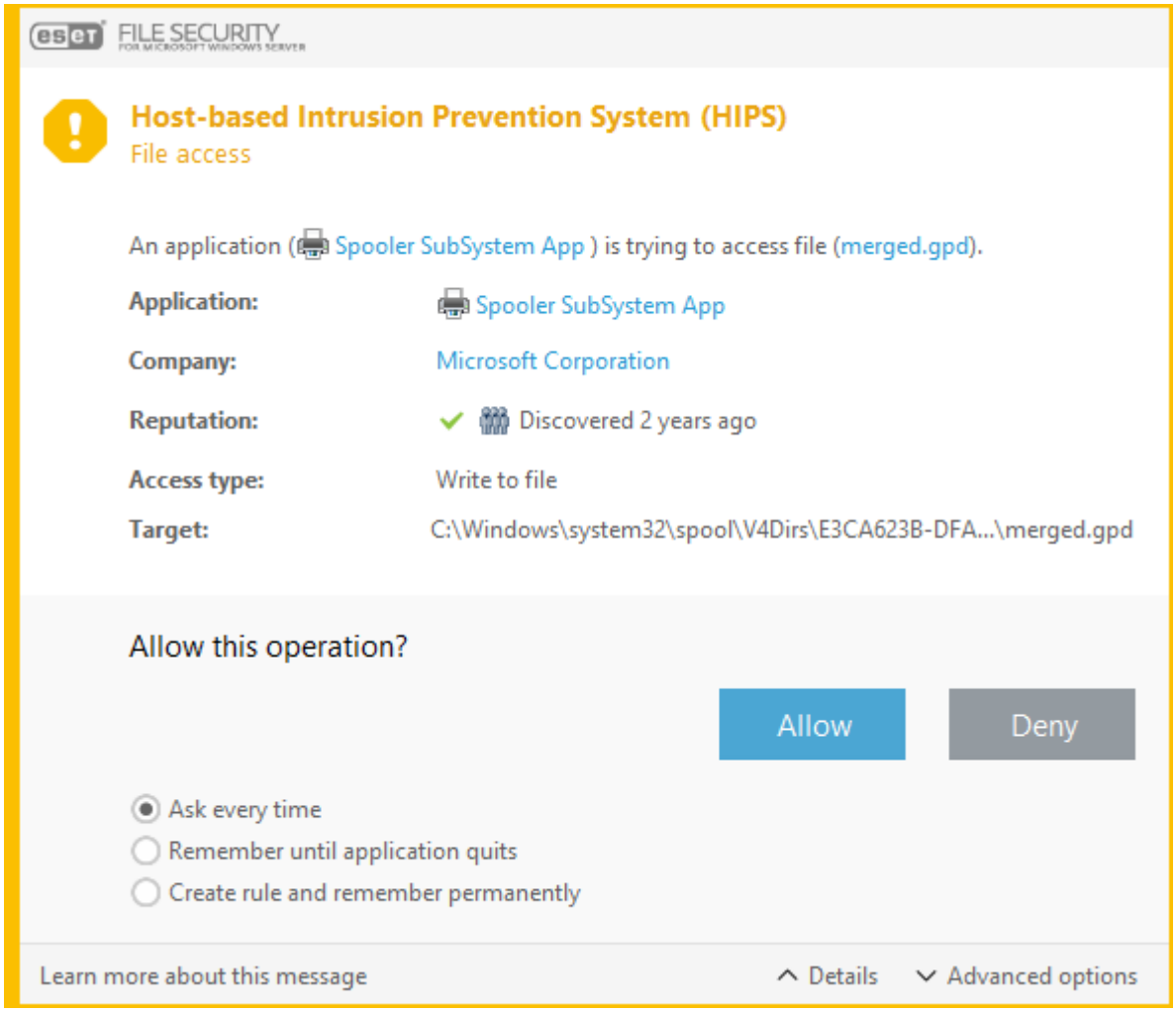
Puede elegir uno de los siguientes modos de filtrado:

- **Modo automático**: las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema. Se permiten todas las operaciones excepto las acciones denegadas por la regla.
- **Modo inteligente**: solo se informará al usuario de los sucesos muy sospechosos.
- **Modo interactivo**: el usuario debe confirmar las operaciones (Permitir/denegar acceso, Crear regla, Recordar temporalmente esta acción).
- **Modo basado en reglas**: las operaciones están bloqueadas. Solo acepta las reglas del usuario/predefinidas.
- **Modo de aprendizaje**: las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de reglas, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el **Modo de aprendizaje** en el menú desplegable del modo de filtrado de HIPS, el ajuste **El modo de aprendizaje finalizará a las** estará disponible. Seleccione el periodo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada se le pedirá que modifique las reglas creadas por el HIPS mientras estaba en el modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje.

Reglas

Las reglas determinan los archivos, partes del registro y aplicaciones a los que tienen acceso las diferentes aplicaciones. El sistema HIPS supervisa los sucesos del sistema operativo y reacciona de acuerdo con reglas similares a las que utiliza el cortafuegos personal. Haga clic en Editar para abrir la ventana de gestión de reglas de HIPS. Si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla. Puede seleccionar entre **Bloquear** o **Permitir** la operación. Si no selecciona una opción en el tiempo indicado, se aplican las reglas para seleccionar la nueva acción.

El cuadro de diálogo permite crear reglas de acuerdo con cualquier nueva acción que detecte HIPS y definir las condiciones en las que se **permite** o se **bloquea** dicha acción. Para ver más información, haga clic en **Detalles**. Las reglas creadas con este método se tratan igual que las creadas manualmente, por lo que una regla creada desde un cuadro de diálogo puede ser menos específica que la regla que activó dicho cuadro de diálogo. Esto significa que, después de crear esta regla, la misma operación puede activar la misma ventana.



Preguntar siempre

El cuadro de diálogo se mostrará cada vez que se desencadene dicha regla. Puede elegir entre **Denegar** y **Permitir** la operación.

Recordar hasta el cierre de la aplicación

Elegir la acción **Denegar** o **Permitir** creará una regla del HIPS temporal que se utilizará hasta que se cierre la aplicación en cuestión. Además, si cambia el modo de filtrado, modifica las reglas o se actualiza el módulo del HIPS y reinicia el sistema, las reglas temporales se eliminarán.

Crear regla y recordar permanentemente

Cree una nueva regla del HIPS. Puede modificarla posteriormente en la sección de gestión de reglas del HIPS.

Configuración de regla de HIPS

En esta ventana se muestra una descripción general de las reglas de HIPS existentes.

Regla	Nombre de la regla definido por el usuario o seleccionado automáticamente.
Activado	Desactive este conmutador si desea conservar la regla en la lista pero no quiere utilizarla.
Acción	La regla especifica una acción: **Permitir**, **Bloquear** o **Preguntar** que debe realizarse cuando se cumplen las condiciones.

Regla	Nombre de la regla definido por el usuario o seleccionado automáticamente.
Orígenes	La regla solo se utilizará si una aplicación activa el suceso.
Destinos	La regla solo se usará si la operación está relacionada con un archivo, una aplicación o una entrada del registro específicos.
Nivel de registro	Si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.
Notificar	Cuando se activa un suceso se abre una ventana emergente pequeña en la esquina inferior derecha.

Cree una nueva regla; haga clic en **Agregar** nuevas reglas de HIPS o en **Editar** las entradas seleccionadas.

Nombre de la regla

Nombre de la regla definido por el usuario o seleccionado automáticamente.

Acción

La regla especifica una acción: **Permitir**, **Bloquear** o **Preguntar** que debe realizarse cuando se cumplen las condiciones.

Operaciones afectadas

Debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se utilizará para este tipo de operación y para el destino seleccionado. La regla consta de partes que describen las condiciones que activan esta regla.

Aplicaciones de origen

La regla solo se utilizará si esta aplicación activa el suceso. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

> NOTA
> Algunas operaciones de reglas específicas predefinidas por HIPS no se pueden bloquear y se admiten de forma predeterminada. Además, HIPS no supervisa todas las operaciones del sistema, sino que supervisa las operaciones que considera peligrosas.

Descripción de las operaciones importantes:

Operaciones del archivo:

Eliminar archivo	La aplicación solicita permiso para eliminar el archivo objetivo.
Escribir en archivo	La aplicación solicita permiso para escribir en el archivo objetivo.
Acceso directo al disco	La aplicación está intentando realizar una operación de lectura o escritura en el disco de una forma no convencional que burlará los procedimientos habituales de Windows. Esto puede provocar la modificación de archivos sin la aplicación de las reglas correspondientes. Esta operación puede estar provocada por un malware que intente evadir el sistema de detección, un software de copia de seguridad que intente realizar una copia exacta de un disco o un gestor de particiones que intente reorganizar los volúmenes del disco.
Instalar enlace global	Hace referencia a la invocación de la función SetWindowsHookEx desde la biblioteca MSDN.
Cargar controlador	Instalación y carga de controladores en el sistema.

La regla solo se utilizará si la operación está relacionada con este objeto. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas. Además, puede seleccionar **Todos los archivos** en el menú desplegable para agregar todas las aplicaciones.

Operaciones de la aplicación:

Depurar otra aplicación	Conecta un depurador al proceso. Durante el proceso de depuración de una aplicación es posible ver y modificar muchos aspectos de su comportamiento, así como acceder a sus datos.
Interceptar sucesos de otra aplicación	La aplicación de origen está intentando capturar sucesos dirigidos a una aplicación concreta (por ejemplo un registrador de pulsaciones que intenta capturar sucesos del navegador).
Finalizar/suspender otra aplicación	Suspende, reanuda o termina un proceso (se puede acceder a esta operación directamente desde el Process Explorer o la ventana Procesos).
Iniciar una aplicación nueva	Inicio de aplicaciones o procesos nuevos.
Modificar el estado de otra aplicación	La aplicación de origen está intentando escribir en la memoria de la aplicación de destino o ejecutar código en su nombre. Esta función puede ser de utilidad para proteger una aplicación fundamental mediante su configuración como aplicación de destino en una regla que bloquee el uso de esta operación.

La regla solo se utilizará si la operación está relacionada con este objeto. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas. Además, puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Operaciones del registro:

Modificar la configuración de inicio	Cambios realizados en la configuración que definan las aplicaciones que se ejecutarán al iniciar Windows. Estos cambios se pueden buscar, por ejemplo, si se busca la clave en el Registro de Windows.
Eliminar del registro	Elimina una clave del registro o su valor.
Cambiar nombre de la clave del registro	Cambia el nombre de las claves del registro.
Modificar el registro	Crea valores nuevos para las claves del registro, modifica los valores existentes, mueve los datos en el árbol de la base de datos o configura los permisos de usuarios y grupos en las claves del registro.

La regla solo se utilizará si la operación está relacionada con este objetivo. Seleccione **Entradas específicas** del menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas. Además, puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

> NOTA
> Puede utilizar comodines, con determinadas restricciones, para especificar un destino. En las rutas de acceso al registro se puede utilizar el símbolo * (asterisco) en vez de una clave determinada. Por ejemplo *HKEY_USERS*\software can mean HKEY_USER\.default\software*, pero no *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software. HKEY_LOCAL_MACHINE\system\ControlSet** no es una ruta válida para la clave del registro. Una ruta de la clave del registro que tenga * incluye "esta ruta, o cualquier ruta de cualquier nivel después del símbolo". Este es el único uso posible de los comodines en los destinos. Primero se evalúa la parte específica de una ruta de acceso y, después, la ruta que sigue al comodín (*).

ADVERTENCIA
Puede recibir una notificación si crea una regla demasiado genérica.

Configuración avanzada del HIPS

Las opciones siguientes son útiles para depurar y analizar el comportamiento de una aplicación:

Controladores con carga siempre autorizada

Los controladores seleccionados pueden cargarse siempre sea cual sea el modo de filtrado configurado, a menos que la regla del usuario los bloquee de forma explícita. Los controladores que aparezcan en esta lista podrán cargarse siempre, sea cual sea el modo de filtrado del HIPS, a menos que una regla del usuario los bloquee de forma explícita. Puede **Agregar** nuevo controlador, **Editar** o **Eliminar** el controlador seleccionado de la lista.

NOTA
haga clic en **Restablecer** si no desea incluir los controladores que ha agregado manualmente. Esto puede resultar útil si ha agregado varios controladores y no puede eliminarlos de la lista manualmente.

Registrar todas las operaciones bloqueadas

Todas las operaciones bloqueadas se anotarán en el registro de HIPS.

Notificar cuando se produzcan cambios en las aplicaciones de inicio

Muestra una notificación en el escritorio cada vez que se agrega o se elimina una aplicación del inicio del sistema.

Actualizar configuración

En esta sección se indica información de origen de actualización como los servidores de actualización en uso y los datos de autenticación para estos servidores.

NOTA
Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente todos los parámetros de actualización. Si utiliza un cortafuegos, asegúrese de que su programa de ESET tiene permiso para comunicarse con Internet (por ejemplo, comunicación HTTP).

Básico

Seleccionar perfil de actualización predeterminado

Elija un perfil existente o cree uno nuevo que se aplicará de forma predeterminada durante las actualizaciones.

Borrar caché de actualización

Si tiene problemas con la actualización, haga clic en el botón **Borrar** para vaciar la caché de actualización temporal.

Establecer automáticamente una antigüedad máxima para el motor de detección/Antigüedad máxima del motor de detección (días)

Le permite establecer el número máximo de días tras el cual el motor de detección se considerará desactualizado. El valor predeterminado es 7.

Reversión del módulo

Si sospecha que una nueva actualización del motor de detección o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente. ESET Server Security registra instantáneas del motor de detección y los módulos del programa para usarlas con la función Revertir. Para crear instantáneas del motor de detección, deje activada la opción **Crear instantáneas de módulo**.

Número de instantáneas almacenadas localmente

Define el número de instantáneas de módulo anteriores guardadas.

Perfiles

Para crear un perfil de actualización personalizado, seleccione **Editar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**. **Seleccione el perfil que desea modificar** y modifique los parámetros de los tipos de **actualizaciones de módulo** o cree un **Mirror de actualización**.

Actualizaciones

Seleccione el tipo de actualización que desee utilizar en el menú desplegable:

- **Actualización normal**: de forma predeterminada, el Tipo de actualización se establece en Actualización normal para garantizar que todos los archivos de actualización se descarguen automáticamente del servidor de ESET cuando la carga de red sea menor.
- **Actualización de prueba**: son actualizaciones que han sido sometidas a completas pruebas internas y en breve estarán disponibles para el público en general. Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. No obstante, la actualización de prueba no siempre es estable, por lo que NO debe utilizarse en servidores de producción y estaciones de trabajo que requieran un elevado nivel de disponibilidad y estabilidad.
- **Actualización demorada**: permite actualizar desde servidores de actualización especiales que ofrecen nuevas versiones de bases de firmas de virus con un retraso de al menos X horas (es decir, de bases de firmas comprobadas en un entorno real y que, por lo tanto, se consideran estables).

Preguntar antes de descargar la actualización

Cuando esté disponible una nueva actualización, se le preguntará antes de descargarla.

Preguntar si un archivo de actualización es mayor de (kB)

Si el tamaño del archivo de actualización es superior al valor especificado en el campo, se mostrará una notificación.

Desactivar la notificación de actualización correcta

Desactiva la notificación de la bandeja del sistema en la esquina inferior derecha de la pantalla. Seleccione esta opción si está ejecutando una aplicación a pantalla completa. Tenga en cuenta que el modo Presentación desactiva todas las notificaciones.

Actualizaciones del módulo

Las actualizaciones de módulo están establecidas en **Elegir automáticamente** de forma predeterminada. El servidor de actualización es la ubicación donde las actualizaciones se almacenan. Si utiliza un servidor ESET, le recomendamos que deje seleccionada la opción predeterminada.

Cuando se utiliza un servidor local HTTP, también conocido como Mirror, el servidor de actualización debe configurarse de la forma siguiente: ***http://computer_name_or_its_IP_address:2221***
Cuando se utiliza un servidor local HTTP con SSL, el servidor de actualización debe configurarse de la forma siguiente: *https://computer_name_or_its_IP_address:2221*
Cuando se utiliza una carpeta local compartida, el servidor de actualización debe configurarse de la forma siguiente: *computer_name_or_its_IP_address**shared_folder*

Activar actualizaciones más frecuentes de las firmas de detección

El motor de detección se actualizará en intervalos más breves. Desactivar esta opción puede afectar negativamente a la tasa de detección.

Permitir actualizaciones del módulo desde soportes extraíbles

Actualice desde un medio extraíble si contiene el servidor mirror creado. Cuando se selecciona la opción **Automático**, las actualizaciones se ejecutarán en segundo plano. Si quiere mostrar los cuadros de diálogo de actualización, seleccione **Preguntar siempre**.

Actualización de componentes del programa

Utilice el menú desplegable **Modo de actualización** para seleccionar cómo se aplicarán las actualizaciones de componentes del programa (PCU) y las micro actualizaciones de componentes del programa (µPCU) ESET Server Security cuando haya una nueva actualización disponible. Las actualizaciones de componentes suelen modificar las funciones existentes, pero también pueden incluir nuevas funciones y correcciones. En función del modo de actualización seleccionado, la actualización de componentes puede realizarse de forma automática sin intervención ni confirmación (si es necesario reiniciar, se le indicará). También puede seleccionar la opción de recibir una notificación antes de que se instalen las actualizaciones.

NOTA
En algunos casos, puede que sea necesario reiniciar el servidor después de la actualización de componentes.

Están disponibles los siguientes modos de actualización:

- **Preguntar antes de actualizar**: se le solicitará que confirme o rechace las actualizaciones del producto cuando estén disponibles. Esta es la opción predeterminada. Es posible que sea necesario reiniciar el servidor después de la actualización de los componentes.

- **Actualizar automáticamente**: las actualizaciones de componentes se descargarán e instalarán

automáticamente. Tenga en cuenta que podría ser necesario reiniciar el servidor.

• **No actualizar nunca**: las actualizaciones de componentes no se realizarán. Esta opción permite ejecutar las actualizaciones de los componentes de forma manual y reiniciar el servidor durante el periodo de mantenimiento programado.

IMPORTANTE
El modo de actualización automática reinicia el servidor de forma automática una vez finalizada la actualización de los componentes.

Opciones de conexión

Servidor proxy

Esta opción permite acceder a las opciones de configuración del servidor proxy de un perfil de actualización determinado. Haga clic en **Modo proxy** y seleccione una de las tres opciones siguientes:

• **No usar servidor proxy**: ESET Server Security no utilizará ningún servidor proxy al realizar las actualizaciones.

• **Usar la configuración global del servidor proxy**: se utilizará la configuración del servidor proxy especificada en **Configuración avanzada** (F5) > **Herramientas** > Servidor proxy.

• **Conexión a través de un servidor proxy**: utilice esta opción en el caso de que:

Para actualizar ESET Server Security es necesario utilizar un servidor proxy diferente al especificado en la configuración global (Herramientas > Servidor proxy). En este caso, será necesario especificar la configuración aquí: Dirección del Servidor proxy, Puerto de comunicación (3128 de forma predeterminada), Nombre de usuario y Contraseña del servidor proxy, si es necesario.
La configuración del servidor proxy no se ha definido globalmente, pero ESET Server Security se conectará a un servidor proxy para las actualizaciones.
El ordenador se conecta a Internet mediante un servidor proxy. La configuración se toma de Internet Explorer durante la instalación del programa; no obstante, si esta cambia (por ejemplo, al cambiar de proveedor de Internet), compruebe que la configuración del servidor proxy HTTP es correcta en esta ventana. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

NOTA
Los datos de autenticación, como el **Nombre de usuario** y la **Contraseña** sirven para acceder al servidor proxy. Rellene estos campos únicamente si es necesario introducir un nombre de usuario y una contraseña. Tenga en cuenta que en estos campos no debe introducir su contraseña y nombre de usuario de ESET Server Security, que únicamente debe proporcionar si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor proxy.

Usar conexión directa si el proxy no está disponible

Si un producto está configurado para utilizar un proxy HTTP y el proxy está inaccesible, el producto ignorará el proxy y se comunicará directamente con los servidores de ESET.

Recursos compartidos de Windows

Para realizar una actualización desde un servidor local en el que se ejecute Windows, es necesario autenticar cada conexión de red de forma predeterminada.

Conectarse a la LAN como

Para configurar su cuenta, seleccione una de las siguientes opciones:

- **Cuenta del sistema (predeterminado)**: utilice la cuenta del sistema para la autenticación. Normalmente no se realiza ningún proceso de autenticación si no se proporcionan datos en la sección de configuración de actualizaciones.
- **Usuario actual**: seleccione esta opción para garantizar que el programa se autentica con la cuenta de un usuario registrado en ese momento. El inconveniente de esta solución es que el programa no se puede conectar al servidor de actualizaciones si no hay ningún usuario registrado.
- **Usuario especificado**: seleccione esta opción para utilizar una cuenta de usuario específica para la autenticación. Utilice este método cuando falle la conexión predeterminada con la cuenta del sistema. Recuerde que la cuenta del usuario especificada debe tener acceso al directorio de archivos actualizados del servidor local. Si el usuario no tiene acceso, el programa no podrá establecer ninguna conexión ni descargar las actualizaciones.

ADVERTENCIA
Cuando se selecciona **Usuario actual** o **Usuario especificado**, puede producirse un error al cambiar la identidad del programa para el usuario deseado. Por este motivo, se recomienda que introduzca los datos de autenticación de la red local en la sección principal de configuración de actualizaciones, donde los datos de autenticación se deben introducir de la forma siguiente: *domain_name**user* (si es un grupo de trabajo, escriba *workgroup_name**name*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no es necesaria ninguna autenticación.

Desconectar del servidor tras la actualización

Para forzar la desconexión si una conexión al servidor permanece activa incluso después de descargar las actualizaciones.

Mirror de actualización

Las opciones de configuración del servidor Mirror local se encuentran en **Configuración avanzada** (F5) en la ficha **Actualización** > **Perfiles** > Mirror de actualización.

Reversión de actualización

Si hace clic en **Revertir**, deberá seleccionar un intervalo de tiempo en el menú desplegable que representa el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.

Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, no recomendamos que se seleccione esta opción.

La versión de la base de datos del motor de detección se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del ordenador local.

Tarea programada: Actualización

Si desea actualizar el programa desde dos servidores de actualización, es necesario crear dos perfiles de actualización diferentes. Así, si el primer servidor no descarga los archivos de actualización, el programa cambia al otro automáticamente. Esta función es útil para portátiles, por ejemplo, ya que normalmente se actualizan desde un servidor de actualización LAN local, aunque sus propietarios suelen conectarse a Internet utilizando otras redes. Por tanto, en caso de que el primer perfil falle, el segundo descargará automáticamente los archivos de actualización de los servidores de actualización de ESET.

EJEMPLO
Los siguientes pasos lo guiarán en una tarea para editar una **Actualización automática de rutina** existente.
1.En la pantalla principal de **Tareas programadas**, seleccione la tarea **Actualizar** con el nombre **Actualización automática de rutina** y haga clic en **Editar**, se abrirá el asistente de configuración.
2.Establezca la tarea de Tareas programadas que desea ejecutar, seleccione una de las siguientes opciones de repetición de la tarea para especificar cuándo quiere la ejecución de la tarea programada.
3.Si desea evitar que la tarea se ejecute cuando el sistema funciona con baterías (por ejemplo, con un SAI), haga clic en el conmutador situado junto a **No ejecutar la tarea si está funcionando con batería**.
4.Seleccione el perfil de actualización que desea utilizar para la actualización. Seleccione la acción que debe realizarse si se produce un error al ejecutar la tarea programada por cualquier motivo.
5.Haga clic en **Finalizar** para aplicar la tarea.

Mirror de actualización

Abrir ESET Server Security
Pulse F5 > Actualización > Perfiles > Mirror de actualización.

ESET Server Security le permite crear copias de los archivos de actualización que puede utilizar para actualizar otras estaciones de trabajo de la red. El uso de un "mirror": es conveniente realizar una copia de los archivos de actualización del entorno de red local, dado que no necesitan descargarse del servidor de actualización del proveedor varias veces ni que los descarguen todas las estaciones de trabajo. Las actualizaciones se descargan de manera centralizada en el servidor Repositorio local y, después, se distribuyen a todas las estaciones de trabajo para así evitar el riesgo de sobrecargar el tráfico de red. La actualización de estaciones de trabajo cliente desde un servidor Mirror optimiza el equilibrio de carga de la red y ahorra ancho de banda de la conexión a Internet.

Mirror de actualización

Crear mirror de actualización

Activa las opciones de configuración del Mirror.

Carpeta de almacenamiento

Haga clic en **Borrar** si desea cambiar una carpeta predeterminada y definida para almacenar archivos replicados *C:\ProgramData\ESET\ESET Security\mirror.* Haga clic en **Editar** para buscar una carpeta en el ordenador local o la carpeta de red compartida. Si es necesaria una autorización para la carpeta especificada, deberá especificar los datos de autenticación en los campos Nombre de usuario y Contraseña. Si la carpeta de destino seleccionada se encuentra en un disco de red que ejecuta los sistemas operativos Windows NT, 2000 o XP, el nombre de usuario y la contraseña especificados deben contar con privilegios de escritura para la carpeta seleccionada.

El nombre de usuario y la contraseña deben introducirse con el formato *Domain/User* o *Workgroup/User*. No olvide que debe introducir las contraseñas correspondientes.

Actualización de componentes del programa

Archivos

Durante la configuración del servidor Mirror puede especificar las versiones de idioma de las actualizaciones que desea descargar. Los idiomas seleccionados deben ser compatibles con el servidor Mirror configurado por el usuario.

Actualizar componentes automáticamente

Permite instalar funciones nuevas y actualizaciones de las funciones existentes. La actualización se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación. Después de instalar una actualización del producto que se ha instalado, puede que sea necesario reiniciar el ordenador.

Actualizar componentes ahora

Actualiza los componentes del programa a la versión más reciente.

Servidor HTTP

Puerto de servidor

El puerto predeterminado es 2221. Cambie este valor si utiliza otro puerto.

Autenticación

Define el método de autenticación utilizado para acceder a los archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**.

- Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña.
- La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados.
- La configuración predeterminada es **Ninguna** y concede acceso a los archivos de actualización sin necesidad de autenticación.

ADVERTENCIA
Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta Mirror debe encontrarse en el mismo ordenador que la instancia de ESET Server Security que vaya a crearla.

SSL para el servidor HTTP

Si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL), agregue el **Archivo de cadena de certificados** o genere un certificado autofirmado. Están disponibles los siguientes tipos de certificado: PEM, PFX y ASN. Para una mayor seguridad, puede utilizar el protocolo HTTPS para descargar los archivos de actualización. Resulta casi imposible hacer un seguimiento de las transferencias de datos y credenciales de inicio de sesión utilizando este protocolo.
La opción **Tipo de clave privada** está establecida de forma predeterminada en **Integrada** (y, por lo tanto, la

opción Archivo de clave privada está desactivada de forma predeterminada). Esto significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.

Opciones de conexión

Recursos compartidos de Windows

Para realizar una actualización desde un servidor local en el que se ejecute Windows, es necesario autenticar cada conexión de red de forma predeterminada.

Conectarse a la LAN como

Para configurar su cuenta, seleccione una de las siguientes opciones:

- **Cuenta del sistema (predeterminado)**: utilice la cuenta del sistema para la autenticación. Normalmente no se realiza ningún proceso de autenticación si no se proporcionan datos en la sección de configuración de actualizaciones.
- **Usuario actual**: seleccione esta opción para garantizar que el programa se autentica con la cuenta de un usuario registrado en ese momento. El inconveniente de esta solución es que el programa no se puede conectar al servidor de actualizaciones si no hay ningún usuario registrado.
- **Usuario especificado**: seleccione esta opción para utilizar una cuenta de usuario específica para la autenticación. Utilice este método cuando falle la conexión predeterminada con la cuenta del sistema. Recuerde que la cuenta del usuario especificada debe tener acceso al directorio de archivos actualizados del servidor local. Si el usuario no tiene acceso, el programa no podrá establecer ninguna conexión ni descargar las actualizaciones.

ADVERTENCIA
Cuando se selecciona **Usuario actual** o **Usuario especificado**, puede producirse un error al cambiar la identidad del programa para el usuario deseado. Por este motivo, se recomienda que introduzca los datos de autenticación de la red local en la sección principal de configuración de actualizaciones, donde los datos de autenticación se deben introducir de la forma siguiente: *domain_name**user* (si es un grupo de trabajo, escriba *workgroup_name**name*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no es necesaria ninguna autenticación.

Desconectar del servidor tras la actualización

Para forzar la desconexión si una conexión al servidor permanece activa incluso después de descargar las actualizaciones.

Protección contra los ataques de red

Activar la protección contra los ataques de red (IDS)

Esta opción le permite acceder a algunos de los servicios que se ejecutan en su ordenador desde la zona de confianza y activar o desactivar la detección de varios tipos de ataques y exploits que pueden utilizarse para dañar su ordenador.

Activar protección contra botnets

Detecta y bloquea la comunicación con servidores de control y comando maliciosos en función de los patrones habituales que suelen producirse cuando el ordenador está infectado y un bot intenta comunicarse.

Excepciones de IDS

Se puede considerar que las excepciones del Sistema de detección de intrusiones (IDS) son reglas de protección de la red. Haga clic en editar para definir las excepciones de IDS.

> NOTA
> Si su entorno ejecuta una red de alta velocidad (10 GbE o más), lea el artículo de la base de conocimiento para obtener información sobre el rendimiento de velocidad de la red y ESET Server Security.

Protección contra ataques de fuerza bruta

ESET Server Security inspecciona el contenido del tráfico de red y bloquea los intentos de ataques de adivinación de contraseñas.

Opciones avanzadas

Configure las opciones avanzadas de filtrado para detectar mejor los distintos tipos de ataques y vulnerabilidades que puede sufrir su ordenador.

Detección de intrusiones:

Protocolo SMB: detecta y bloquea varios problemas de seguridad del protocolo SMB.
Protocolo RPC: detecta y bloquea varias CVE del sistema en el sistema de llamada de procedimientos remotos desarrollado para el Entorno de computación distribuido (DCE).
Protocolo RDP: detecta y bloquea varias CVE en el protocolo RDP (consulte el procedimiento anterior).
Bloquear la dirección no segura una vez detectado el ataque: las direcciones IP que se han detectado como fuente de ataques se agregan a la lista negra para evitar la conexión durante un período de tiempo concreto.
Mostrar una notificación al detectar un ataque: activa las notificaciones en la bandeja del sistema en la esquina inferior derecha de la pantalla.
Mostrar notificaciones al recibir ataques que se aprovechen de fallos de seguridad: le alerta si se detectan ataques que se aprovechen de fallos de seguridad o si una amenaza intenta acceder al sistema de esta forma.

Inspección del paquete:

Permitir una conexión entrante para intercambio de admin en el protocolo de SMB: los intercambios administrativos (intercambios de admin) son los intercambios de red predeterminados que comparten particiones de disco duro (C$, D$...) del sistema de forma conjunta con la carpeta del sistema (ADMIN$). La desactivación de la conexión a los intercambios de admin debe mitigar un gran número de riesgos de seguridad. Por ejemplo, el gusano Conficker realiza ataques de diccionario para conectarse a los intercambios de admin.
Denegar dialectos SMB anteriores (no compatibles): le permite denegar sesiones SMB que utilicen un dialecto SMB no compatible con IDS. Los sistemas operativos actuales de Windows admiten los antiguos dialectos SMB gracias a la compatibilidad con sistemas operativos anteriores, tales como Windows 95. El atacante puede utilizar un dialecto antiguo en una sesión SMB con el fin de evadir la inspección del tráfico. Deniegue antiguos dialectos SMB si su ordenador no necesita compartir archivos (o utilice la comunicación SMB en general) con un ordenador que cuente con una versión antigua de Windows.
Denegar sesiones SMB sin extensiones de seguridad: se puede utilizar una mayor seguridad durante la negociación de la sesión SMB para proporcionar un mecanismo de autenticación más seguro que la autenticación Respuesta/desafío del administrador de LAN (LM). El esquema LM se considera una protección débil y no se recomienda su uso.
Permitir la comunicación con el servicio Security Account Manager: si desea obtener más información sobre este servicio, consulte [MS-SAMR].
Permitir la comunicación con el servicio Local Security Authority: si desea obtener más información sobre este servicio, consulte [MS-LSAD] y [MS-LSAT].
Permitir la comunicación con el servicio Remote Registry: si desea obtener más información sobre este servicio, consulte [MS-RRP].
Permitir la comunicación con el servicio Service Control Manager: si desea obtener más información sobre este servicio, consulte [MS-SCMR].
Permitir la comunicación con el servicio Server Service: si desea obtener más información sobre este servicio, consulte [MS-SRVS].
Permitir la comunicación con los otros servicios: otros servicios MSRPC.

Excepciones de IDS

Las excepciones del Sistema de detección de intrusiones (IDS) son, básicamente, reglas de protección de la red. Las excepciones se evalúan desde arriba hacia abajo. El editor de excepciones de IDS le permite personalizar el comportamiento de protección de la red según diversas excepciones del IDS. En primer lugar, se aplica la excepción de coincidencia para cada tipo de acción (Bloquear, Notificar, Registrar) por separado. **Primera/Arriba/Abajo/Última** le permite ajustar el nivel de prioridad de las excepciones. Para crear una excepción de IDS nueva, haga clic en **Agregar**. Haga clic en **Editar** para modificar una excepción de IDS existente, o en **Eliminar** para quitarla.

Seleccione el tipo **Alerta** en la lista desplegable. Especifique el **Nombre de la amenaza** y la **Dirección**. Examine hasta la **Aplicación** para la que desea crear la excepción. Especifique una lista de direcciones IP (IPv4 o IPv6) o subredes. Para varias entradas, utilice la coma como delimitador.

Configure la **Acción** para la excepción del IDS al seleccionar una de las opciones del menú desplegable (**Predeterminado**, **Sí**, **No**). Hágalo para cada tipo de acción (**Bloquear**, **Notificar**, **Registrar**).

> EJEMPLO
> Si desea que se muestre una notificación en caso de producirse una alerta de excepción del IDS, además de que se registre la hora del suceso, mantenga el tipo de acción **Bloquear Predeterminado** y, para los otros dos tipos de acción (**Notificar** y **Registrar**), seleccione **Sí** en el menú desplegable.

Lista negra temporal de direcciones IP

Le permite ver una lista de direcciones IP que se han detectado como fuente de los ataques y se han agregado a la lista negra para bloquear la conexión durante un período de tiempo concreto. Muestra las **Direcciones IP** que se han bloqueado.

Motivo del bloqueo

Muestra el tipo de ataque que se ha evitado de la dirección (por ejemplo, ataque al puerto de exploración TCP).

Tiempo de espera

Muestra la hora y la fecha de caducidad de la dirección en la lista negra.

Quitar/Quitar todo

Elimina la dirección IP seleccionada de la lista negra temporal antes de que caduque o elimina de forma inmediata todas las direcciones de la lista negra.

Agregar excepción

Agrega una excepción del cortafuegos en el filtrado de IDS para la dirección IP seleccionada.

Web y correo electrónico

Puede configurar el filtrado de protocolos, la protección del cliente de correo electrónico, la protección del acceso a la Web y la protección Anti-Phishing para proteger su servidor durante la comunicación por Internet.

Protección del cliente de correo electrónico

Controla toda la comunicación por correo electrónico, protege el ordenador frente al código malicioso y le permite seleccionar la acción que se realizará al detectar una amenaza.

Protección del tráfico de Internet

Supervisa la comunicación entre los navegadores web y los servidores remotos, y cumple las reglas HTTP y HTTPS. Esta función también le permite bloquear, permitir o excluir determinadas direcciones URL.

Filtrado de protocolos

Ofrece protección avanzada para los protocolos de aplicaciones disponibles en el motor de análisis ThreatSense. Este control es automático, independientemente de si se utiliza un navegador de Internet o un cliente de correo electrónico. También funciona para la comunicación cifrada (SSL/TLS).

Protección Anti-Phishing

Le permite bloquear páginas web conocidas por distribuir contenido de phishing.

Filtrado de protocolos

El motor de análisis ThreatSense, que integra varias técnicas avanzadas de análisis de malware, proporciona protección contra el malware a los protocolos de aplicación. El filtrado de protocolos funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizados. Si el filtrado de protocolos está activado, ESET Server Security comprobará las comunicaciones que utilicen el protocolo SSL/TLS: vaya a **Web y correo electrónico** > SSL/TLS.

Activar el filtrado del contenido de los protocolos de aplicación

Si desactiva el filtrado de protocolos, tenga en cuenta que muchos componentes de ESET Server Security (**Protección del tráfico de Internet**, **Protección de protocolos de correo electrónico** y **Protección Anti-Phishing**) dependen de esto para funcionar y no todas las funciones estarán disponibles.

Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones de red específicas, selecciónelas en la lista. No se comprobará la presencia de amenazas en la comunicación HTTP/POP3 de las aplicaciones seleccionadas. Le permite excluir aplicaciones específicas del filtrado de protocolos. Haga clic en **Editar** y **Agregar** para seleccionar un archivo ejecutable de la lista de aplicaciones para excluirlo del filtrado de protocolos.

IMPORTANTE
Se recomienda utilizar esta opción únicamente en aplicaciones que no funcionen correctamente cuando se comprueba su comunicación.

Direcciones IP excluidas

Le permite excluir determinadas direcciones remotas del filtrado de protocolos. Las direcciones IP de esta lista no se incluirán en el filtrado de contenidos del protocolo. No se comprobará la presencia de amenazas en las comunicaciones HTTP/POP3/IMAP entrantes y salientes de las direcciones seleccionadas.

IMPORTANTE
Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Haga clic en **Editar** y **Agregar** para especificar una dirección IP, un intervalo de direcciones o una subred a los que se aplicará la exclusión. Seleccione **Introduzca múltiples valores** para añadir varias direcciones IP delimitadas por líneas, comas o punto y coma. Si está activada la selección múltiple, las direcciones se mostrarán en la lista de direcciones IP excluidas.

NOTA
Las exclusiones son útiles cuando el filtrado de protocolos provoca problemas de compatibilidad.

Clientes de Internet y correo electrónico

Dada la ingente cantidad de código malicioso que circula en Internet, la navegación segura es un aspecto crucial para la protección de los ordenadores. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET Server Security se centra en la seguridad de los navegadores web. Cada aplicación que acceda a la red se puede marcar

como un navegador de Internet. Las aplicaciones que ya utilicen protocolos para la comunicación o procedentes de las rutas seleccionadas se pueden añadir a la lista de clientes web y de correo electrónico.

SSL/TLS

ESET Server Security es capaz de comprobar la presencia de amenazas en comunicaciones que utilizan los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte).

Puede utilizar varios modos de análisis para examinar las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos de la comprobación de comunicaciones protegidas mediante el protocolo SSL.

Habilitar el filtrado del protocolo de SSL/TLS

Si está desactivado el filtrado de protocolos, el programa no analizará las comunicaciones realizadas a través de SSL/TLS. El modo de filtrado de protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte) está disponible en las siguientes opciones:

- **Modo automático**: seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL/TLS, excepto las protegidas por certificados excluidos del análisis. Si se establece una comunicación nueva que utiliza un certificado firmado desconocido, no se le informará y la comunicación se filtrará automáticamente. Si accede a un servidor con un certificado que no sea de confianza pero que usted ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.
- **Modo interactivo**: si introduce un sitio nuevo protegido mediante SSL/TLS (con un certificado desconocido), se muestra un cuadro de diálogo con las acciones posibles. Este modo le permite crear una lista de certificados SSL/TLS que se excluirán del análisis.
- **Modo Política**: se filtran todas las conexiones SSL/TLS, a excepción de las exclusiones configuradas.

Lista de aplicaciones con filtrado SSL/TLS

Le permite añadir una aplicación con filtrado y establecer una de las acciones de análisis. La lista de aplicaciones con filtrado SSL/TLS puede utilizarse para personalizar el comportamiento de ESET Server Security para determinadas aplicaciones y para recordar acciones seleccionadas si el **Modo interactivo** está seleccionado en el **Modo de filtrado de protocolos SSL/TLS**.

Lista de certificados conocidos

Le permite personalizar el comportamiento de ESET Server Security para certificados SSL específicos. Si hace clic en Editar junto a la **Lista de certificados conocidos** podrá visualizar y gestionar la lista.

Excluir la comunicación con los dominios de confianza

Para excluir la comunicación con certificados de validación ampliados de la comprobación de protocolos (banca a través de Internet).

Bloquear las comunicaciones cifradas usando el protocolo obsoleto SSL v2

La comunicación establecida con esta versión anterior del protocolo SSL se bloqueará automáticamente.

Certificado raíz

Para que la comunicación SSL/TLS funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). La opción Agregar el certificado raíz a los navegadores conocidos debe estar activada. Seleccione esta opción para agregar el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

Validez del certificado

Si el certificado no se puede verificar mediante el almacén de certificados TRCA

A veces no es posible verificar el certificado de un sitio web con el almacén de **autoridades certificadoras de confianza** (TRCA). Esto significa que el certificado ha sido firmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre representa un riesgo. La mayoría de las empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (opción predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a sitios que tienen certificados sin verificar.

Si el certificado no es válido o está dañado

Significa que ha caducado o que la firma no es correcta. En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**.

Lista de certificados conocidos

Para personalizar el comportamiento de ESET Server Security para certificados específicos SSL (capa de sockets segura) y TLS (seguridad de la capa de transporte y recordar acciones seleccionadas si el **Modo interactivo** está seleccionado en el modo de filtrado de protocolos SSL/TLS. Puede configurar un certificado seleccionado o **Agregar** un certificado de una URL o Archivo. Cuando se encuentre en la ventana Agregar certificado, haga clic en el botón URL o Archivo y especifique la URL del certificado o busque un archivo de certificado. Los siguientes campos se completarán automáticamente con datos del certificado:

- **Nombre del certificado**: nombre del certificado.
- **Emisor del certificado**: nombre del creador del certificado.
- **Sujeto del certificado**: en este campo se identifica a la entidad asociada a la clave pública almacenada en el campo de clave pública del asunto.

Acción del acceso

- **Automático**: permitir certificados de confianza y preguntar por no confiables.
- **Permitir o Bloquear**: para permitir o bloquear la comunicación que protege este certificado, independientemente de su fiabilidad.

- **Preguntar**: para recibir un mensaje cuando se encuentre un certificado específico.

Acción de análisis

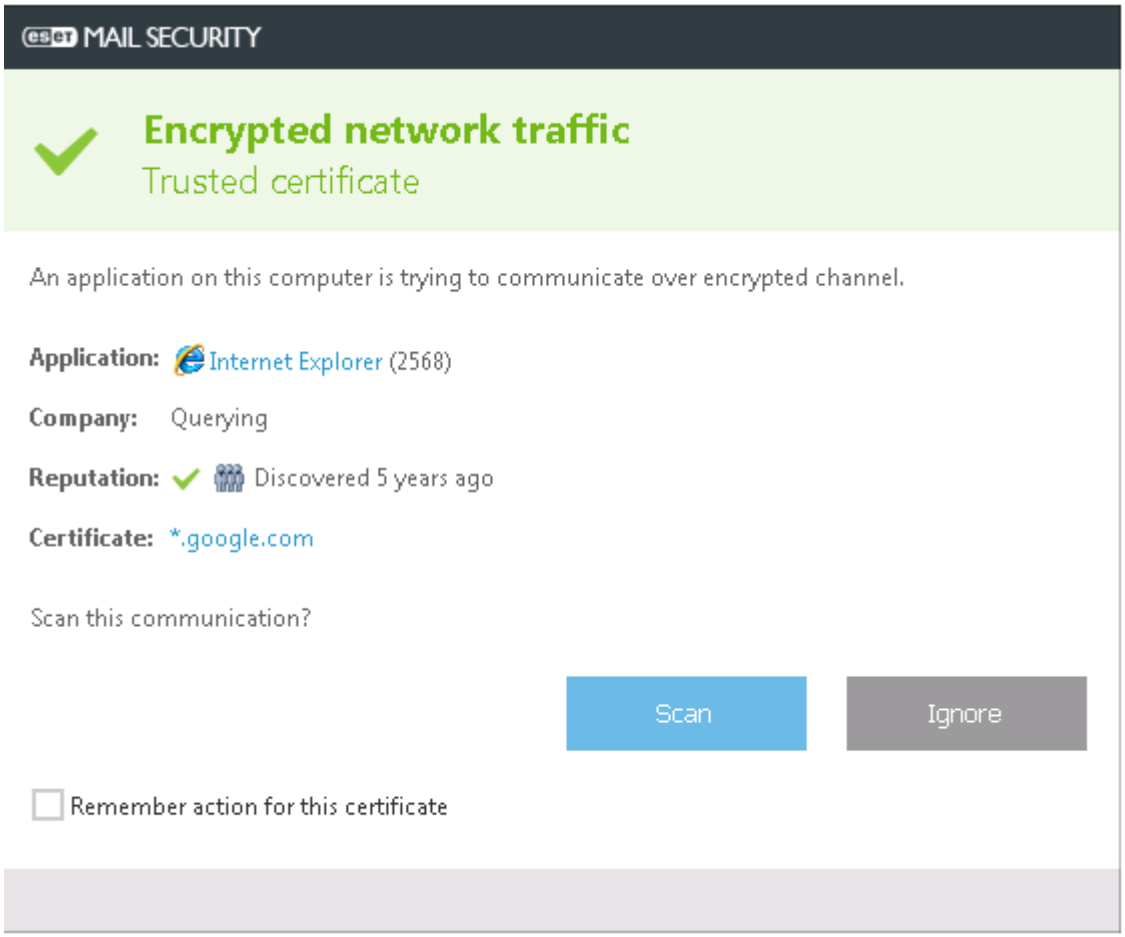
- **Automático**: para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo.
- **Analizar o Ignorar**: para analizar o ignorar la comunicación que protege este certificado.
- **Preguntar**: para recibir un mensaje cuando se encuentre un certificado específico.

Comunicación SSL cifrada

Si su sistema está configurado para utilizar el análisis del protocolo SSL, se mostrará un cuadro de diálogo para solicitarle que seleccione una acción en dos situaciones diferentes:

En primer lugar, si un sitio web utiliza un certificado no válido o que no se puede verificar y ESET Server Security está configurado para preguntar al usuario en estos casos (la opción predeterminada es sí para los certificados que no se pueden verificar y no para los que no son válidos), se abre un cuadro de diálogo para preguntarle si desea **Permitir** o **Bloquear** la conexión.

En segundo lugar, si el **Modo de filtrado del protocolo SSL** está establecido en **Modo interactivo**, se mostrará un cuadro de diálogo para cada sitio web para preguntarle si desea **Analizar** o **Ignorar** el tráfico. Algunas aplicaciones comprueban que nadie haya modificado ni inspeccionado su tráfico SSL; en estos casos, ESET Server Security debe **Ignorar** el tráfico para que la aplicación siga funcionando.



En ambos casos, el usuario tiene la opción de recordar la acción seleccionada. Las acciones guardadas se almacenan en la Lista de certificados conocidos.

Protección del cliente de correo electrónico

La integración de ESET Server Security con clientes de clientes de correo electrónico aumenta el nivel de la protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, la integración puede activarse en ESET Server Security. Al activar la integración, la barra de herramientas de ESET Server Security se inserta directamente en el cliente de correo electrónico (la barra de herramientas de las versiones más recientes de Windows Live Mail no se inserta), lo que aumenta la eficacia de la protección de correo electrónico.

Integración en el cliente de correo electrónico

Actualmente se admiten los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus. Aunque la integración no esté activada, la comunicación por correo electrónico sigue estando protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP). Para ver una lista completa de los clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la Base de conocimiento.

Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada

Si el sistema se ralentiza cuando trabaja con su cliente de correo electrónico (solo MS Outlook). Esto puede suceder cuando recupera correo electrónico de Kerio Outlook Connector Store, por ejemplo.

Activar protección del correo electrónico mediante complementos del cliente

Le permite desactivar la protección del cliente de correo electrónico sin eliminar la integración en su cliente de correo electrónico. Puede desactivar todos los complementos de forma simultánea o desactivar las siguientes opciones de forma selectiva:

- **Correo recibido**: activa el análisis de los mensajes recibidos.
- **Correo enviado**: activa el análisis de los mensajes enviados.
- **Correo leído**: activa el análisis de los mensajes leídos.

Acción que se realizará en correos electrónicos infectados

- **Sin acciones**: si esta opción está activada, el programa identificará los archivos adjuntos infectados, pero dejará los mensajes sin realizar ninguna acción.
- **Eliminar mensajes**: el programa informará al usuario sobre las amenazas y eliminará el mensaje.
- **Mover el correo electrónico a la carpeta de elementos eliminados**: los mensajes infectados se moverán automáticamente a la carpeta Elementos eliminados.
- **Mover mensajes a la carpeta**: los mensajes infectados se moverán automáticamente a la carpeta especificada.
- **Carpeta**: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Repetir el análisis tras la actualización

Activa y desactiva la repetición del análisis después de una actualización del Motor de detección.

Aceptar los resultados de los análisis realizados por otros módulos

Al seleccionar esta opción, el módulo de protección de correo electrónico acepta los resultados del análisis de otros módulos de protección (análisis de los protocolos POP3 e IMAP).

Protocolos de correo electrónico

Activar la protección del correo electrónico mediante el filtrado de protocolos

Los protocolos IMAP y POP3 son los más utilizados para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo electrónico. ESET Server Security proporciona protección para estos protocolos, independientemente del cliente de correo electrónico que se utilice.

ESET Server Security también admite el análisis de los protocolos IMAPS y POP3S, que utilizan un canal cifrado para transferir información entre el servidor y el cliente. ESET Server Security comprueba la comunicación con los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en Puertos utilizados por el **protocolo IMAPS / POP3S**, independientemente de la versión del sistema operativo.

Configuración del análisis de IMAPS/POP3S

Las comunicaciones cifradas no se analizarán cuando se utilice la configuración predeterminada. Para habilitar el análisis de comunicaciones cifradas, diríjase a Comprobación del protocolo SSL/TLS.

El número de puerto identifica qué tipo de puerto es. Estos son los puertos de correo electrónico predeterminados para:

Nombre del puerto	Números de puerto	Descripción
POP3	110	Puerto POP3 no cifrado predeterminado.
IMAP	143	Puerto IMAP no cifrado predeterminado.
IMAP seguro (IMAP4-SSL)	585	Habilitar el filtrado del protocolo de SSL/TLS. Cuando haya varios números de puerto, deben delimitarse con una coma.
IMAP4 a través de SSL (IMAPS)	993	Habilitar el filtrado del protocolo de SSL/TLS. Cuando haya varios números de puerto, deben delimitarse con una coma.
POP3 seguro (SSL-POP)	995	Habilitar el filtrado del protocolo de SSL/TLS. Cuando haya varios números de puerto, deben delimitarse con una coma.

Alertas y notificaciones

La protección del correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET Server Security ofrece control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP). Al examinar los mensajes entrantes, el programa utiliza todos los métodos de análisis avanzados incluidos en el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con la base de datos de virus. El análisis de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

Después de analizar un mensaje de correo electrónico, se puede adjuntar al mensaje una notificación del análisis. Puede elegir entre las opciones **Notificar en los mensajes recibidos y leídos**, **Agregar una nota al asunto de los correos electrónicos infectados que fueron recibidos y leídos** o **Notificar en los mensajes enviados**. Tenga en

cuenta que, en ocasiones puntuales, es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o que hayan sido falsificados por código malicioso. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Las opciones disponibles son:

- **Nunca**: no se agregará ningún mensaje con etiqueta.
- **Solo a mensajes infectados**: únicamente se marcarán como analizados los mensajes que contengan software malicioso (opción predeterminada).
- **A todos los mensajes analizados**: el programa agregará un mensaje a todo el correo analizado.

Agregar una nota al asunto de los correos electrónicos infectados enviados

Desactive esta casilla de verificación si no desea que la protección de correo electrónico incluya una alerta de virus en el asunto de los mensajes infectados. Esta función permite el filtrado sencillo y por asunto de los mensajes infectados (si su programa de correo electrónico lo admite). Además, aumenta la credibilidad ante el destinatario y, si se detecta una amenaza, proporciona información valiosa sobre el nivel de amenaza de un correo electrónico o remitente determinado.

En mensajes infectados, agregar en el Asunto la siguiente etiqueta

Modifique esta plantilla si desea modificar el formato de prefijo del asunto de un correo electrónico infectado. Esta función sustituye el asunto del mensaje `Hello` con un valor de prefijo especificado `[virus]` por el formato siguiente: `[virus] Hello`. La variable `%VIRUSNAME%` representa la amenaza detectada.

Barra de herramientas de MS Outlook

La protección de Microsoft Outlook funciona como un módulo de complemento. Después de instalar ESET Server Security, esta barra de herramientas que contiene las opciones de protección contra malware se agrega a Microsoft Outlook:

ESET Server Security

Al hacer clic en el **icono**, se abre la ventana principal del programa de ESET Server Security.

Analizar de nuevo los mensajes

Le permite iniciar la comprobación del correo electrónico de forma manual. Puede especificar los mensajes que se comprobarán y activar un nuevo análisis del correo recibido. Para obtener más información, consulte Protección del cliente de correo electrónico.

Configuración del análisis

Muestra las opciones de configuración de la Protección del cliente de correo electrónico.

Barra de herramientas de Outlook Express y Windows Mail

La protección de Outlook Express y Windows Mail funciona como un módulo de complemento. Después de instalar ESET Server Security, esta barra de herramientas que contiene las opciones de protección contra malware se agrega a Outlook Express o Windows Mail:

ESET Server Security

Al hacer clic en el **icono**, se abre la ventana principal del programa de ESET Server Security.

Analizar de nuevo los mensajes

Le permite iniciar la comprobación del correo electrónico de forma manual. Puede especificar los mensajes que se comprobarán y activar un nuevo análisis del correo recibido. Para obtener más información, consulte Protección del cliente de correo electrónico.

Configuración del análisis

Muestra las opciones de configuración de la Protección del cliente de correo electrónico.

Personalizar la apariencia

La apariencia de la barra de herramientas se puede modificar para el cliente de correo electrónico. Desactive la opción que personaliza la apariencia independientemente de los parámetros del programa de correo electrónico.

- **Mostrar texto** : muestra descripciones de los iconos.
- **Texto a la derecha**: las descripciones se mueven de la parte inferior al lado derecho de los iconos.
- **Iconos grandes**: muestra iconos grandes para las opciones de menú.

Cuadro de diálogo de confirmación

Esta notificación sirve para comprobar que el usuario realmente desea realizar la acción seleccionada, de forma que se deberían eliminar los posibles errores. El cuadro de diálogo también ofrece la posibilidad de desactivar las confirmaciones.

Analizar de nuevo los mensajes

La barra de herramientas de ESET Server Security integrada en los clientes de correo electrónico permite a los usuarios especificar varias opciones de análisis del correo electrónico. La opción **Analizar de nuevo los mensajes** ofrece dos modos de análisis:

- **Todos los mensajes de la carpeta actual**: analiza los mensajes de la carpeta que se muestra en ese momento.
- **Solo los mensajes seleccionados**: analiza únicamente los mensajes marcados por el usuario.
- **Volver a analizar los mensajes ya analizados**: proporciona al usuario una opción para ejecutar otro análisis en mensajes ya analizados.

Protección del tráfico de Internet

La protección del acceso a la Web funciona supervisando la comunicación entre navegadores web y servidores remotos para protegerlo de amenazas en línea, y cumple con las reglas HTTP (Protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se sabe que contienen código malicioso se bloquea antes de descargar contenido. El motor de análisis ThreatSense analiza todas las demás páginas web cuando se cargan y bloquean en caso de

detección de contenido malicioso. La protección del acceso a la Web ofrece dos niveles de protección: bloqueo por lista negra y bloqueo por contenido.

Básico

Le recomendamos encarecidamente que deje activada la opción **Protección del tráfico de Internet**. A esta opción también se puede acceder desde la ventana principal del programa de ESET Server Security, en **Configuración** > **Web y correo electrónico** > **Protección del acceso a la Web**.

Activar análisis avanzado de los scripts del navegador

De forma predeterminada, el motor de detección comprobará todos los programas JavaScript ejecutados por los navegadores web.

Protocolos web

Le permite configurar la supervisión de estos protocolos estándar que utilizan la mayoría de los navegadores de Internet. De forma predeterminada, ESET Server Security está configurado para supervisar el protocolo HTTP que utilizan la mayoría de los navegadores de Internet.

ESET Server Security admite también la comprobación del protocolo HTTPS. La comunicación HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Server Security comprueba la comunicación mediante los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo.

La comunicación cifrada no se analizará cuando se utilice la configuración predeterminada. Para activar el análisis de la comunicación cifrada, vaya a **Configuración avanzada** (**F5**) > **Web y correo electrónico** > SSL/TLS.

Parámetros de ThreatSense

Le permite configurar opciones como los tipos de análisis (mensajes de correo electrónico, archivos comprimidos, exclusiones, límites, etc.) y los métodos de detección para la protección del acceso a la Web.

Administración de direcciones URL

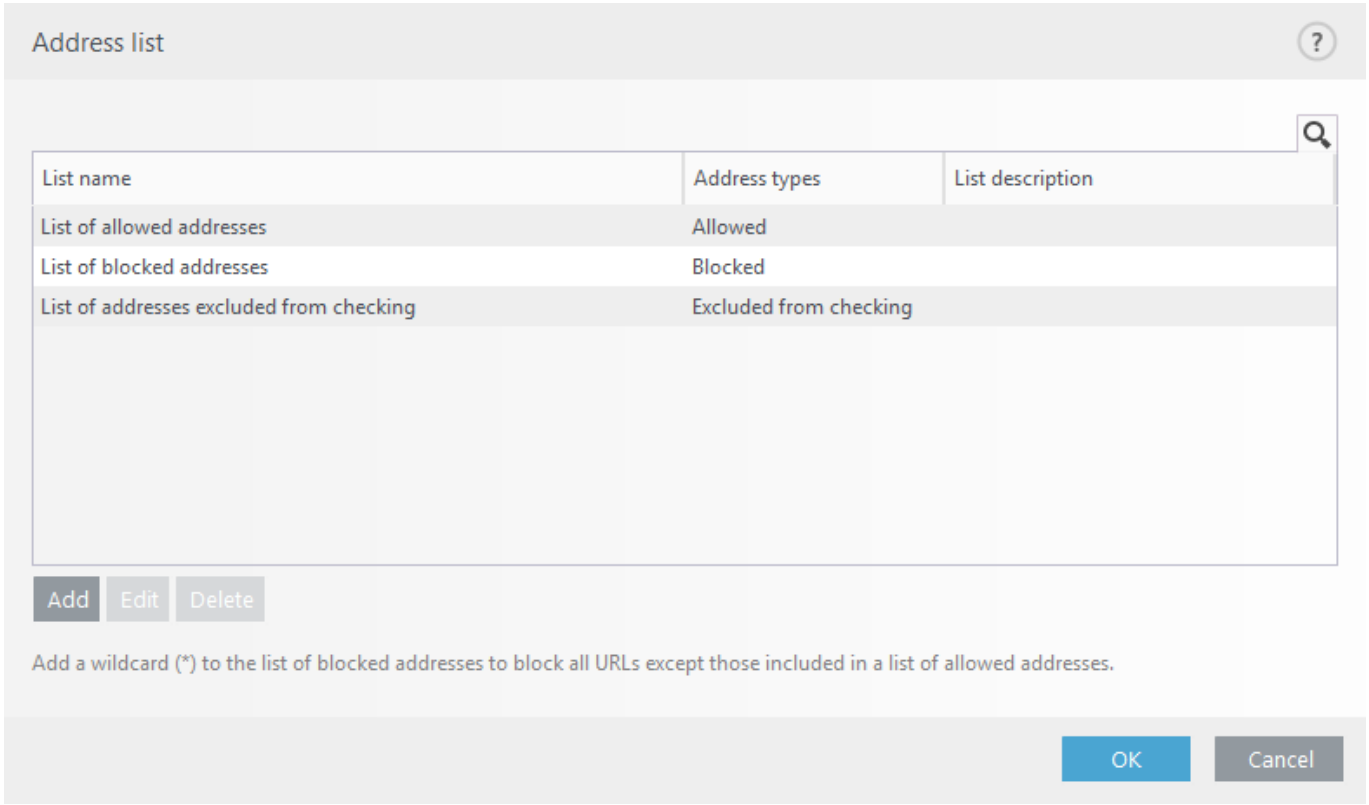
La administración de direcciones URL le permite especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis. No podrá acceder a los sitios web de la Lista de direcciones bloqueadas, a menos que también se incluyan en la Lista de direcciones permitidas. Cuando acceda a los sitios web que se encuentran en la Lista de direcciones que no se analizarán, no se buscará ningún código malicioso en ellos. Debe activar Filtrado de protocolos SSL/TLS si desea filtrar las direcciones HTTPS, además de las páginas web HTTP. Si no lo hace, solo se agregarán los dominios de los sitios HTTP que haya visitado, pero no la dirección URL completa.

Una lista de direcciones bloqueadas puede contener direcciones de algunas listas negras públicas externas, mientras que otra contiene su propia lista negra. Esto facilita la actualización de la lista externa sin que la suya se vea afectada.

Haga clic en **Editar** y en **Agregar** para crear una lista de direcciones nueva además de las predefinidas. Esta opción puede ser útil si se desea dividir varios grupos de direcciones de forma lógica. De forma predeterminada, están

disponibles estas tres listas:

- **Lista de direcciones excluidas de la verificación**: no se comprobará la existencia de código malicioso en ninguna de las direcciones agregadas a esta lista.
- **Lista de direcciones permitidas**: si está activada la opción Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones especificadas en esta lista. Las direcciones de esta lista estarán autorizadas incluso si se incluyen en la lista de direcciones bloqueadas.
- **Lista de direcciones bloqueadas**: el usuario no tendrá acceso a las direcciones incluidas en esta lista a menos que aparezcan también en la lista de direcciones permitidas.



Puede **Agregar** una nueva dirección URL a la lista. También puede introducir varios valores con el separador. Haga clic en **Editar** para modificar una dirección existente de la lista o en **Eliminar** para eliminarla. Solo pueden eliminarse direcciones creadas con la opción **Agregar**, no las que se importaron.

En todas las listas pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier número o carácter y el signo de interrogación, a cualquier carácter. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista.

> NOTA
> Si desea bloquear todas las direcciones HTTP menos las incluidas en la Lista de direcciones permitidas activa, agregue el símbolo * a la Lista de direcciones bloqueadas activa.

Crear nueva lista

La lista incluirá las direcciones URL/máscaras de dominio que se bloquearán, permitirán o excluirán del análisis. Cuando cree una lista nueva, especifique lo siguiente:

- **Tipo de lista de direcciones**: elija el tipo (Excluida del análisis, Bloqueada o Permitida) en la lista desplegable.
- **Nombre de la lista**: especifique el nombre de la lista. Este campo está desactivado cuando se edita una de las tres listas predefinidas.
- **Descripción de la lista**: escriba una breve descripción de la lista (opcional). Este campo está desactivado cuando se edita una de las tres listas predefinidas.
- **Lista activa**: utilice el conmutador para desactivar la lista. Podrá activarla más adelante cuando lo necesite.
- **Notificar al aplicar**: si desea recibir una notificación cuando se utilice una lista determinada al evaluar un sitio HTTP/HTTPS que ha visitado. Se emitirá una notificación si un sitio web se bloquea o admite porque se ha incluido en la lista de direcciones bloqueadas o permitidas. La notificación contendrá el nombre de la lista donde se incluye el sitio web especificado.
- **Nivel de registro**: elija el nivel de registro (Ninguno, Diagnóstico, Información o Advertencia) en la lista desplegable. ESET PROTECT puede recopilar registros con el nivel de detalle **Advertencia**.

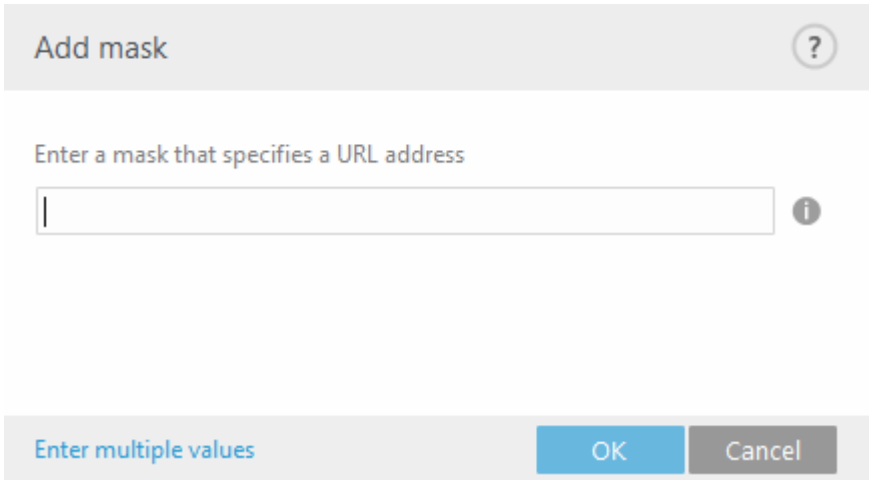
ESET Server Security permite al usuario bloquear el acceso a determinados sitios web para evitar que el navegador de Internet muestre su contenido. Además, permite especificar las direcciones que no se deben comprobar. Si no se conoce el nombre completo del servidor remoto o si el usuario desea especificar un grupo completo de servidores remotos, se pueden utilizar máscaras para identificar dicho grupo.

Las máscaras incluyen los símbolos ? y *:

- Utilice ? para sustituir un símbolo.
- Utilice * para sustituir una cadena de texto.

> EJEMPLO
> **.c?m* se aplica a todas las direcciones cuya última parte comience por la letra c, termine por la letra m y contenga un símbolo desconocido entre las dos (*.com*, *.cam*, etc.).

Las secuencias que empiezan por *. reciben un trato especial si se utilizan al principio de un nombre de dominio. En primer lugar, el comodín * no puede representar el carácter de barra ('/') en este caso. Con esto se pretende evitar que se burle la máscara; por ejemplo, la máscara **.domain.com* no coincidirá con *https://anydomain.com/anypath#.domain.com* (este sufijo se puede agregar a cualquier URL sin que la descarga se vea afectada). En segundo lugar, la secuencia *. también corresponde a una cadena vacía en este caso especial. El objetivo es permitir la detección de un dominio completo, incluidos todos sus subdominios, con una sola máscara. Por ejemplo, la máscara **.domain.com* también coincide con *https://domain.com*. No sería correcto utilizar **domain.com*, ya que esta cadena también detectaría *https://anotherdomain.com*.



Introduzca múltiples valores

Añada varias direcciones URL delimitadas por nuevas líneas, comas o punto y coma. Si está activada la selección múltiple, las direcciones se mostrarán en la lista.

Importar

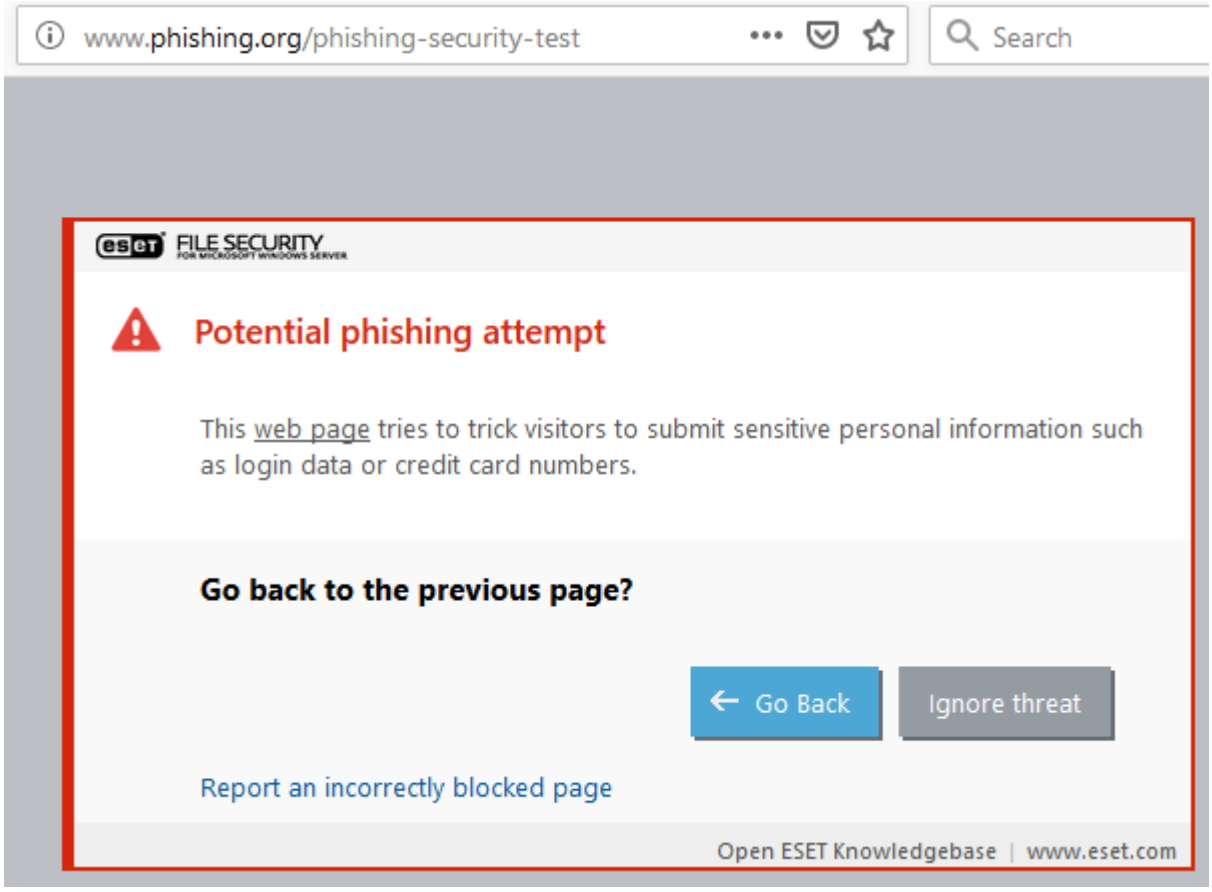
Importe un archivo de texto con direcciones URL (valores separados por un salto de línea, por ejemplo, `*.txt` utilizando la codificación UTF-8).

Protección web Anti-Phishing

El término phishing, o suplantación de la identidad, define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo suele ser acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc.

ESET Server Security incluye protección Anti-Phishing, que bloquea las páginas web conocidas por distribuir este tipo de contenido. Se recomienda encarecidamente que active la protección Anti-Phishing en ESET Server Security. Visite nuestro artículo de la Base de conocimiento para obtener más información sobre la protección Anti-Phishing de ESET Server Security.

Cuando entre en un sitio web de phishing reconocido, se mostrará el siguiente cuadro de diálogo en su navegador web. Si aún así quiere acceder al sitio web, haga clic en **Ignorar amenaza** (no recomendado).



NOTA
Los posibles sitios web de phishing que se han incluido en la lista blanca expirarán de forma predeterminada después de unas horas. Para permitir un sitio web permanentemente, use la herramienta Gestión de direcciones URL.

Informar sobre una página de phishing

Si se encuentra con un sitio web sospechoso que parece que es un sitio de phishing o con código malicioso, puede enviarlo a ESET para su análisis. Antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:

- El sitio web no se detecta en absoluto.
- El sitio web se detecta como una amenaza, pero no lo es. En este caso, puede informar de un falso positivo de phishing.

También puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el sitio web (por ejemplo, el sitio web que le refirió a este, cómo tuvo constancia de su existencia, etc.).

Control del dispositivo

ESET Server Security incluye control automático de dispositivos (CD, DVD, USB, etc.). Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un determinado dispositivo y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no deseado.

NOTA
Si activa el control de dispositivos con el conmutador junto a **Integrar en el sistema**, se activará la función de control de dispositivos de ESET Server Security. Sin embargo, es necesario reiniciar el sistema para que se aplique este cambio.

El control de dispositivos se activará, lo que le permitirá editar la configuración. Si se detecta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación y se prohíbe el acceso a dicho dispositivo.

Reglas

Una regla de control de dispositivos define la acción que se realizará al conectar al ordenador un dispositivo que cumple los criterios de la regla.

Grupos

Si hace clic en Editar, puede administrar grupos de dispositivos, crear un nuevo grupo de dispositivos o seleccionar uno existente para añadir o eliminar dispositivos de la lista.

NOTA
Puede ver las entradas del registro de control de dispositivos en Archivos de registro.

Reglas de dispositivos

Determinados dispositivos se pueden permitir o bloquear por usuario, por grupo de usuarios o según varios parámetros adicionales que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que se debe realizar cuando se detecta un dispositivo y el nivel de gravedad de registro.

Puede **Añadir** una nueva regla o modificar la configuración de la existente. Introduzca una descripción de la regla en el campo **Nombre** para facilitar la identificación. Haga clic en el conmutador situado junto a **Regla activada** para activar o desactivar esta regla, lo cual puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Aplicar durante

Puede limitar las reglas con la opción Intervalos de tiempo. Cree primero el intervalo de tiempo para que aparezca en el menú desplegable.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (Almacenamiento en disco, Dispositivo portátil, Bluetooth, FireWire…). Los tipos de dispositivos se heredan del sistema operativo y se pueden ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Los lectores de tarjetas inteligentes abarcan todos los lectores que tienen incrustado un circuito integrado, como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras; estos dispositivos no proporcionan información sobre los usuarios, sino únicamente sobre sus acciones. Esto significa que los dispositivos de imagen solo se pueden bloquear globalmente.

Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/Escritura**: se permitirá el acceso completo al dispositivo.
- **Bloquear**: se bloqueará el acceso al dispositivo.
- **Solo lectura**: solo se permitirá el acceso de lectura al dispositivo.
- **Advertir**: cada vez que se conecte un dispositivo se informará al usuario de si está permitido o bloqueado, y se efectuará una entrada de registro. Los dispositivos no se recuerdan, se seguirá mostrando una notificación en las siguientes conexiones del mismo dispositivo.

> NOTA
> Tenga en cuenta que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivos. Si un dispositivo dispone de espacio de almacenamiento, estarán disponibles las cuatro acciones. Para los dispositivos que no son de almacenamiento, solo hay solo dos (por ejemplo, **Solo lectura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir o bloquear).

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas y adaptarlas a dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas:

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

> NOTA
> Si estas tres descripciones mencionadas están vacías, la regla ignorará estos campos al establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).

si desea averiguar los parámetros de un dispositivo, cree una regla para permitir ese tipo de dispositivo, conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo en el Registro de control de dispositivos.

Elija la opción **Nivel de registro** en la lista desplegable:

- **Siempre**: registra todos los sucesos.
- **Diagnóstico**: registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta.
- **Ninguno**: no se registra nada.

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios agregándolos a la **Lista de usuarios**. Haga clic en **Editar** para gestionar la lista de usuarios.

- **Agregar**: abre el cuadro de diálogo **Tipos de objeto**: Usuarios o grupos, que le permite seleccionar los usuarios que desee.
- **Eliminar**: elimina del filtro al usuario seleccionado.

NOTA
los dispositivos se pueden filtrar mediante reglas de usuario (por ejemplo, los dispositivos de imagen no proporcionan información sobre los usuarios, sino únicamente sobre las acciones invocadas).

Están disponibles las funciones siguientes:

Modificar

Le permite modificar el nombre de la regla seleccionada o los parámetros (proveedor, modelo, número de serie) de los dispositivos que esta contiene.

Copiar

Crea una regla nueva basada en los parámetros de la regla seleccionada.

Eliminar

Si desea eliminar la regla seleccionada. También puede utilizar la casilla situada junto a la regla para desactivarla. Esta opción puede ser útil si no desea eliminar una regla de forma permanente para poder utilizarla más adelante.

Llenar

Ofrece una visión general de todos los dispositivos conectados actualmente con la siguiente información: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible). Cuando selecciona un dispositivo (de la lista de dispositivos detectados) y hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (puede modificar todos los ajustes).

Las reglas se muestran en orden de prioridad; las que tienen más prioridad se muestran en la parte superior de la lista. Puede seleccionar varias reglas y aplicar acciones, como, por ejemplo, eliminarlas o moverlas en la lista con los botones **Superior**/**Arriba**/**Abajo**/**Inferior** (botones de flecha).

Grupos de dispositivos

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo correspondiente, mientras que la parte izquierda contiene los grupos existentes. Seleccione el grupo que contiene los dispositivos que desea mostrar en el panel derecho.

Puede crear varios grupos de dispositivos a los que se aplicarán reglas distintas. También puede crear un solo grupo de dispositivos configurados como **Lectura**/**Escritura** o **Solo lectura**. Esto garantiza el bloqueo de dispositivos no reconocidos por el control de dispositivos pero conectados al ordenador.

ADVERTENCIA
La conexión de un dispositivo externo al ordenador puede presentar un riesgo para la seguridad.

Están disponibles las funciones siguientes:

Agregar

Le permite crear un nuevo grupo de dispositivos si escribe su nombre o agregar un dispositivo a un grupo existente (también puede especificar, si lo desea, datos como el nombre del proveedor, el modelo y el

número de serie), en función del punto de la ventana en el que hiciera clic en el botón.

Modificar

Le permite modificar el nombre del grupo seleccionado o los parámetros (proveedor, modelo, número de serie) de los dispositivos que este contiene.

Eliminar

Elimina el grupo o dispositivo seleccionado en función del punto de la ventana en el que hiciera clic en el botón. También puede utilizar la casilla situada junto a la regla para desactivarla. Esta opción puede ser útil si no desea eliminar una regla de forma permanente para poder utilizarla más adelante.

Importar

Importa una lista de números de serie de dispositivos desde un archivo.

Llenar

Ofrece una visión general de todos los dispositivos conectados actualmente con la siguiente información: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible). Cuando selecciona un dispositivo (de la lista de dispositivos detectados) y hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (puede modificar todos los ajustes).

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** si desea cerrar la ventana **Grupos de dispositivos** sin guardar los cambios.

> NOTA
> Tenga en cuenta que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivos. Si un dispositivo dispone de espacio de almacenamiento, estarán disponibles las cuatro acciones. Para los dispositivos que no son de almacenamiento, solo hay solo dos (por ejemplo, Solo lectura no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir o bloquear).

Configuración de las herramientas

Puede personalizar la configuración avanzada de las siguientes opciones:

- Intervalos de tiempo
- ESET PROTECT objetos del análisis
- Modo de anulación
- CMD DE ESET
- ESET RMM
- Licencia
- Proveedor WMI
- Archivos de registro
- Servidor proxy
- Notificaciones por correo electrónico
- Modo de presentación
- Diagnósticos
- Clúster

Intervalos de tiempo

En las reglas de control de dispositivos se utilizan los intervalos de tiempo, que limitan las reglas cuando se aplican. Cree un intervalo de tiempo y selecciónelo al agregar nuevas reglas o al modificar reglas existentes (parámetro**Aplicar durante**). Esto le permite definir intervalos de tiempo usados habitualmente (horario laboral, fin de semana, etc.) y volver a utilizarlos de forma sencilla sin definir de nuevo los intervalos de tiempo de cada regla. Debe aplicarse un intervalo de tiempo a cualquier tipo de regla relevante que admita el control temporal.

Microsoft Windows Update

Las actualizaciones de Windows ofrecen correcciones importantes de vulnerabilidades potencialmente peligrosas, y mejoran el nivel de seguridad global del ordenador. Por eso es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Server Security le informa sobre las actualizaciones que faltan, según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **Sin actualizaciones**: no se ofrecerá ninguna actualización del sistema para la descarga.
- **Actualizaciones opcionales**: se ofrecerán para la descarga las actualizaciones marcadas como de baja prioridad y de niveles superiores.
- **Actualizaciones recomendadas**: se ofrecerán para la descarga las actualizaciones marcadas como habituales y de niveles superiores.
- **Actualizaciones importantes**: se ofrecerán para la descarga las actualizaciones marcadas como importantes y de niveles superiores.
- **Actualizaciones críticas**: solo se ofrecerá la descarga de actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará después de la verificación del estado con el servidor de actualización. Es posible que la información de actualización del sistema no esté disponible inmediatamente después de guardar los cambios.

Análisis de línea de comandos

Como alternativa a eShell, puede ejecutar el análisis ESET Server Security a petición desde la línea de comandos con el archivo `ecls.exe` de la carpeta de instalación.

A continuación se muestra una lista de parámetros y modificadores:

Opciones:

`/base-dir=FOLDER`	cargar módulos desde CARPETA
`/quar-dir=FOLDER`	CARPETA de Cuarentena
`/exclude=MASK`	excluir del análisis los archivos que cumplan MÁSCARA
`/subdir`	analizar subcarpetas (predeterminado)
`/no-subdir`	no analizar subcarpetas
`/max-subdir-level=LEVEL`	máximo nivel de anidamiento para subcarpetas a analizar

/symlink	seguir enlaces simbólicos (predeterminado)
/no-symlink	omitir enlaces simbólicos
/ads	analizar ADS (predeterminado)
/no-ads	no analizar ADS
/log-file=FILE	registrar en archivo
/log-rewrite	sobrescribir el archivo de salida (predeterminado - agregar)
/log-console	enviar registro a la consola (predeterminado)
/no-log-console	no enviar registro a la consola
/log-all	registrar también los archivos desinfectados
/no-log-all	no registrar archivos sin infectar (predeterminado)
/aind	mostrar indicador de actividad
/auto	analiza y desinfecta automáticamente todos los discos locales

Opciones de análisis:

/files	analizar archivos (predeterminado)
/no-files	no analizar archivos
/memory	memoria de análisis
/boots	analizar sectores de inicio
/no-boots	no analizar sectores de inicio (predeterminado)
/arch	analizar archivos comprimidos (predeterminado)
/no-arch	no analizar archivos comprimidos
/max-obj-size=SIZE	analizar sólo archivos menores de TAMAÑO megabytes (predeterminado 0 = ilimitado)
/max-arch-level=LEVEL	máxima profundidad de anidamiento para archivos comprimidos
/scan-timeout=LIMIT	analizar archivos comprimidos con un LIMITE máximo de segundos
/max-arch-size=SIZE	analizar los archivos dentro de un archivo comprimido sólo si su tamaño es inferior a TAMAÑO (predeterminado 0 = ilimitado)
/max-sfx-size=SIZE	analizar sólo los archivos en un archivo comprimido de auto extracción si su tamaño es inferior a TAMAÑO megabytes (predeterminado 0 = ilimitado)
/mail	analizar archivos de correo (predeterminado)
/no-mail	no analizar archivos de correo
/mailbox	analizar buzones de correo (predeterminado)
/no-mailbox	no analizar buzones de correo
/sfx	analizar archivos comprimidos de auto extracción (predeterminado)
/no-sfx	no analizar archivos comprimidos de autoextracción
/rtp	analizar empaquetadores de ejecución en tiempo real (predeterminado)
/no-rtp	no analizar empaquetadores en tiempo real
/unsafe	analizar en busca de aplicaciones potencialmente peligrosas
/no-unsafe	no analizar aplicaciones potencialmente peligrosas (predeterminado)
/unwanted	analizar en busca de aplicaciones potencialmente indeseables
/no-unwanted	no analizar aplicaciones potencialmente indeseables (predeterminado)

/suspicious	analizar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no analizar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	activar heurística (predeterminado)
/no-heur	desactivar heurística
/adv-heur	activar la Heurística avanzada (predeterminado)
/no-adv-heur	desactivar Heurística avanzada
/ext-exclude=EXTENSIONS	excluir del análisis las EXTENSIONES de archivo delimitadas por los dos puntos
/clean-mode=MODE	utilizar el MODO de limpieza con los objetos infectados Están disponibles las opciones siguientes: • none (predeterminado): no se realizará la desinfección automática. • standard: ecls.exe intentará desinfectar o eliminar automáticamente los archivos infectados. • strict: ecls.exe intentará desinfectar o eliminará automáticamente los archivos infectados sin la intervención del usuario (no se le preguntará antes de que se eliminen los archivos). • rigorous: ecls.exe eliminará los archivos sin intentar desinfectarlos, sea cual sea el archivo. • delete: ecls.exe eliminará los archivos sin intentar limpiarlos, pero no eliminará archivos delicados como los archivos del sistema de Windows.
/quarantine	copiar archivos infectados (si se han desinfectado) a la cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar archivos infectados a Cuarentena

Opciones generales:

/help	mostrar la ayuda y salir
/version	mostrar información de la versión y salir
/preserve-time	conservar hora del último acceso

Códigos de salida:

0	no se ha detectado ninguna amenaza
1	amenaza detectada y eliminada
10	no se han podido analizar todos los archivos (podrían ser amenazas)
50	amenaza detectada
100	error (los códigos de salida mayores que 100 significan que no se ha analizado el archivo y que no se puede considerar desinfectado)

CMD DE ESET

Se trata de una función que activa comandos de ecmd avanzados. Le permite exportar e importar la configuración utilizando la línea de comandos (ecmd.exe). Hasta ahora, solo era posible exportar la configuración con la interfaz gráfica de usuario. La configuración de ESET Server Security puede exportarse a un archivo *.xml*.

Si tiene activado CMD de ESET, dispone de dos métodos de autorización:

- **Ninguno**: sin autorización. No se recomienda este método, ya que permite importar configuraciones no firmadas, lo que supone un riesgo.
- **Configuración avanzada de contraseña**: se requiere contraseña para importar una configuración de un archivo *.xml*. Este archivo debe estar firmado (consulte cómo se firma un archivo de configuración *.xml* más adelante). Debe introducirse la contraseña especificada en Configuración de acceso para poder importar una nueva configuración. Si no ha activado la configuración de acceso, la contraseña no coincide o el archivo de configuración *.xml* no está firmado, la configuración no se importará.

Una vez que CMD de ESET esté activado, podrá utilizar la línea de comandos para importar o exportar configuraciones de ESET Server Security. Podrá hacerlo de forma manual o crear un script con fines de automatización.

IMPORTANTE
Para poder utilizar comandos de ecmd avanzados, deberá ejecutarlos con privilegios de administrador o abrir el símbolo del sistema de Windows (cmd) con **Ejecutar como administrador**. De lo contrario, aparecerá el mensaje **Error executing command.**. Asimismo, a la hora de exportar una configuración, deberá existir una carpeta de destino. El comando de exportación sigue funcionando cuando se desactiva el ajuste CMD de ESET.

EJEMPLO
Comando para exportar configuración:
`ecmd /getcfg c:\config\settings.xml`

Comando para importar configuración:
`ecmd /setcfg c:\config\settings.xml`

NOTA
Los comandos de ecmd avanzados solo pueden ejecutarse de forma local. La ejecución de la tarea de cliente **Ejecutar comando** mediante ESET PROTECT no funcionará.

Cómo firmar un archivo de configuración *.xml*:

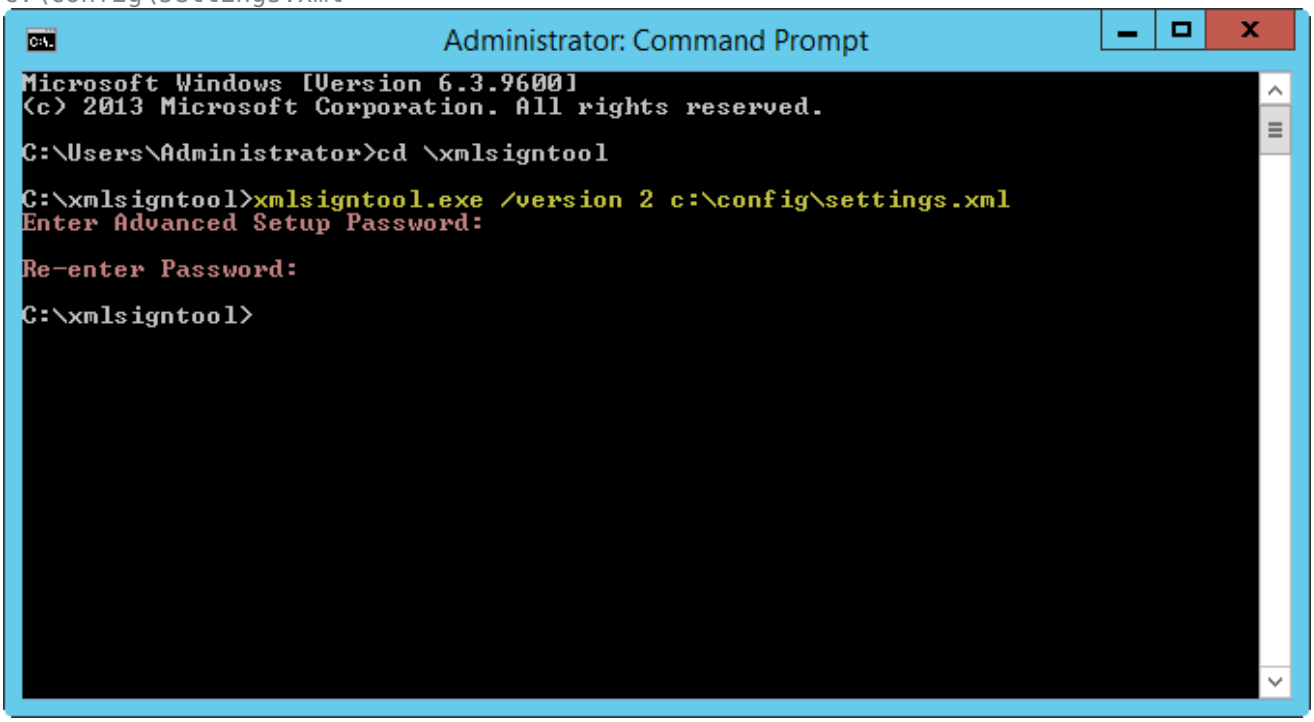
1. Descargue el archivo ejecutable XmlSignTool.
2. Abra el símbolo del sistema de Windows (cmd) con **Ejecutar como administrador**.
3. Vaya hasta donde esté `xmlsigntool.exe`
4. Ejecute un comando para firmar el archivo de configuración *.xml*; utilice: `xmlsigntool /version 1|2 <xml_file_path>`

IMPORTANTE
El valor del parámetro `/version` depende de la versión de su ESET Server Security. Utilice `/version 2` para ESET Server Security 7 y versiones más recientes.

5. Introduzca y vuelva a introducir la contraseña de Configuración avanzada cuando se lo solicite

XmlSignTool. Su archivo de configuración *.xml* ya estará firmado y podrá utilizarse para importarse en otra instancia de ESET Server Security con CMD de ESET mediante el método de autorización de contraseña.

EJEMPLO
Comando para firmar un archivo de configuración exportado: `xmlsigntool /version 2 c:\config\settings.xml`



NOTA
Si la contraseña de Configuración de acceso cambia y desea importar una configuración firmada anteriormente con una contraseña antigua, podrá volver a firmar el archivo de configuración *.xml* con la contraseña actual. Esto le permitirá utilizar un archivo de configuración más antiguo sin necesidad de exportarlo en otra máquina que ejecute ESET Server Security antes de la importación.

ESET RMM

La supervisión y administración remotas (RMM) son el proceso de supervisar y controlar los sistemas de software (como los que están instalados en escritorios, servidores y dispositivos móviles) mediante un agente instalado a nivel local al que un proveedor de servicios de administración puede acceder.

Activar RMM

Activa el comando de supervisión y administración remotas. Debe tener privilegios de administrador para utilizar la utilidad RMM.

Modo de trabajo

Seleccione el modo de trabajo de RMM en el menú desplegable:

- **Solo operaciones seguras**: si desea activar la interfaz RMM para operaciones seguras y de solo lectura
- **Todas las operaciones**: si desea activar la interfaz RMM para todas las operaciones

Método de autorización

Establezca el método de autorización de RMM en el menú desplegable:

- **Ninguno**: no se realizará ninguna comprobación de la ruta de acceso de la aplicación; puede ejecutar *ermm.exe* desde cualquier aplicación.
- **Ruta de acceso de la aplicación**: especifique la aplicación que puede ejecutar *ermm.exe*

La instalación predeterminada de ESET Endpoint Security incluye el archivo *ermm.exe* que se encuentra en ESET Server Security (ruta predeterminada c*:**Program Files**ESET**ESET Server Security*). *ermm.exe* intercambia datos con el complemento RMM, que se comunica con RMM Agent, que está vinculado a un RMM Server.

- *ermm.exe*: utilidad de línea de comandos desarrollada por ESET que permite la administración de productos Endpoint y la comunicación con cualquier complemento RMM.
- Complemento RMM: una aplicación de terceros que se ejecuta a nivel local en sistemas Endpoint de Windows. El complemento se ha diseñado para comunicarse con un RMM Agent determinado (por ejemplo, solo Kaseya) y con *ermm.exe*.
- RMM Agent: una aplicación de terceros (por ejemplo, Kaseya) que se ejecuta a nivel local en sistemas Endpoint de Windows. El agente se comunica con el complemento RMM y con RMM Server.
- RMM Server: se ejecuta como un servicio en un servidor de terceros. Los sistemas RMM compatibles son: Kaseya, Labtech, Autotask, Max Focus y Solarwinds N-able.

Visite nuestro artículo de la base de conocimiento para obtener más información sobre ESET RMM en ESET Server Security.

Plugins de ESET Direct Endpoint Management para soluciones RMM de terceros

RMM Server se ejecuta como servicio en un servidor de terceros. Si desea obtener más información, consulte los siguientes manuales de usuario en línea de ESET Direct Endpoint Management:

- Plugin de ESET Direct Endpoint Management para ConnectWise Automate
- Plugin de ESET Direct Endpoint Management para DattoRMM
- ESET Direct Endpoint Management para SolarWinds N-Central
- ESET Direct Endpoint Management para NinjaRMM

Licencia

ESET Server Security se conecta al servidor de licencias de ESET varias veces por hora para realizar comprobaciones. El parámetro **Intervalo de comprobación** está establecido en **Automático** de forma predeterminada. Si desea disminuir el tráfico de red provocado por las comprobaciones de licencias, cambie el intervalo de comprobación a **Limitado** y la comprobación de licencias solo se realizará una vez al día (también cuando se reinicie el servidor).

Cuando el intervalo de comprobación está establecido en **Limitado**, todos los cambios relacionados con la licencia que se realicen en ESET Server Security con ESET Business Account y ESET MSP Administrator pueden tardar hasta un día en aplicarse.

Proveedor WMI

El Instrumental de administración de Windows (WMI) es la implementación de Microsoft de WBEM (siglas del inglés Web-Based Enterprise Management), iniciativa que el sector ha adoptado para desarrollar una tecnología estándar a la hora de obtener acceso a la información de administración en entornos empresariales.

Si desea obtener más información sobre WMI, consulte http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx (en inglés).

Proveedor WMI de ESET

La finalidad del Proveedor WMI de ESET es permitir la supervisión remota de los productos de ESET en un entorno empresarial sin necesidad de software o herramientas propios de ESET. Al exponer la información básica del producto, su estado y estadísticas a través de WMI, crecen considerablemente las posibilidades que los administradores de las empresas tienen a su disposición durante la supervisión de los productos de ESET. Los administradores tendrán la posibilidad de emplear los diversos métodos de acceso ofrecidos por WMI (línea de comandos, scripts y herramientas de supervisión de terceros) para supervisar el estado de los productos de ESET.

En la implementación actual se permite acceso de solo lectura a información básica del producto, funciones instaladas y su estado de protección, estadísticas de módulos de análisis concretos y archivos de registro del producto.

El Proveedor WMI permite utilizar una infraestructura y herramientas estándar de Windows WMI para leer el estado y los registros del producto.

Datos proporcionados

Todas las clases WMI relacionadas con el producto ESET se encuentran en el espacio de nombres "root\ESET". A día de hoy están implementadas las siguientes clases, descritas a continuación con más detalle:

General

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

Registros

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**
- **ESET_HyperVScanLogs**

- **ESET_HyperVScanLogRecords**

ESET_Product class

Solo puede haber una instancia de la clase ESET_Product. Las propiedades de esta clase hacen referencia a información básica sobre el producto ESET instalado:

- **ID**: identificador de tipo de producto, por ejemplo "emsl"
- **Name**: nombre del producto, por ejemplo, "ESET Mail Security"
- **FullName**: nombre completo del producto, por ejemplo, "ESET Mail Security for IBM Domino"
- **Version**: versión del producto, por ejemplo "6.5.14003.0"
- **VirusDBVersion**: versión de la base de datos de virus, por ejemplo "14533 (20161201)"
- **VirusDBLastUpdate**: fecha y hora de la última actualización de la base de datos de virus. La cadena contiene la fecha y la hora en formato WMI, por ejemplo, "20161201095245.000000+060"
- **LicenseExpiration**: plazo de caducidad de la licencia. La cadena contiene la fecha y la hora en formato WMI
- **KernelRunning**: el valor booleano que indica si el servicio ekrn se encuentra en ejecución en el ordenador, por ejemplo, "TRUE".
- **StatusCode**: número que indica el estado de protección del producto: 0: verde (correcto), 1: amarillo (advertencia), 2: rojo (error)
- **StatusText**: mensaje que describe el motivo de un código de estado que no sea cero; de lo contrario será un valor nulo.

ESET_Features class

La clase ESET_Features cuenta con varias instancias, en función del número de funciones del producto. Cada instancia contiene los siguientes elementos:

- **Name**: nombre de la función (a continuación se expone la lista de nombres).
- **Status**: estado de la función: 0: inactiva; 1: desactivada, 2; activada

Una lista de cadenas que representa las funciones del producto actualmente reconocidas:

- **CLIENT_FILE_AV**: protección antivirus del sistema de archivos en tiempo real.
- **CLIENT_WEB_AV**: protección antivirus de Internet del cliente.
- **CLIENT_DOC_AV**: protección antivirus de documentos del cliente.
- **CLIENT_NET_FW** : cortafuegos personal del cliente.
- **CLIENT_EMAIL_AV**: protección antivirus del correo electrónico del cliente.
- **CLIENT_EMAIL_AS**: protección antispam del correo electrónico del cliente.
- **SERVER_FILE_AV**: protección antivirus en tiempo real de archivos del producto de servidor de archivos protegido; por ejemplo, archivos en la base de datos de contenido de SharePoint en el caso de ESET Server Security.
- **SERVER_EMAIL_AV**: protección antivirus de correos electrónicos de producto de servidor protegido, por ejemplo correos electrónicos en MS Exchange o IBM Domino
- **SERVER_EMAIL_AS**: protección antispam de correos electrónicos de producto de servidor protegido, por ejemplo correos electrónicos en MS Exchange o IBM Domino
- **SERVER_GATEWAY_AV**: protección antivirus de protocolos de red protegidos en la puerta de enlace.
- **SERVER_GATEWAY_AS**: protección antispam de protocolos de red protegidos en la puerta de enlace.

ESET_Statistics class

La clase ESET_Statistics cuenta con varias instancias, en función del número de módulos de análisis del producto. Cada instancia contiene los siguientes elementos:

- **Scanner**: código de cadena del escáner concreto, por ejemplo "CLIENT_FILE".
- **Total**: número total de archivos analizados.
- **Infected**: número de archivos infectados detectados.
- **Cleaned**: número de archivos desinfectados.
- **Timestamp**: hora y fecha del último cambio de esta estadística. En formato de fecha y hora WMI, por ejemplo, "20130118115511.000000+060".
- **ResetTime**: fecha y hora del último restablecimiento del contador de estadísticas. En formato de fecha y hora WMI, por ejemplo, "20130118115511.000000+060".

Lista de cadenas que representan módulos de análisis actualmente reconocidos:

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog class

La clase ESET_ThreatLog cuenta con varias instancias, y cada una de ellas representa un historial del registro "Detected threats". Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner**: nombre del módulo de análisis que creó este suceso del registro.
- **ObjectType**: tipo de objeto que generó este suceso del registro.
- **ObjectName**: nombre del objeto que generó este suceso del registro.
- **Threat**: nombre de la amenaza detectada en el objeto descrito por las propiedades ObjectName y ObjectType.
- **Action**: acción efectuada tras la identificación de la amenaza.
- **User**: cuenta de usuario que provocó la generación de este suceso del registro.
- **Information**: descripción adicional del evento.
- **Hash**: hash del objeto que generó este suceso del registro.

ESET_EventLog

La clase ESET_EventLog cuenta con varias instancias, y cada una de ellas representa un historial del registro "Events". Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresada como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

- **Module**: nombre del módulo de análisis que creó este suceso del registro.
- **Event**: descripción del suceso.
- **User**: cuenta de usuario que provocó la generación de este suceso del registro.

ESET_ODFileScanLogs

La clase ESET_ODFileScanLogs cuenta con varias instancias, y cada una de ellas representa un registro de análisis de archivo a petición. Equivale a la lista de registros "On-demand computer scan" de la interfaz gráfica de usuario. Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **Targets** : carpetas/objetos destino del análisis.
- **TotalScanned**: número total de objetos analizados.
- **Infected**: número de objetos infectados encontrados.
- **Cleaned**: número de objetos desinfectados.
- **Status**: estado del proceso de análisis.

ESET_ODFileScanLogRecords

La clase ESET_ODFileScanLogRecords cuenta con varias instancias, y cada una de ellas representa un historial del registro en uno de los registros de análisis representados por las instancias de la clase ESET_ODFileScanLogs. Las instancias de esta clase contienen historiales de registro de todos los análisis/registros a petición. Cuando solo se requiere la instancia de un registro de análisis determinado, debe filtrarse por medio de la propiedad LogID. Cada instancia de la clase contiene los siguientes elementos:

- **LogID**: identificador del registro de análisis al que pertenece este historial (identificador de una de las instancias de la clase ESET_ODFileScanLogs).
- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log**: mensaje de registro real.

ESET_ODServerScanLogs

La clase ESET_ODServerScanLogs cuenta con varias instancias, y cada una de ellas representa una ejecución del análisis a petición del servidor. Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **Targets** : carpetas/objetos destino del análisis.
- **TotalScanned**: número total de objetos analizados.
- **Infected**: número de objetos infectados encontrados.
- **Cleaned**: número de objetos desinfectados.
- **RuleHits**: número total de coincidencias de la regla.
- **Status**: estado del proceso de análisis.

ESET_ODServerScanLogRecords

La clase ESET_ODServerScanLogRecords cuenta con varias instancias, y cada una de ellas representa un historial

del registro en uno de los registros de análisis representados por las instancias de la clase ESET_ODServerScanLogRecords. Las instancias de esta clase contienen historiales de registro de todos los análisis/registros a petición. Cuando solo se requiere la instancia de un registro de análisis determinado, debe filtrarse por medio de la propiedad LogID. Cada instancia de la clase contiene los siguientes elementos:

- **LogID**: identificador del registro de análisis al que pertenece este historial (identificador de una de las instancias de la clase ESET_ODServerScanLogRecords).
- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresada como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log**: mensaje de registro real.

ESET_SmtpProtectionLog

La clase ESET_SmtpProtectionLog cuenta con varias instancias y cada una de ellas representa un historial del registro "Protección SMTP". Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro de análisis
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning , Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain**: nombre del dominio HELO.
- **IP**: dirección IP de origen.
- **Sender**: remitente del correo electrónico.
- **Recipient**: destinatario del correo electrónico.
- **ProtectionType**: tipo de protección empleada.
- **Action**: acción realizada.
- **Reason**: motivo que lleva a realizar la acción.
- **TimeToAccept**: cantidad de minutos tras la que se aceptará el correo electrónico.

ESET_HIPSLog

La clase ESET_HIPSLog cuenta con varias instancias y cada una de ellas representa un historial del registro "HIPS". Cada instancia incluye los siguientes elementos:

- **ID** : identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresada como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Application**: aplicación Fuente.
- **Target**: tipo de operación.
- **Action**: acción realizada por HIPS, por ejemplo, permitir, denegar, etc.
- **Rule**: nombre de la regla responsable de la acción.
- **AdditionalInfo**

ESET_URLLog

La clase ESET_URLLog cuenta con varias instancias y cada una de ellas representa un historial del registro "Sitios web filtrados". Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning , Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **URL**: la dirección URL.
- **Status**: lo que le ha ocurrido a la dirección URL, por ejemplo, "Bloqueada por Control de acceso web".
- **Application**: aplicación que ha tratado de acceder a la dirección URL.
- **User**: la cuenta del usuario en la que la aplicación se estaba ejecutando.

ESET_DevCtrlLog

La clase ESET_DevCtrlLog cuenta con varias instancias y cada una de ellas representa un historial del registro "Control de dispositivos". Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Device**: nombre del dispositivo.
- **User**: nombre de la cuenta del usuario.
- **UserSID**: SID de la cuenta del usuario.
- **Group**: nombre del grupo de usuarios.
- **GroupSID**: SID del grupo de usuarios.
- **Status**: lo que le ha ocurrido al dispositivo, por ejemplo, "Escritura bloqueada".
- **DeviceDetails**: información adicional relacionada con el dispositivo.
- **EventDetails**: información adicional relacionada con el suceso.

ESET_MailServerLog

La clase ESET_MailServerLog cuenta con varias instancias y cada una de ellas representa un historial del registro "Servidor de correo". Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **IPAddr**: dirección IP de origen.
- **HELODomain**: nombre del dominio HELO.
- **Sender**: remitente del correo electrónico.
- **Recipient**: destinatario del correo electrónico.
- **Subject**: asunto del correo electrónico.
- **ProtectionType**: el tipo de protección que ha realizado la acción descrita por el registro actual, es decir, Malware, Antispam o Reglas.
- **Action**: acción realizada.
- **Reason**: el motivo por el que el ProtectionType indicado realizó la acción en el objeto.

ESET_HyperVScanLogs

La clase ESET_HyperVScanLogs cuenta con varias instancias y cada una de ellas representa una ejecución del análisis del archivo Hyper-V, que equivale a la lista de registros "Análisis Hyper-V" de la interfaz gráfica de usuario. Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **Targets**: máquinas/discos/volúmenes objeto del análisis.
- **TotalScanned**: número total de objetos analizados.
- **Infected**: número de objetos infectados encontrados.
- **Cleaned**: número de objetos desinfectados.
- **Status**: estado del proceso de análisis.

ESET_HyperVScanLogRecords

La clase ESET_HyperVScanLogRecords cuenta con varias instancias y cada una de ellas representa un historial del registro en uno de los registros de análisis representados por las instancias de la clase ESET_HyperVScanLogs. Las instancias de esta clase incluyen historiales de registro de todos los análisis/registros Hyper-V. Cuando solo se requiere la instancia de un registro de análisis determinado, debe filtrarse por medio de la propiedad LogID. Cada instancia de la clase incluye los siguientes elementos:

- **LogID**: identificador del registro de análisis al que pertenece este historial (identificador de una de las instancias de la clase ESET_HyperVScanLogs).
- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning , Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log**: mensaje de registro real.

ESET_NetworkProtectionLog

La clase ESET_NetworkProtectionLog cuenta con varias instancias y cada una de ellas representa un historial del registro "Protección de red". Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning , Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Event**: suceso que activa la acción de protección de la red.
- **Action**: acción realizada por la protección de la red.
- **Source**: dirección de origen del dispositivo de red.
- **Target**: dirección de destino del dispositivo de red.
- **Protocol**: protocolo de comunicación de la red.
- **RuleOrWormName**: nombre de gusano o regla asociados al suceso.
- **Application**: aplicación que inició la comunicación de red.
- **User**: cuenta de usuario que provocó la generación de este suceso del registro.

ESET_SentFilesLog

La clase ESET_SentFilesLog cuenta con varias instancias y cada una de ellas representa un historial del registro "Archivos enviados". Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este historial del registro
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI)
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning , Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Sha1**: hash Sha-1 del archivo enviado.
- **File**: archivo enviado.
- **Size**: tamaño del archivo enviado.
- **Category**: categoría del archivo enviado.
- **Reason**: motivo del envío del archivo.
- **SentTo**: departamento de ESET al que se envió el archivo.
- **User**: cuenta de usuario que provocó la generación de este suceso del registro.

ESET_OneDriveScanLogs

La clase ESET_OneDriveScanLogs cuenta con varias instancias y cada una de ellas representa una ejecución del análisis de OneDrive, que equivale a la lista de registros "Análisis de OneDrive" de la interfaz gráfica de usuario. Cada instancia incluye los siguientes elementos:

- **ID**: identificador único de este registro de OneDrive.
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **Targets** : carpetas/objetos destino del análisis.
- **TotalScanned**: número total de objetos analizados.
- **Infected**: número de objetos infectados encontrados.
- **Cleaned**: número de objetos desinfectados.
- **Status**: estado del proceso de análisis.

ESET_OneDriveScanLogRecords

La clase ESET_OneDriveScanLogRecords cuenta con varias instancias, y cada una de ellas representa un historial del registro en uno de los registros de análisis representados por las instancias de la clase ESET_OneDriveScanLogRecords. Las instancias de esta clase contienen historiales de registro de todos los análisis/registros de OneDrive. Cuando solo se requiere la instancia de un registro de análisis determinado, debe filtrarse por medio de la propiedad LogID. Cada instancia contiene los siguientes elementos:

- **LogID**: identificador del registro de análisis al que pertenece este historial (identificador de una de las instancias de la clase ESET_OneDriveScanLogs).
- **ID**: identificador único de este registro de OneDrive.
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log**: mensaje de registro real.

Acceso a datos proporcionados

A continuación se exponen varios ejemplos de cómo acceder a los datos WMI de ESET desde la línea de comandos de Windows y PowerShell, herramientas que deberían funcionar en cualquier sistema operativo Windows. Además de estas, hay otras muchas formas de acceder a los datos desde otros lenguajes y herramientas de scripts.

Línea de comandos sin scripts

La herramienta de la línea de comandos `wmic` puede utilizarse para acceder a varias clases WMI predefinidas y personalizadas.

Si desea mostrar información completa sobre el producto del ordenador local:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Para mostrar únicamente el número de versión del producto del ordenador local:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Para mostrar toda la información del producto de un ordenador remoto con la IP 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Obtener y mostrar información completa sobre el producto del ordenador local:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Obtener y mostrar toda la información del producto de un ordenador remoto con la IP 10.1.118.180:

```
$cred = Get-Credential # promts the user for credentials and stores it in the
variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred
$cred
```

ESET PROTECT objetos del análisis

Esta funcionalidad permite a ESET PROTECT utilizar objetos de análisis (análisis a petición de base de datos de buzones y Análisis Hyper-V) cuando se ejecuta la tarea del cliente **Análisis del servidor** en un servidor con ESET Server Security. El ajuste de objetos de análisis ESET PROTECT solo está disponible si tiene ESET Management Agent instalado; de lo contrario, aparecerá atenuado.

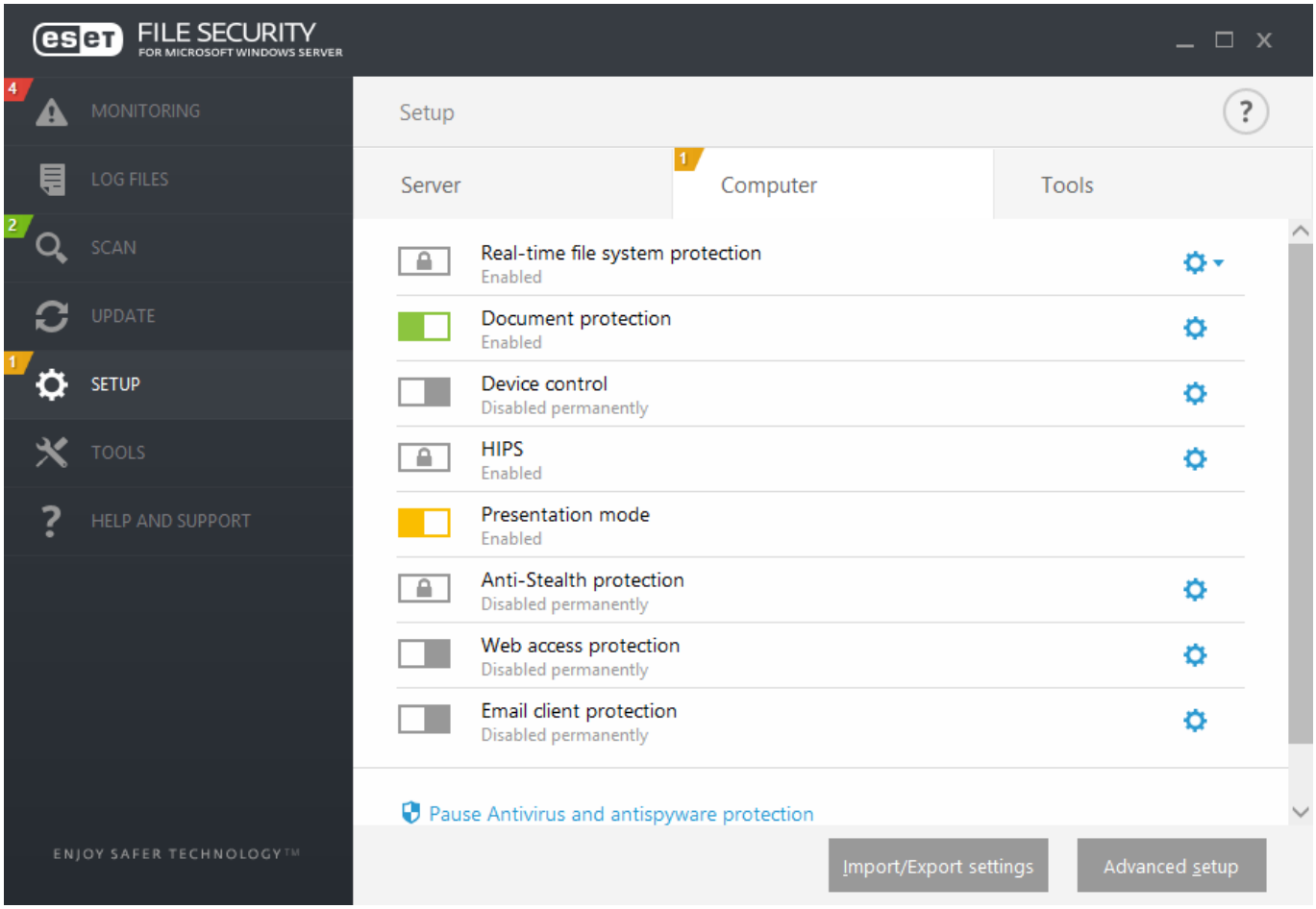
Cuando se activa **Generar lista de objetos**, ESET Server Security crea una lista de objetos de análisis disponibles. Esta lista se genera periódicamente en función del **Periodo de actualización** definido.

NOTA
La primera vez que se activa **Generar lista de objetos**, ESET PROTECT tarda aproximadamente la mitad del tiempo especificado en **Periodo de actualización** en recopilar la lista. Esto significa que si el valor de **Periodo de actualización** es de 60 minutos, ESET PROTECT tardará unos 30 minutos en recibir la lista de objetos de análisis. Si necesita que ESET PROTECT recopile la lista antes, establezca el periodo de actualización en un valor más bajo. Siempre puede aumentarlo posteriormente.

Cuando ESET PROTECT ejecute la tarea del cliente **Análisis del servidor**, recopilará la lista y se le pedirá que seleccione los objetos para el Análisis Hyper-V en ese servidor determinado.

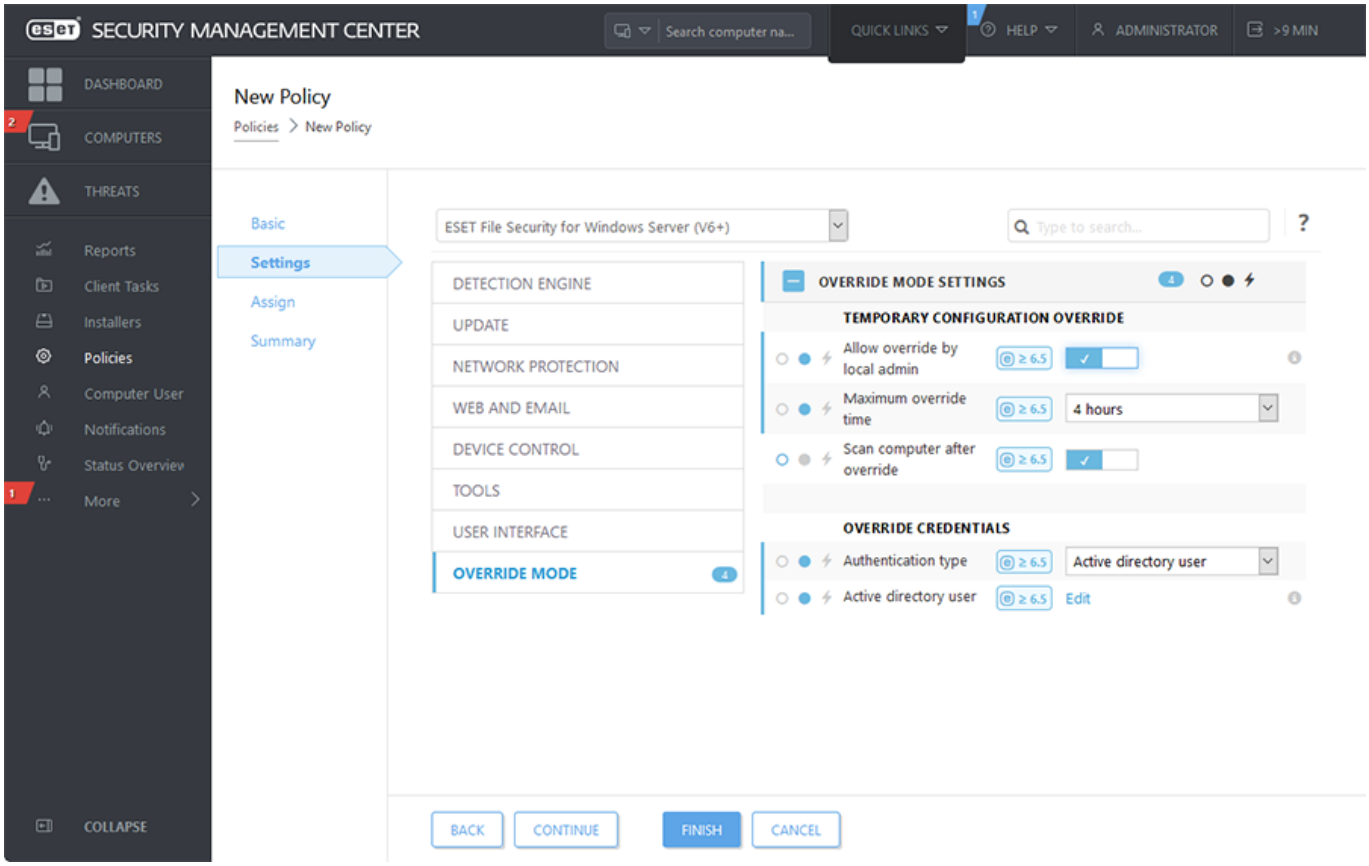
Modo de anulación

Si tiene la política de ESET PROTECT aplicada a ESET Server Security, verá un icono de candado en vez del conmutador Activar/desactivar en la página Configuración y un icono de candado junto al conmutador en la ventana **Configuración avanzada**.

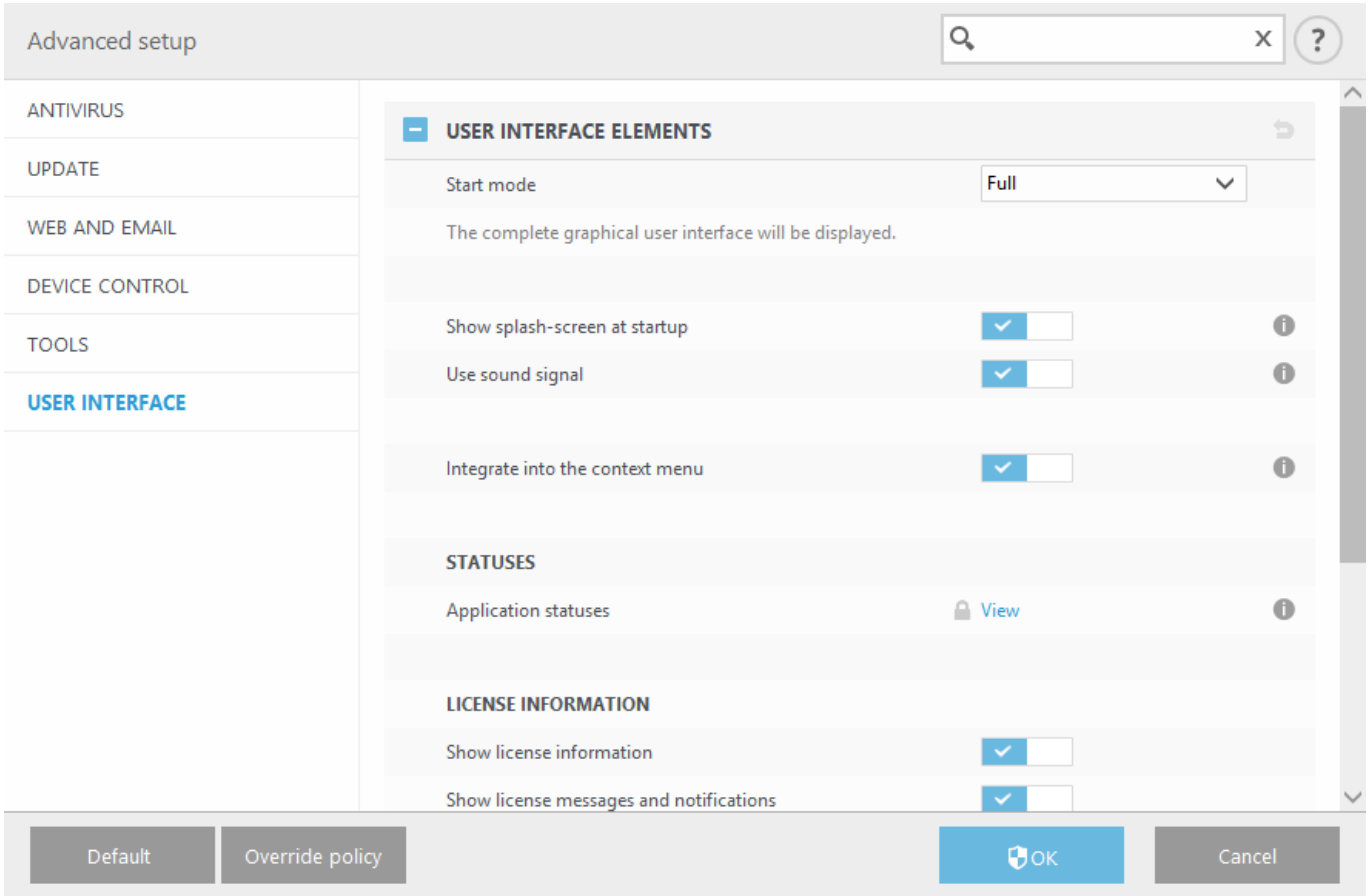


Normalmente, los ajustes configurados a través de la política de ESET PROTECT no se pueden modificar. El modo de anulación le permite desbloquear temporalmente estos ajustes. No obstante, debe activar **Modo de anulación** utilizando la política de ESET PROTECT.

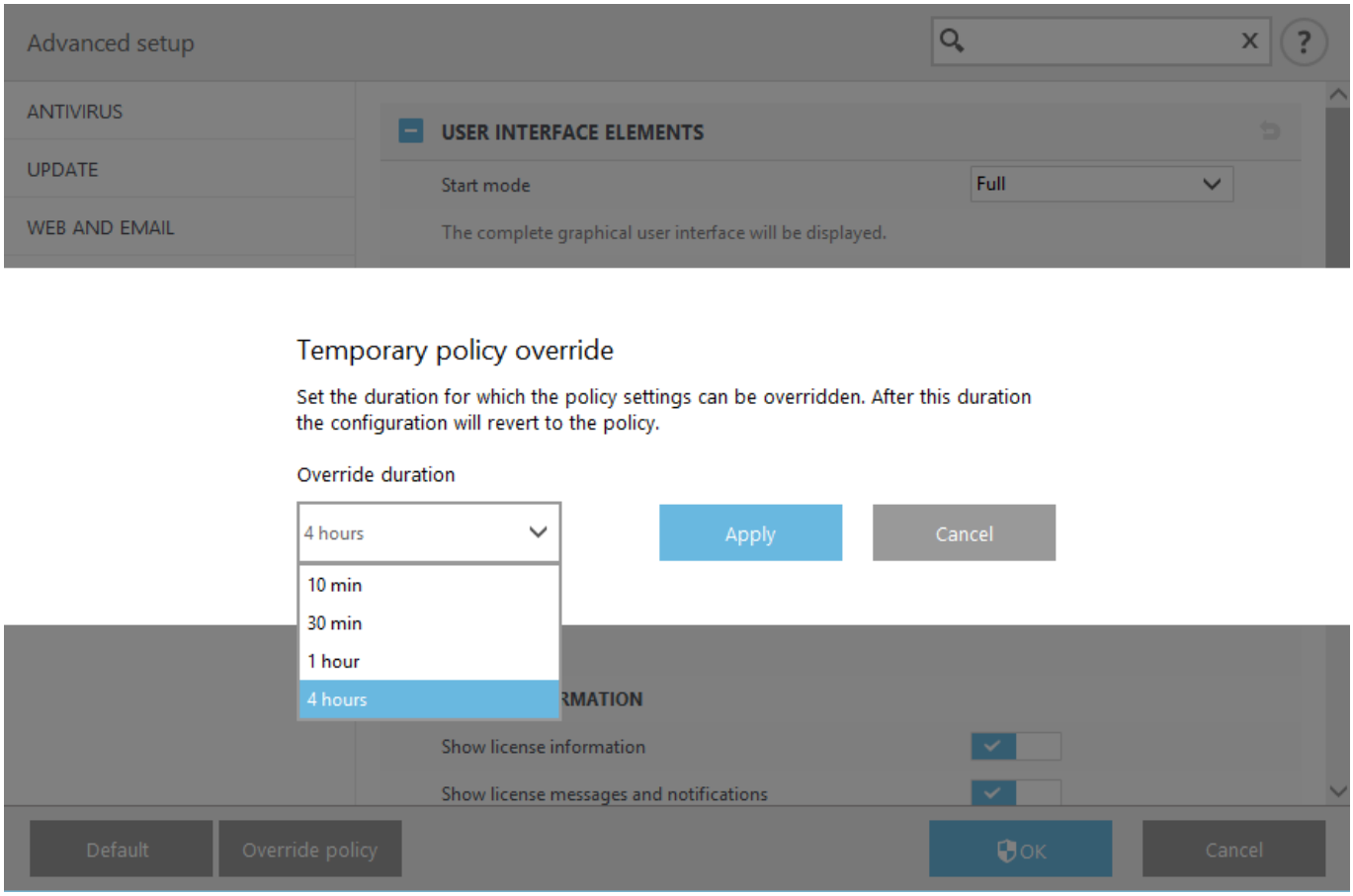
Inicie sesión en ESET PROTECT Web Console, vaya a **Políticas**, seleccione y modifique la política existente aplicada a ESET Server Security o cree una nueva. En **Configuración**, haga clic en **Modo de anulación**, actívelo y configure el resto de sus ajustes, incluido Tipo de autenticación (**Usuario de Active Directory** o **Contraseña**).



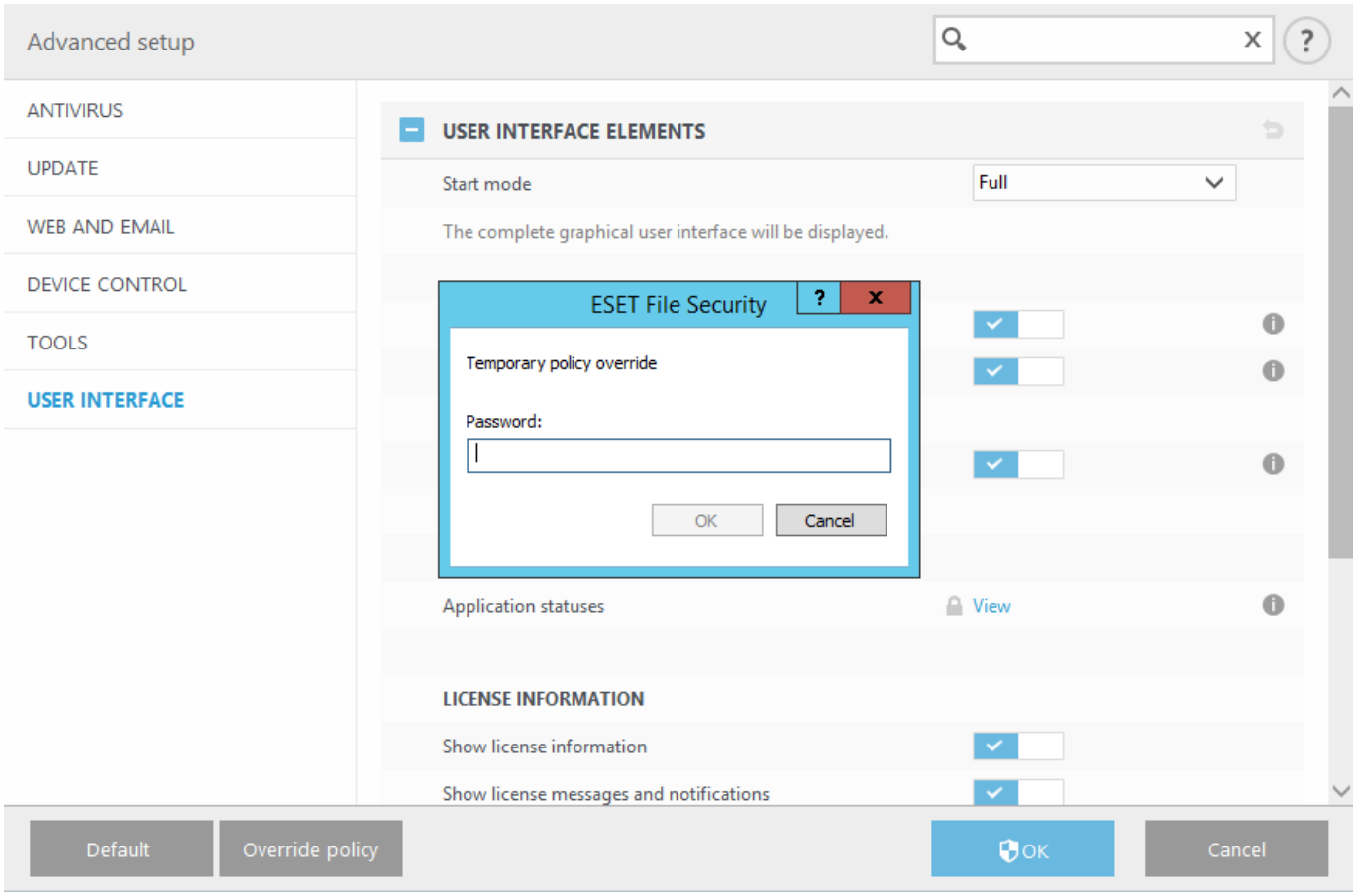
Una vez modificada la política o aplicada la nueva política a ESET Server Security, aparecerá el botón Anular política en la ventana Configuración avanzada.



Haga clic en el botón **Anular política**, configure la duración y haga clic en **Aplicar**.



Si seleccionó **Contraseña** como Tipo de autenticación, introduzca la contraseña de la anulación de la política.



Cuando caduque el Modo de anulación, los cambios de configuración que haya realizado volverán a la

configuración original de la política de ESET PROTECT. Verá una notificación antes de que caduque la Anulación.

Puede seleccionar **Finalizar anulación** en cualquier momento antes de que caduque en la página Estado de la protección o en la ventana **Configuración avanzada**.

Archivos de registro

Esta sección le permite modificar la configuración del registro de ESET Server Security.

Filtro de registros

Genera una gran cantidad de datos porque todas las opciones de registro están activadas de forma predeterminada. Le recomendamos desactivar de forma selectiva el registro de los componentes que no sean útiles o que estén relacionados con el problema.

> NOTA
> Para iniciar el registro real tendrá que activar el **Registro de diagnóstico** general a nivel de producto en el menú principal, **Configuración** > Herramientas. Una vez que el propio registro esté activado, ESET Server Security recopilará registros detallados según las funciones que se activen en esta sección.

Utilice los conmutadores para activar o desactivar cada función. Estas opciones también se combinan en función de la disponibilidad de los componentes individuales de ESET Server Security

- **Registro de diagnóstico del clúster**: el registro del clúster se incluirá en el registro de diagnóstico general.

Archivos de registro

Defina cómo se gestionarán los registros. Esto es importante sobre todo para evitar un uso excesivo del disco. La configuración predeterminada permite la eliminación automática de registros más antiguos para ahorrar espacio en disco.

Eliminar automáticamente los registros con una antigüedad de más de (días)

Las entradas de registro anteriores al número de días especificado se eliminarán.

Eliminar automáticamente registros antiguos si se supera el tamaño máximo del registro

Cuando el tamaño del registro supera el valor de **Tamaño máx. del registro [MB]**, los registros antiguos se eliminan hasta que se alcanza el valor de **Tamaño reducido del registro [MB]**.

Realizar copia de seguridad automática de los registros eliminados

Se realizará una copia de seguridad automática de los historiales y archivos de registro eliminados automáticamente en el directorio especificado; si se especifica, se comprimirán como archivos ZIP.

Realizar copia de seguridad de los registros de diagnóstico

Se realizará una copia de seguridad automática de los registros de diagnóstico eliminados automáticamente.

Si esta opción no está activada, no se realizará copia de seguridad de los historiales de registro de diagnóstico.

Carpeta de copia de seguridad

Carpeta en la que se almacenarán las copias de seguridad de los registros. Puede activar Comprimir las copias de seguridad de registros en formato ZIP.

Optimizar archivos de registro automáticamente

Si se selecciona esta opción, los archivos de registro se desfragmentarán automáticamente si el porcentaje de fragmentación es superior al valor especificado en el campo **Si la cantidad de registros eliminados supera el (%)**. Haga clic en **Optimizar** para empezar la desfragmentación de los archivos de registro. Se eliminan todas las entradas vacías del registro para mejorar el rendimiento y aumentar la velocidad del proceso de registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

Habilitar formato del texto

Para activar el almacenamiento de registros en otro formato de archivo, por separado de Archivos de registro:

- **Directorio de destino**: directorio donde se almacenarán los archivos de registro (solo se aplica a los formatos de **Texto/CSV**). Cada sección de registros tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, *virlog.txt* para la sección Amenazas detectadas de Archivos de registro, si se utiliza un archivo de texto sin formato para almacenar registros).
- **Tipo**: si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto y los datos se separarán mediante tabuladores. El comportamiento es el mismo para el formato de archivo **CSV** con datos separados por comas. Si selecciona **Suceso**, los registros se almacenarán en el registro de eventos de Windows (que se puede ver en el Visor de eventos del Panel de control), en vez de en un archivo.
- **Eliminar todos los archivos de registro**: borra todos los registros almacenados que se seleccionen en el menú desplegable **Tipo**.

NOTA
El servicio de Soporte técnico de ESET podría solicitarle los registros de su ordenador para agilizar la solución de problemas. El ESET Log Collector facilita la recopilación de los datos necesarios. Para obtener más información sobre el ESET Log Collector, consulte el artículo de la Base de conocimiento.

Registro de auditoría

Realizar un control de los cambios realizados en la configuración o la protección. Como la modificación del producto puede tener una influencia importante en el funcionamiento del producto, en algunos casos se recomienda controlar los cambios con fines de auditoría. Puede ver los registros de cambios en la sección **Archivos de registro** > Registro de auditoría.

Servidor Proxy

En las redes LAN de gran tamaño, un servidor Proxy puede mediar en la conexión del ordenador a Internet. Si este es el caso, es necesario definir los siguientes ajustes. Si no lo hace, el programa no se podrá actualizar de manera

automática. En ESET Server Security, el servidor proxy se puede configurar en dos secciones diferentes de la ventana **Configuración avanzada** (**F5**):

1. **Configuración avanzada** (**F5**) > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** > Proxy HTTP
   Esta configuración se aplica al perfil de actualización indicado y se recomienda para ordenadores portátiles que suelen recibir módulos de distintas ubicaciones.

2. **Configuración avanzada** (**F5**) > **Herramientas** > **Servidor proxy**
   Especificar el servidor proxy a este nivel define los ajustes del servidor proxy a nivel global para todas las instancias de ESET Server Security. Todos los módulos conectados a Internet utilizarán estos parámetros.

Para especificar la configuración del servidor proxy en este nivel, active el conmutador **Usar servidor proxy** y, a continuación, especifique la dirección del servidor proxy en el campo **Servidor proxy** y su número de **Puerto**.

El servidor proxy requiere autenticación

Si la comunicación de red a través del servidor proxy requiere la autenticación, active esta opción y especifique un **Nombre de usuario** y **Contraseña**.

Detectar el servidor proxy

Haga clic en **Detectar** para detectar y cumplimentar la configuración del servidor proxy de forma automática. Se copiarán los parámetros especificados en Internet Explorer.

NOTA
Esta función no recupera los datos de autenticación (nombre de usuario y contraseña); debe proporcionarlos.

Usar conexión directa si el proxy no está disponible

Si un producto está configurado para utilizar un proxy HTTP y el proxy está inaccesible, el producto ignorará el proxy y se comunicará directamente con los servidores de ESET.

Notificaciones

Las notificaciones del escritorio y los globos de sugerencias son medios de información que no requieren la intervención del usuario. Se muestran en el área de notificación, situada en la esquina inferior derecha de la pantalla. A continuación encontrará más opciones avanzadas, como la modificación del tiempo de visualización de las notificaciones y la transparencia de las ventanas. Active el conmutador **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa** para suprimir todas las notificaciones que no sean interactivas.

Mostrar notificación de actualización correcta

Cuando se realice una actualización correctamente, se mostrará una notificación emergente.

Enviar notificaciones de sucesos por correo electrónico

Habilite esta opción para activar las notificaciones por correo electrónico.

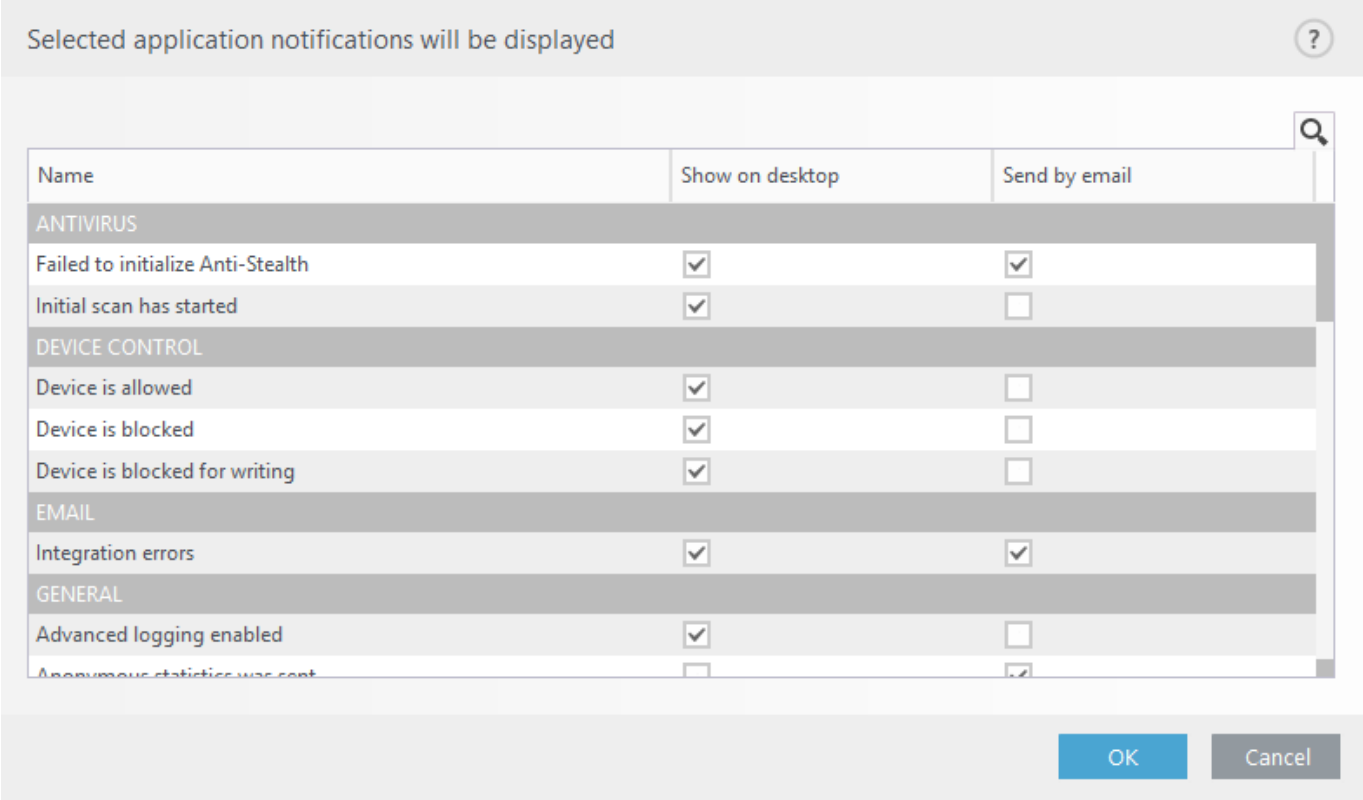
Notificaciones de aplicaciones

Haga clic en Editar para activar o desactivar la visualización de notificaciones de aplicaciones.

Notificaciones de aplicaciones

Puede configurar las notificaciones de ESET Server Security para que se muestren en el escritorio o se envíen por correo electrónico.

NOTA
Para las notificaciones por correo electrónico, asegúrese de activar **Enviar notificaciones de sucesos por correo electrónico** en la sección **Básico** y luego configure el servidor SMTP y otros detalles según sea necesario.



Notificaciones en el escritorio

Le permite configurar cómo ESET Server Security gestiona las alertas de amenaza y las notificaciones del sistema (como los mensajes de actualización correcta). Por ejemplo, la **Duración** del tiempo de visualización y la **Transparencia** de las notificaciones en la bandeja del sistema (esto se aplica únicamente a los sistemas que admiten notificaciones en la bandeja del sistema).

En el menú desplegable **Nivel mínimo de detalle de los sucesos a mostrar** puede seleccionar el nivel de gravedad de las alertas y notificaciones. Están disponibles las opciones siguientes:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".

- **Crítico**: registra únicamente errores críticos.

En el campo **En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este usuario** se especifica el usuario que recibirá notificaciones del sistema y de otro tipo en sistemas que permitan la conexión de varios usuarios al mismo tiempo. Normalmente, este usuario es un administrador de sistemas o de redes. Esta opción resulta especialmente útil para servidores de terminal, siempre que todas las notificaciones del sistema se envíen al administrador.

Notificaciones por correo electrónico

ESET Server Security puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado.

> NOTA
> Los servidores SMTP con cifrado TLS son compatibles con ESET Server Security.

Servidor SMTP

El nombre del servidor de SMTP empleado para enviar alertas y notificaciones. Habitualmente es el nombre del servidor de Microsoft Exchange.

Nombre de usuario y contraseña

Si el servidor SMTP requiere autenticación, estos campos deben cumplimentarse con un nombre de usuario y una contraseña válidos que faciliten el acceso al servidor SMTP.

Dirección del remitente

Introduzca la dirección del remitente que aparecerá en el encabezado de los correos electrónicos de notificación. Esto es lo que verá el destinatario en el campo **De**.

Dirección del destinatario

Especifique la dirección de correo electrónico del destinatario **Para** al que se entregarán las notificaciones.

Habilitar TLS

Active el envío de mensajes de notificación y alerta que admite el cifrado TLS.

Configuración de correo electrónico

Nivel mínimo de detalle para las notificaciones

Especifica el nivel mínimo de detalle de las notificaciones que se enviarán.

Intervalo tras el que se enviarán nuevos correos electrónicos de notificación (min)

Intervalo en minutos tras el cual se enviarán nuevas notificaciones mediante correo electrónico. Si desea que estas notificaciones se envíen inmediatamente, ajuste este valor a 0.

Enviar cada notificación en un correo electrónico distinto

Si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría suponer la recepción de numerosos correos electrónicos en un breve periodo de tiempo.

Formato de mensajes

Las comunicaciones entre el programa y un usuario o administrador de sistemas remotos se realizan a través de mensajes de correo electrónico o mensajes de red local (mediante el servicio de Messenger de Windows). El formato predeterminado de los mensajes de alerta y las notificaciones será el óptimo para la mayoría de situaciones. En algunas circunstancias, tendrá que cambiar el formato de los mensajes de sucesos.

Para notificar la ocurrencia de sucesos

Formato de los mensajes de suceso que se muestran en los ordenadores remotos.

Para alertar sobre amenazas

Los mensajes de notificación y alerta de amenazas tienen un formato predefinido de forma predeterminada. Le aconsejamos que no modifique este formato. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes.

Las palabras clave (cadenas separadas por signos %) se sustituyen en el mensaje por la información real especificada. Están disponibles las siguientes palabras clave:

- **%TimeStamp%**: fecha y hora del suceso.
- **%Scanner%**: módulo correspondiente.
- **%ComputerName%**: nombre del ordenador en el que se produjo la alerta.
- **%ProgramName%**: programa que generó la alerta.
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectados.
- **%VirusName%**: identificación de la infección.
- **%ErrorDescription%**: descripción de un suceso que no está relacionado con un virus.

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se utilizan en los mensajes de alerta de amenaza y **%ErrorDescription%**, en los mensajes de sucesos.

Conjunto de caracteres

Puede elegir la codificación en el menú desplegable. El mensaje de correo electrónico se convertirá según la codificación de caracteres seleccionada.

Usar codificación Quoted-printable

El origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo puede transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (áéíóú).

Personalización

Este mensaje se mostrará en el pie de página de todas las notificaciones seleccionadas.

Mensaje de notificación predeterminado

Un mensaje predeterminado que se mostrará en el pie de página de las notificaciones.

Amenazas

No cerrar las notificaciones de malware automáticamente

Activa la opción de que las notificaciones de malware permanezcan en pantalla hasta que las cierra manualmente.

Usar mensaje predeterminado

Puede desactivar el mensaje predeterminado y especificar un **Mensaje de notificación de amenaza** personalizado que se mostrará cuando se bloquee una amenaza.

Mensaje de notificación de amenaza

Introduzca el mensaje personalizado que desea mostrar cuando se bloquea una amenaza.

Modo de presentación

El modo presentación es una función para usuarios que demandan el uso ininterrumpido de su software, no desean ser interrumpidos por ventanas emergentes y quieren reducir al mínimo el uso de la CPU. El modo presentación también puede utilizarse durante presentaciones que no puedan ser interrumpidas por la actividad de ESET Server Security. Cuando está activado, se desactivan todas las ventanas emergentes y las tareas programadas no se ejecutan. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere interacción del usuario.

Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa

El modo Presentación se activa automáticamente cada vez que ejecuta una aplicación a pantalla completa. Con el modo Presentación activado, no podrá ver notificaciones ni un cambio de estado de su ESET Server Security.

Deshabilitar el modo de presentación automáticamente después de

Para definir la cantidad de tiempo, en minutos, que tardará en desactivarse automáticamente el modo Presentación.

Diagnósticos

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, *ekrn*). Cuando una aplicación se bloquea, se genera un volcado de memoria que puede ayudar a los desarrolladores a depurar y arreglar ESET Server Security problemas diversos.

Haga clic en el menú desplegable situado junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- **Desactivar**: para desactivar esta función.
- **Mini** (opción predeterminada): registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de volcado puede resultar útil cuando el espacio es limitado. Sin embargo, dada la poca información que proporciona, es posible que el análisis de este archivo no detecte los errores que no estén relacionados directamente con el subproceso que se estaba ejecutando cuando se produjo el problema.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.

Directorio de destino

Directorio en el que se genera el volcado durante el bloqueo.

Abrir la carpeta de diagnóstico

Haga clic en **Abrir** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

Crear volcado de diagnóstico

Haga clic en **Crear** para crear archivos de volcado de diagnóstico en el directorio de destino.

Registro avanzado

Activar registro avanzado de Control de dispositivos

Registre todos los sucesos que se produzcan en Control de dispositivos para permitir el diagnóstico y la resolución de problemas.

Activar registro avanzado del núcleo

Registre todos los sucesos que se produzcan en el servicio del núcleo de ESET (`ekrn`) para permitir el diagnóstico y la resolución de problemas.

Activar registro avanzado de licencias

Registrar todas las comunicaciones del producto con el servidor de licencias.

Activar registro avanzado de la protección de red

Registre todos los datos de red que pasan a través de la protección de red en formato PCAP con el fin de ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con la protección de red.

Activar registro avanzado del sistema operativo

Se recopilará información adicional sobre el sistema operativo, tal como los procesos en ejecución, la actividad de la CPU, las operaciones del disco, etc.

Activar el registro avanzado del filtrado de protocolos

Registre todos los datos que pasan a través del motor de filtrado de protocolos en formato PCAP con el fin de ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el filtrado de protocolos.

Activar registro avanzado del motor de actualización

Registre todos los eventos que se producen durante el proceso de actualización con el fin de ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el motor de actualización.

Soporte técnico

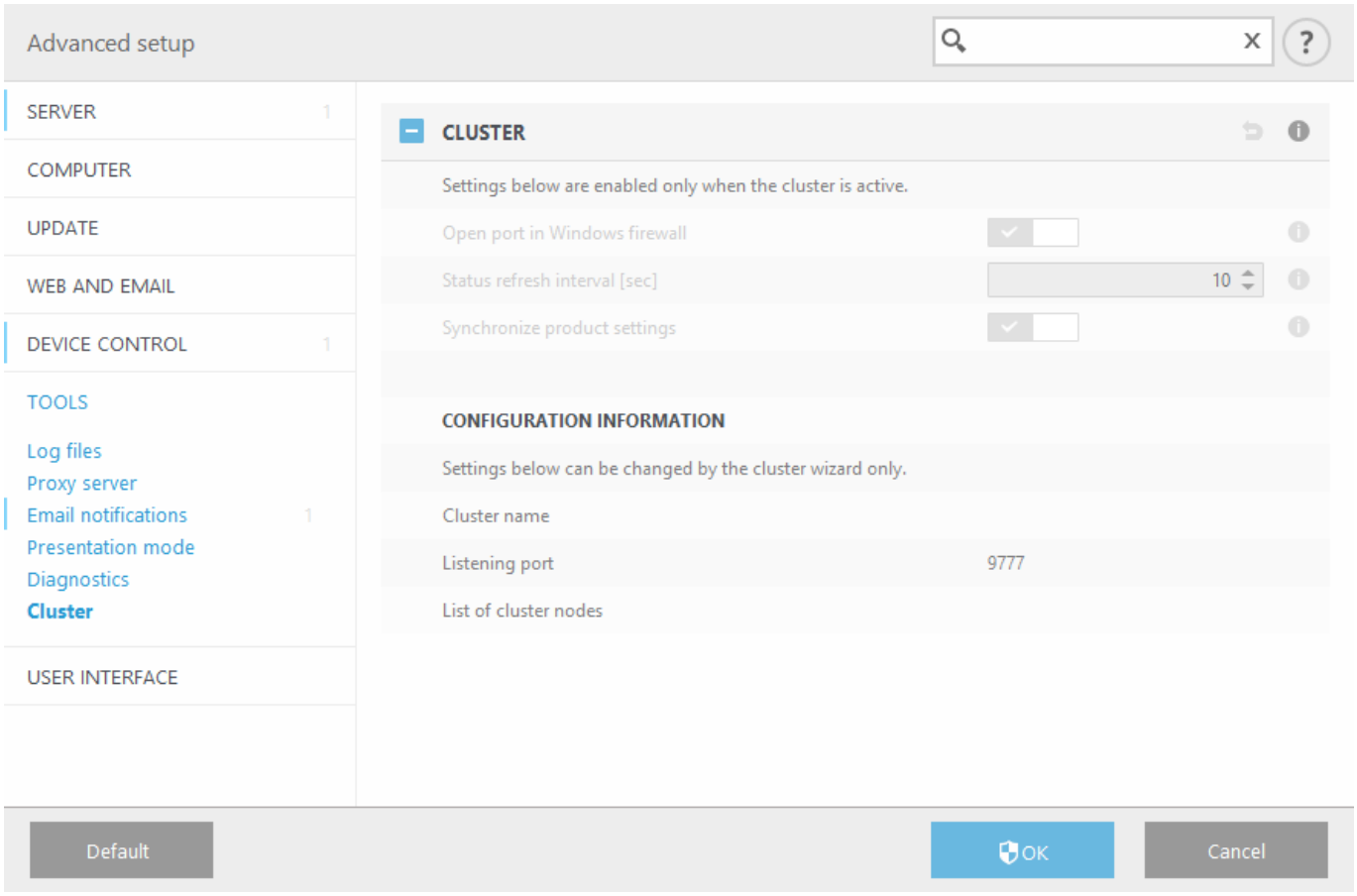
Enviar datos de configuración del sistema

Seleccione **Enviar siempre** para que no se le pregunte antes de enviar sus datos de configuración de ESET Server Security al servicio de atención al cliente o utilice la opción **Preguntar antes de enviar**.

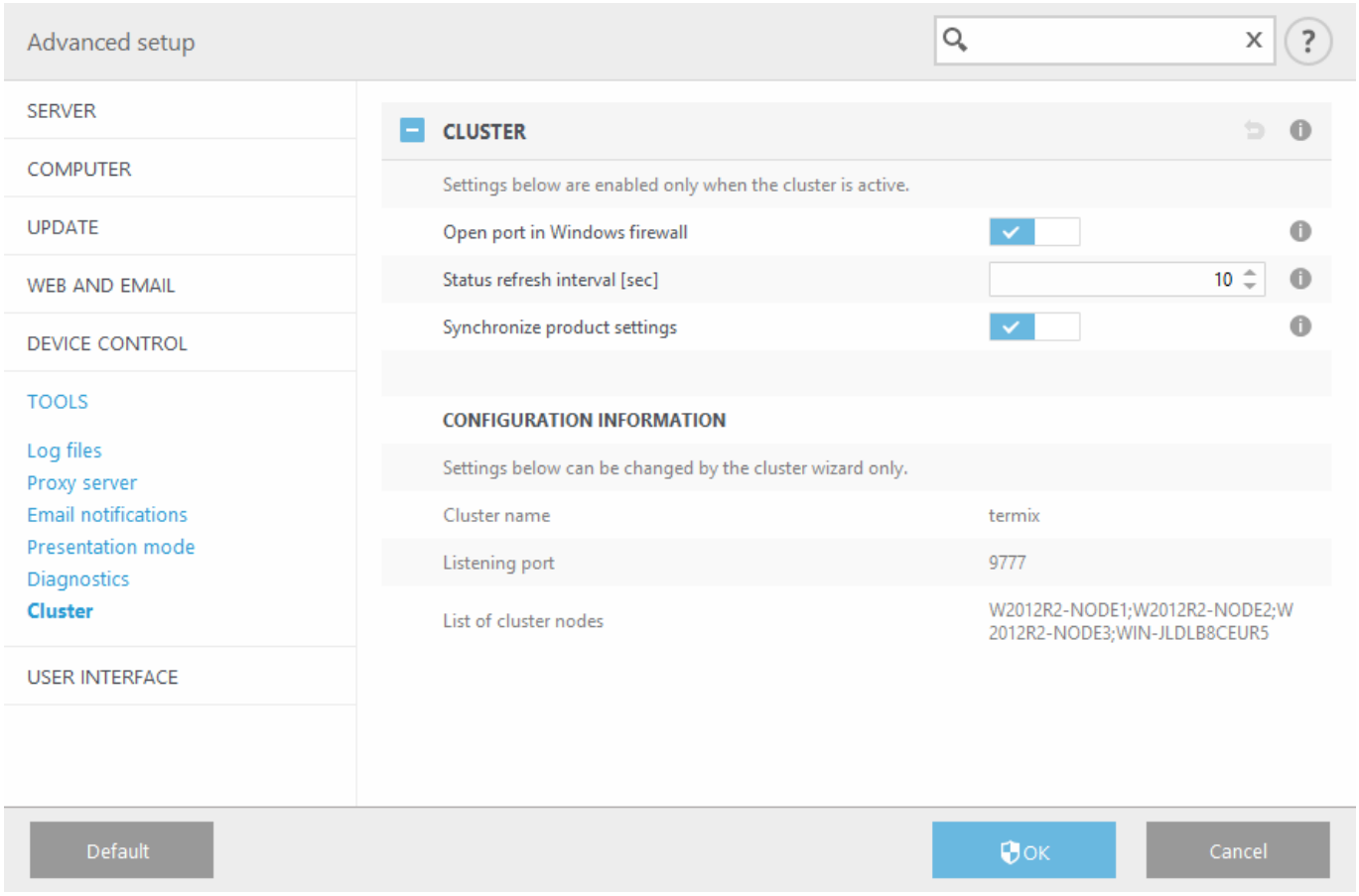
Clúster

La opción Activar clúster se activa automáticamente cuando se configura el Clúster de ESET. Puede desactivarla manualmente en la ventana de **Configuración avanzada** (**F5**); para ello, haga clic en el icono del conmutador (es una opción idónea cuando necesita cambiar la configuración sin que esto tenga consecuencias sobre el resto de nodos del Clúster de ESET). Este conmutador solo activa o desactiva la funcionalidad Clúster de ESET. Para configurar o destruir el clúster, utilice el Asistente de clúster o la opción **Destruir** el clúster de la sección **Herramientas** > **Clúster** de la ventana principal del programa.

Clúster de ESET no configurado y desactivado:



Clúster de ESET correctamente configurado con sus detalles y opciones:



Interfaz de usuario

Configure el comportamiento de la interfaz gráfica de usuario (GUI) de ESET Server Security. Es posible ajustar el aspecto y los efectos visuales del programa.

Elementos de la interfaz del usuario

Utilice el menú desplegable Modo de inicio GUI para seleccionar uno de los siguientes modos de inicio de la interfaz gráfica de usuario (GUI):

- **Completo**: se muestra la GUI completa.
- **Terminal**: no se muestra ninguna notificación ni alerta. La GUI solo la puede iniciar el administrador. Si los elementos gráficos ralentizan el ordenador o provocan otros problemas, establezca la interfaz de usuario en Terminal. También se recomienda desactivar la interfaz gráfica de usuario en un Terminal Server. Si desea obtener más información sobre la instalación de ESET Server Security en un Terminal Server, consulte el tema Desactivar la GUI en Terminal Server.

Mostrar la pantalla de bienvenida al iniciar el programa

Desactive esta opción si prefiere que no se muestre la pantalla de bienvenida al iniciar la GUI de ESET Server Security, por ejemplo, cuando inicie sesión en el sistema.

Usar señal acústica

ESET Server Security reproduce un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis.

Integrar en el menú contextual

Al activar esta opción, los elementos de control de ESET Server Security se integran en el menú contextual. El menú contextual aparece al hacer clic con el botón derecho en un objeto (archivo). En el menú se muestra una lista de todas las acciones que se pueden realizar en un objeto.

Estados de la aplicación

Haga clic en Editar para seleccionar los estados que se muestran en la ventana Supervisión. También puede utilizar Políticas de ESET PROTECT para configurar los estados de su aplicación. El estado de una aplicación también se muestra cuando no se ha activado el producto o si la licencia ha caducado.

Información de la licencia/Mostrar información de licencia

Si esta opción está activada, aparecerán mensajes y notificaciones sobre su licencia.

Cuadros de alertas y mensajes

Al configurar Alertas y notificaciones puede cambiar el comportamiento de las alertas de amenaza detectadas y las notificaciones del sistema, que se pueden adaptar a las necesidades de cada uno. Si elige la opción de no mostrar algunas notificaciones, estas se mostrarán en el área Mensajes y estados desactivados. Aquí puede comprobar su estado, ver más información o eliminarlas de esta ventana.

Configuración de acceso

Puede evitar cambios no autorizados con la herramienta Configuración de acceso para garantizar un nivel alto de seguridad.

ESET Shell

Puede configurar los derechos de acceso a la configuración del producto, sus funciones y los datos que contiene desde eShell, mediante la modificación de la política de ejecución de ESET Shell.

Icono en la bandeja del sistema

Restaurar la configuración de esta sección

Cuadros de alertas y mensajes

Le permite configurar cómo ESET Server Security gestiona las alertas de amenaza y las notificaciones del sistema (como los mensajes de actualización correcta). Por ejemplo, la **Duración** del tiempo de visualización y la **Transparencia** de las notificaciones en la bandeja del sistema (esto se aplica únicamente a los sistemas que admiten notificaciones en la bandeja del sistema).

Mostrar alertas interactivas

Si no desea que ESET Server Security muestre alertas en el área de notificación de Windows, desactive esta función.

Lista de alertas interactivas

Útil para la automatización. Anule la selección de la opción **Preguntar al usuario** para los elementos que quiera automatizar y elija la acción que se realizará en lugar de que la ventana de alerta espere su interacción.

Las **ventanas de notificación** se utilizan para mostrar preguntas o mensajes de texto corto.

Cerrar ventanas de notificación automáticamente

Esta opción se utiliza para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado. Si no se cierran de forma manual, las ventanas de alerta se cerrarán automáticamente cuando haya transcurrido el periodo de tiempo especificado.

Mensajes de confirmación

Si hace clic en **Editar**, aparecerá una ventana emergente con una lista de mensajes de confirmación que ESET Server Security muestra antes de realizar cualquier acción. Utilice las casillas para personalizar sus preferencias para los mensajes de confirmación.

Configuración de acceso

Para la máxima seguridad del sistema, es esencial que ESET Server Security esté configurado de forma correcta. Una modificación incorrecta puede provocar problemas o incluso la pérdida de datos importantes. Para evitar modificaciones incorrectas, la configuración de ESET Server Security se puede proteger mediante contraseña.

IMPORTANTE
Si desinstala ESET Server Security mientras utiliza la protección por contraseña de configuración de acceso, se le pedirá que introduzca la contraseña. De lo contrario, no podrá desinstalar ESET Server Security.

Configuración de la protección por contraseña

Bloquea o desbloquea los parámetros de configuración del programa. Haga clic en la ventana **Configuración de la contraseña**.

Establecer contraseña

Para establecer o cambiar una contraseña que proteja los parámetros de configuración, haga clic en **Establecer**. Debe definir una nueva contraseña para proteger los parámetros de configuración de ESET Server Security con el fin de evitar modificaciones no autorizadas. Si desea cambiar una contraseña, escriba la contraseña actual en el campo **Contraseña anterior**, escriba la nueva contraseña en los campos **Contraseña nueva** y **Confirmar contraseña**; a continuación, haga clic en **Aceptar**. Esta contraseña será necesaria para realizar modificaciones en ESET Server Security.

Exigir derechos completos de administrador para cuentas de administrador limitadas

Seleccione esta opción para solicitar al usuario actual (si no tiene derechos de administrador) que introduzca las credenciales de la cuenta de administrador al modificar determinados parámetros, como, por ejemplo, la desactivación de los módulos de protección.

NOTA
Si la contraseña de Configuración de acceso cambia y desea importar un archivo de configuración *.xml* existente (que se firmó antes del cambio de la contraseña) desde la línea de comandos del CMD de ESET, asegúrese de firmarlo de nuevo con la contraseña actual. Esto le permitirá utilizar un archivo de configuración más antiguo sin necesidad de exportarlo en otra máquina que ejecute ESET Server Security antes de la importación.

ESET Shell

Puede configurar los derechos de acceso a la configuración del producto, sus funciones y los datos que contiene desde eShell, mediante la modificación de la **política de ejecución de ESET Shell**. El ajuste predeterminado es **Scripts limitados**, pero puede cambiarlo a Desactivado, Solo lectura o Acceso total en caso de ser necesario.

Deshabilitar

eShell no puede usarse. Solo se permite la configuración de eShell en el contexto de `ui eshell`. Puede personalizar la apariencia de eShell, pero no puede acceder a ningún ajuste ni dato del producto.

Solo lectura

eShell puede usarse como herramienta de supervisión. Puede ver todos los ajustes en el Modo interactivo y por lotes, pero no puede modificar ningún ajuste, función ni dato.

Scripts limitados

En el Modo interactivo puede ver y modificar todos los ajustes, funciones y datos. En el Modo por lotes, eShell funcionará como si estuviera en el modo de solo lectura. Sin embargo, si usa archivos por lotes

firmados, podrá editar la configuración y modificar los datos.

Acceso total

Ofrece acceso a todos los ajustes de forma ilimitada, en el modo tanto interactivo como por lotes (al ejecutar archivos por lotes). Puede consultar y modificar cualquier ajuste. Debe usar una cuenta de administrador para ejecutar eShell con acceso total. Si el Control de cuentas de usuario (UAC) está activado, también se requiere elevación.

Desactivar la GUI en Terminal Server

En este capítulo se explica cómo desactivar la ejecución de la interfaz gráfica de usuario de ESET Server Security en Windows Terminal Server para las sesiones de usuario.

Normalmente, la GUI de ESET Server Security se inicia cada vez que un usuario remoto inicia sesión en el servidor y crea una sesión de Terminal, una acción que no suele ser deseable en los servidores Terminal Server. Si desea desactivar la GUI en las sesiones de Terminal, puede hacerlo desde eShell mediante la ejecución del comando `set ui ui gui-start-mode none`. De esta forma activará el modo terminal en la GUI. Estos son los dos modos disponibles para el inicio de la GUI:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

Si desea averiguar qué modo se está usando, ejecute el comando `get ui ui gui-start-mode`.

> NOTA
> Si ha instalado ESET Server Security en un servidor Citrix, le recomendamos que utilice la configuración descrita en el artículo de nuestra Base de conocimiento.

Mensajes y estados desactivados

Mensajes de confirmación

Le muestra una lista de mensajes de confirmación que se pueden seleccionar para que se muestren o no.

Configuración de estados de la aplicación

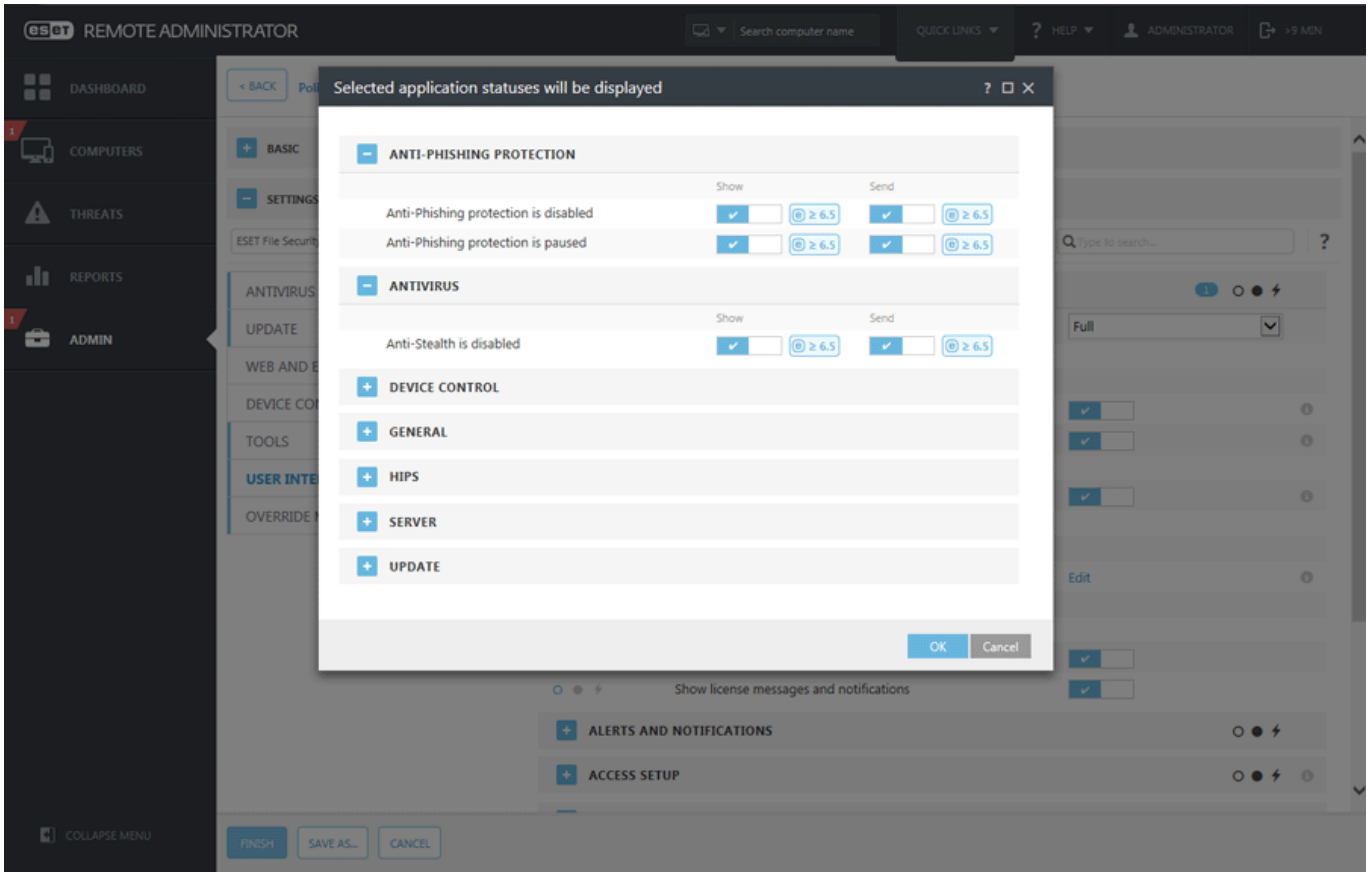
Le permite activar o desactivar la visualización de estado en la página Supervisión del menú principal.

Configuración de estados de la aplicación

En este cuadro de diálogo puede seleccionar los estados de la aplicación que desea que se muestren o no. Por ejemplo, si pausa la protección Antivirus y entiespía, se producirá un cambio en el estado de la protección que aparecerá en la página Estado de la protección. El estado de una aplicación también se muestra cuando no se ha activado el producto o si la licencia ha caducado.

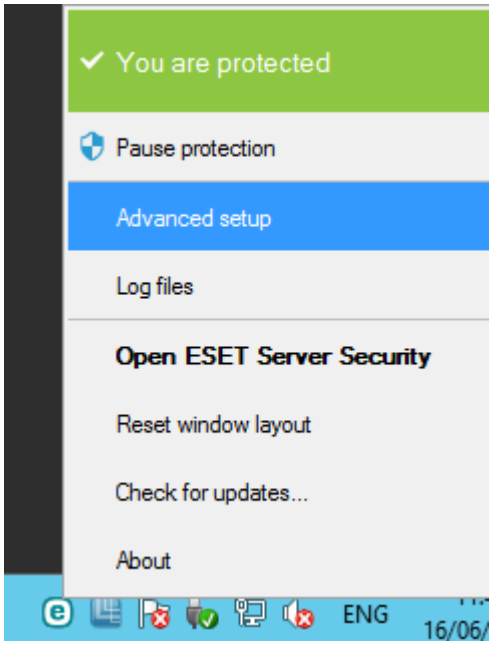
Los estados de la aplicación pueden administrarse a través de Políticas de ESET PROTECT. Las categorías y los estados se muestran en una lista con dos opciones: **Mostrar** y **Enviar** el estado. La columna Enviar los estados de la aplicación solo es visible en la configuración de la política de ESET PROTECT. ESET Server Security muestra la

configuración con un icono de candado. Puede utilizar Modo de anulación para cambiar temporalmente Estados de la aplicación.



Icono en la bandeja del sistema

Actúa como un acceso rápido a funciones y elementos utilizados con frecuencia de ESET Server Security. Estos elementos y funciones están disponibles al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema .



Más información

Abre la página Supervisión para mostrarle los mensajes y el estado de protección actual.

Pausar la protección

Muestra el cuadro de diálogo de confirmación que desactiva la Protección antivirus y antiespía, que protege el sistema frente a ataques mediante el control de archivos, Internet y la comunicación por correo electrónico. Cuando pause temporalmente la protección Antivirus y antiespía con el icono de la bandeja del sistema  , aparecerá el cuadro de diálogo **Pausar protección**. Al hacerlo se desactivará la protección relacionada con el malware durante el periodo de tiempo seleccionado. Para desactivar la protección de forma permanente debe hacerlo desde **Configuración avanzada**. Tenga cuidado, ya que desactivar la protección puede exponer su sistema a amenazas.

Configuración avanzada

Utilice esta opción para introducir la **Configuración avanzada**.

Archivos de registro

Incluyen información acerca de todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas.

Ocultar ESET Server Security

Le permite ocultar la ventana de ESET Server Security en la pantalla.

Restablecer posición y diseño de la ventana

Restablece el tamaño y la posición predeterminados de la ventana de ESET Server Security en la pantalla.

Buscar actualizaciones

Inicia la actualización de los módulos para garantizar el nivel de protección frente a código malicioso.

Acerca de

Contiene información del sistema y detalles acerca de la versión instalada de ESET Server Security, así como de los módulos del programa instalados y la fecha de caducidad de la licencia. Al final de la página encontrará información sobre el sistema operativo y los recursos del sistema.

Restaurar la configuración predeterminada

Puede restaurar la configuración predeterminada desde **Configuración avanzada**. Hay dos opciones: puede recuperar todos los ajustes predeterminados o solo los de una sección concreta (los ajustes de otras secciones permanecerán sin cambios).

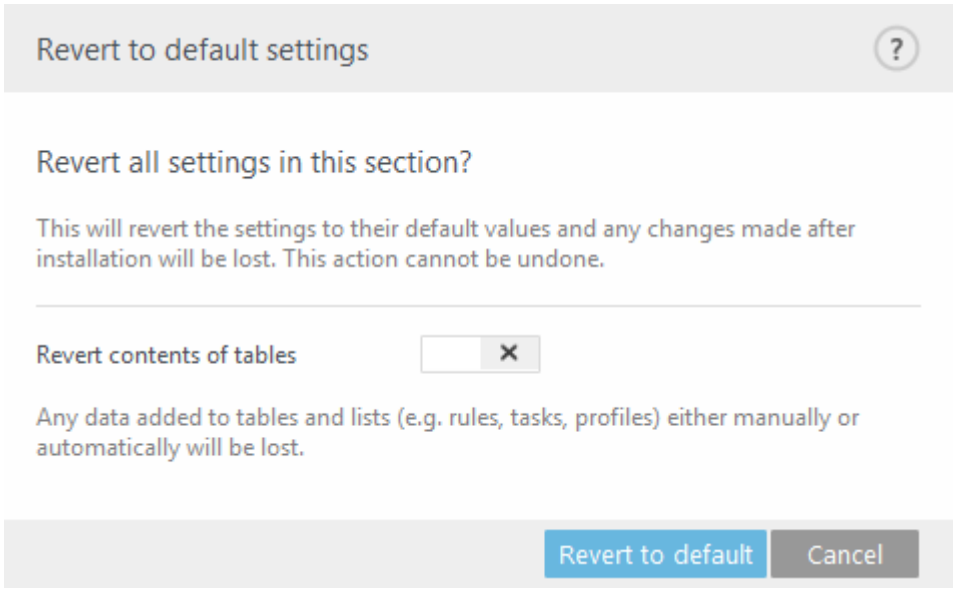
Restaurar toda la configuración

Todos los ajustes de todas las secciones de configuración avanzada se restaurarán al estado en el que se encontraban al instalar ESET Server Security. Es una opción similar a *Restaurar valores predeterminados de fábrica*.

NOTA
Al hacer clic en **Restaurar predeterminados** se perderán todos los cambios que se hubieran efectuado. Esta acción no se puede deshacer.

Restaurar la configuración de esta sección

Recupera los ajustes predeterminados del módulo en la sección seleccionada. Perderá todos los cambios que haya realizado en ella.



Restaurar el contenido de las tablas

Cuando se active, se perderán las reglas, tareas o perfiles que se hayan añadido de forma manual o automática.

Ayuda y asistencia técnica

ESET Server Security contiene herramientas de resolución de problemas e información de soporte que le ayudará a solucionar los problemas que se encuentre.

Ayuda

Buscar en la base de conocimientos de ESET

La Base de conocimiento ESET contiene respuestas a las preguntas más frecuentes y posibles soluciones a diferentes problemas. La actualización periódica por parte de los especialistas técnicos de ESET convierte esta base de conocimiento en la herramienta más potente para resolver diversos problemas.

Abrir la Ayuda

Abre las páginas de ayuda en línea de ESET Server Security.

Respuestas rápidas a consultas frecuentes

Seleccione esta opción para buscar soluciones a los problemas más frecuentes. Es recomendable que lea atentamente esta sección antes de ponerse en contacto con el equipo de asistencia técnica.

Soporte técnico

Enviar solicitud al servicio de asistencia técnica

Si no encuentra respuesta a su problema, también puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con nuestro departamento de Soporte técnico.

Detalles para el soporte técnico

Muestra información detallada (nombre del producto, versión del mismo, etc.) para el departamento de Soporte técnico.

Herramientas de soporte

Enciclopedia de amenazas

Es un enlace a la enciclopedia de amenazas de ESET, que contiene información sobre los peligros y los síntomas de diferentes tipos de amenaza.

ESET Log Collector

Establece un vínculo con la página de descargas del ESET Log Collector. Es una aplicación (ESET Log Collector) que recopila automáticamente información (por ejemplo de configuración) y registros del servidor para contribuir a acelerar la resolución de problemas.

Historial del Motor de detección

Proporciona un enlace al radar de virus de ESET, que contiene información sobre las versiones de los módulos de detección de ESET.

ESET Specialized Cleaner

El Limpiador especializado de ESET es una herramienta de eliminación para infecciones comunes por malware, como Conficker, Sirefef, Necurs, etc.

Información del producto y la licencia

Activar producto / Cambiar licencia

Haga clic para abrir la ventana de activación del producto. Seleccione uno de los métodos disponibles para activar ESET Server Security.

Acerca de ESET Server Security

Muestra información sobre su copia de ESET Server Security.

Enviar una solicitud de soporte

Con el fin de prestar asistencia con la máxima rapidez y precisión posibles, ESET requiere información sobre la configuración de ESET Server Security, información detallada del sistema y de los procesos en ejecución (Archivo de registro de ESET SysInspector) y datos del registro. ESET utilizará estos datos solo para prestar asistencia técnica al cliente. Esta opción también puede configurarse en la ventana **Configuración avanzada** (**F5**) > **Herramientas** > **Diagnósticos** > **Soporte técnico**.

NOTA
Si opta por enviar los datos del sistema, es necesario cumplimentar y enviar el formulario web o, de lo contrario, no se creará su parte y se perderán los datos de su sistema.

Al enviar el formulario web a ESET también se enviarán los datos de configuración de su sistema. Seleccione **Enviar siempre esta información** para recordar esta acción para este proceso.

No enviar datos

Utilice esta opción si no desea enviar datos. Se le redirigirá a la página web del Soporte técnico de ESET.

Acerca de ESET Server Security

Esta ventana ofrece detalles de la versión instalada de ESET Server Security. La parte superior de la ventana contiene información sobre su sistema operativo y los recursos del sistema, así como el usuario que se encuentra conectado en ese momento y el nombre completo del ordenador.

Componentes instalados

Incluyen información sobre los módulos para ver una lista de los componentes instalados y sus detalles. Haga clic en **Copiar** para copiar la lista en el portapapeles. Esta información puede resultarle de utilidad durante la resolución de problemas o cuando se ponga en contacto con el servicio de asistencia técnica.

Glosario

Visite la página Glosario para obtener más información sobre los términos técnicos, las amenazas y la seguridad en Internet.

Acuerdo de licencia para el usuario final

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 (en adelante, "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 (en adelante, "ESET" o "Proveedor") y usted, una persona física o jurídica (en adelante, "Usted" o "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. Si no acepta todos los términos y condiciones de este Acuerdo, 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 (de aquí en adelante, la "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 todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (en adelante denominados "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 (de aquí en adelante, “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 solo 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) **Business Edition.** Debe obtener una versión Business Edition del Software para poder utilizarlo en servidores, relays abiertos y puertas de enlace de correo, así como en 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 OEM solo se puede utilizar en el ordenador con el que se le proporcionó. 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, el usuario debe eliminar, destruir o devolver (a sus expensas) el software y todas las copias de seguridad del mismo a ESET o al lugar 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 son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El Proveedor podrá publicar ocasionalmente 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 suministrar 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.

b) **Envío de amenazas e información al proveedor**. El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet (de aquí en adelante “amenazas”) y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el ordenador o la plataforma en la que el Software está instalado o información sobre las operaciones y las funciones del Software e información sobre dispositivos de la red local como tipo, proveedor, modelo o nombre del dispositivo (de aquí en adelante “información”). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las Amenazas junto con los metadatos asociados.

La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La función del sistema de reputación LiveGrid incluye la recopilación y el envío al proveedor de algoritmos hash unidireccionales relacionados con las amenazas. Esta función se activa en la sección de configuración estándar del software.

ii. La función del Sistema de Respuesta LiveGrid incluye la recopilación y el envío al Proveedor de las Amenazas con los metadatos y la Información asociados. Esta función la puede activar el Usuario final durante el proceso de instalación del Software.

El Proveedor solo podrá utilizar la Información y las Amenazas recibidas con fines de análisis e investigación de las Amenazas y mejora de la verificación de la autenticidad del Software y de la Licencia, y deberá tomar las medidas pertinentes para garantizar la seguridad de las Amenazas y la Información recibidas. Si se activa esta función del Software, el Proveedor podrá recopilar y procesar las Amenazas y la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. Estas funciones se pueden desactivar en cualquier momento.

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. Por la presente acepta recibir notificaciones y mensajes, lo que incluye, entre otros elementos, información de marketing.

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. 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 PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE LAS PÉRDIDAS DE BENEFICIOS, INGRESOS, VENTAS, DATOS O COSTES SOPORTADOS PARA OBTENER PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, CONDUCTA INADECUADA INTENCIONADA, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO A LA UTILIZACIÓN O LA INCAPACIDAD DE UTILIZACIÓN DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR O SUS PROVEEDORES DE LICENCIAS HAYAN SIDO NOTIFICADOS DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. 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. 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 (en adelante, las "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 (en adelante, las "Leyes de control de las exportaciones") 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 (en adelante, las "Leyes sancionadoras").

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 el Software y la Documentación devueltos deben enviarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

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. En caso de discrepancia entre las versiones de este acuerdo en diferentes idiomas, prevalecerá la versión en inglés. Este acuerdo solo se puede modificar por escrito y con la firma de un representante autorizado del proveedor o una persona autorizada expresamente para este fin

mediante un poder notarial.

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.

EULA ID: BUS-STANDARD-20-01

Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, número de registro de la empresa 31333532, como controlador de datos («ESET» o «Nosotros»), quiere ser transparente en cuanto al procesamiento de datos personales y la privacidad de sus clientes. Para alcanzar este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes («Usuario final» o «Usted») sobre los siguientes temas:

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

Los servicios prestados por ESET implementados en el producto se prestan de acuerdo con los términos del Acuerdo de licencia para el usuario final ("EULA"), pero algunos pueden requerir atención específica. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos diferentes servicios descritos en el EULA y en la documentación de producto, como el servicio de actualización, ESET LiveGrid®, protección contra mal uso de datos, soporte, etc. Para que todo funcione, debemos recopilar la siguiente información:

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Algoritmos hash unidireccionales relativos a infiltraciones que forman parte del sistema de reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones contra malware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.
- Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe
  - infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
  - información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;
  - información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y

marcos de Ethernet;

oarchivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

- 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.

Confidencialidad de los datos

ESET es una empresa que opera en todo el mundo a través de filiales o socios que forman parte de su red de distribución, servicio y asistencia. La información procesada por ESET puede transferirse a y de filiales o socios para cumplir el CLUF en aspectos como la prestación de servicios, la asistencia o la facturación. Según su ubicación y el servicio que decida utilizar, podemos vernos obligados a transferir sus datos a un país para el que no exista una decisión de adecuación de la Comisión Europea. Incluso en este caso, todas las transferencias de información cumplen la legislación sobre protección de datos y solo se realizan si es necesario. Deben implementarse sin excepción las cláusulas contractuales tipo, las reglas corporativas vinculantes u otra medida de seguridad adecuada.

Hacemos todo lo posible para evitar que los datos se almacenen más tiempo del necesario durante la prestación de servicios de acuerdo con el EULA. Nuestro período de retención puede ser mayor que el período de validez de su licencia para que tenga tiempo de renovarla de forma sencilla y cómoda. Pueden continuar tratándose estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar en todo momento la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y los servicios de tratamiento. Sin embargo, en caso de filtración de información que ponga en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora y a los interesados. Como titular de los datos, tiene derecho a presentar una reclamación ante una autoridad supervisora.

Derechos del titular de los datos.

ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. Sin perjuicio de las condiciones establecidas por las leyes de protección de datos aplicables, en su calidad de interesado, tiene los siguientes derechos:

- derecho a solicitar a ESET acceso a sus datos personales;
- derecho de rectificación de sus datos personales en caso de que sean incorrectos (también tiene derecho a completarlos en caso de que estén incompletos);
- derecho a solicitar la eliminación de sus datos personales;

- derecho a solicitar la restricción del procesamiento de sus datos personales;
- derecho a oponerse al procesamiento;
- derecho a presentar una reclamación y
- derecho a la portabilidad de datos.

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk