

ESET Server Security for Linux

Manual de usuario

[Haga clic aquí para ver la versión de la Ayuda de este documento](#)



Copyright ©2023 de ESET, spol. s r.o.

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

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

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

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

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

REV. 19/03/2023

1	Introducción	1
1.1	Principales funciones del sistema	1
2	Requisitos del sistema	1
2.1	Arranque seguro	3
3	Instalación	5
3.1	Reinstalar	7
3.2	Desinstalar	7
3.3	Implementación en bloque	7
4	Actualización	12
4.1	Mirror de actualización	14
4.2	Actualización automático de componentes de los programas	15
5	Activación de ESET Server Security for Linux	16
5.1	Dónde está mi licencia	17
5.2	Comprobar el estado de activación	18
6	Si se utiliza ESET Server Security for Linux	18
6.1	Panel	20
6.2	Escaneos	23
6.2	Ejecución de un análisis a petición desde una ventana de terminal	24
6.2	Exclusiones	26
6.2	Criterios de exclusiones de detección	27
6.3	Detecciones	28
6.3	Cuarentena	28
6.4	Archivos enviados	31
6.4	Enviar muestra para el análisis	31
6.5	Sucesos	32
7	Configuración	33
7.1	Motor de detección	34
7.1	Caché local compartida	34
7.1	Exclusiones	35
7.1	Exclusiones de procesos	36
7.1	Exclusiones de detección	37
7.1	Agregar o editar una exclusión de detección	39
7.1	Protección del sistema de archivos en tiempo real	40
7.1	Parámetros de ThreatSense	42
7.1	Parámetros adicionales de ThreatSense	44
7.1	Protección en la nube	45
7.1	Análisis de malware	47
7.1	Análisis remoto (análisis ICAP)	48
7.1	Niveles de desinfección	48
7.2	Actualización	49
7.3	Herramientas	50
7.3	Servidor proxy	50
7.3	Interfaz web	50
7.3	Dirección y puerto de recepción de conexiones	51
7.3	Archivos de registro	51
7.3	Planificador de tareas	53
7.4	Interfaz de usuario	53
7.4	Estados	54
8	Administración remota	54
9	Seguridad de contenedor	55

10 Ejemplos de casos de uso	55
10.1 Integración del servidor de ICAP con EMC Isilon	55
10.2 Recuperación de la información de módulos	57
10.3 Programación de análisis	57
11 Estructura de archivos y carpetas	58
12 Resolución de problemas	61
12.1 Recopilación de registros	61
12.2 Contraseña olvidada	63
12.3 Actualización fallida	63
12.4 La actualización falla debido a políticas de SELinux personalizadas	63
12.5 Uso del marcador noexec	64
12.6 La protección en tiempo real no se puede iniciar	65
12.7 Desactivar protección en tiempo real al arrancar	67
13 Glosario	67
14 Acuerdo de licencia para el usuario final	68
15 Política de privacidad	74

Introducción

El moderno motor de análisis de ESET ofrece una velocidad de análisis y unas tasas de detección insuperables combinadas con un uso de recursos muy bajo que convierten a ESET Server Security for Linux (ESSL, anteriormente ESET File Security for Linux (EFS)) en la opción ideal para cualquier servidor que funciona sobre Linux.

La funcionalidad principal la cubren el Análisis a petición y el Análisis en el acceso ([Protección del sistema de archivos en tiempo real](#)).

El Análisis a petición puede iniciarlo un usuario con privilegios (normalmente un administrador del sistema) mediante la interfaz de línea de comandos, o puede iniciarse mediante la herramienta de planificación automática del sistema operativo (p. ej., cron). El término A petición indica que los objetos del sistema de archivo se analizan a petición del usuario o el sistema.

El análisis en el acceso se invoca siempre que un usuario o un sistema operativo intentan acceder a objetos del sistema de archivos. Así, cualquier intento de acceder a objetos del sistema de archivos desencadena un análisis.

Principales funciones del sistema

- Actualizador automático del producto.
- Interfaz web rediseñada para facilitar la administración y mostrar una visión general de la seguridad del sistema.
- Análisis en el acceso mediante el módulo ligero de ESET, integrado en el kernel.
- Completos registros de análisis.
- Página de configuración rediseñada fácil de usar con una barra de búsqueda.
- Compatibilidad con SELinux.
- Cuarentena
- Se puede administrar mediante [ESET PROTECT](#).
- [Protección en la nube](#)
- [Seguridad de contenedor](#)

Requisitos del sistema

Requisitos de hardware

Los requisitos de hardware dependen del rol del servidor. Para la instalación son necesarios los siguientes requisitos mínimos de hardware:

- Processor Intel/AMD x64

- 700 MB de espacio libres en el disco duro
- 256 MB de RAM libres
- Glibc 2.17 o posterior
- Kernel del sistema operativo Linux versiones 3.10.0 y posteriores
- Configuración regional de codificación UTF-8

Sistemas operativos compatibles

ESET Server Security for Linux (ESSL) se ha probado y se ha comprobado que es compatible con las versiones secundarias más recientes de los sistemas operativos indicados. Actualice el sistema operativo antes de instalar ESSL.

Sistema operativo de 64 bits	Opción Arranque seguro compatible	Compatibilidad con SELinux	Nota
RedHat Enterprise Linux (RHEL) 7	✓	✓	La instalación de la política del módulo ESSL SELinux requiere un paquete selinux-policy-devel instalado. Para iniciar el sistema operativo sin el módulo ESSL SELinux, utilice el parámetro del kernel <code>eset_selinux=0</code> durante el arranque del sistema operativo.
RedHat Enterprise Linux (RHEL) 8	✓	✓	
CentOS 7	✓	✓	
CentOS 8	✓	✓	
Ubuntu Server 16.04 LTS	✓		
Ubuntu Server 18.04 LTS	✓		
Ubuntu Server 20.04 LTS	✓		
Debian 9			
Debian 10	✓		
Debian 11	✓		
SUSE Linux Enterprise Server (SLES) 12	✓		
SUSE Linux Enterprise Server (SLES) 15	✓		
Oracle Linux 8	✓ (solo kernel de stock)		Si se utiliza Unbreakable Enterprise Kernel , el paquete kernel-uek-devel se debe instalar manualmente. En este caso, la opción Arranque seguro no es compatible.
Amazon Linux 2			

ESSL debe funcionar en las distribuciones de Linux de código abierto más recientes y frecuentemente utilizadas si se cumplen los requisitos de hardware indicados antes y no faltan dependencias de software en la distribución de Linux utilizada.

i Las distribuciones de Linux con el kernel [ELREPO](#) y el kernel AWS no son compatibles.
El RHEL con el "Perfil de protección para sistemas operativos de uso general (OSPP)" no es compatible.

[Administración remota mediante ESET PROTECT.](#)

Navegadores compatibles

La interfaz web de ESSL funciona mejor en las versiones de escritorio más recientes de los siguientes navegadores:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

Arranque seguro

Para utilizar la [protección del sistema de archivos en tiempo real](#) en un equipo con la opción [Arranque seguro](#) activada, el módulo del kernel ESET Server Security for Linux (ESSL) debe estar firmado con una clave privada. La clave pública correspondiente debe importarse en UEFI. ESSL versión 8 incluye un script de firma integrado, que funciona en modo [interactivo](#) o [no interactivo](#).

Utilice la utilidad `mokutil` para verificar que la opción Arranque seguro esté activada en el equipo. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
mokutil --sb-state
```

Modo interactivo

Si no dispone de una clave pública y de una clave privada para firmar el módulo del kernel, el modo interactivo puede generar nuevas claves y firmar el módulo del kernel. También ayuda a inscribir las claves generadas en UEFI.

1. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
/opt/eset/efs/lib/install_scripts/sign_modules.sh
```

2. Cuando el script le solicite las claves, escriba **n** y, a continuación, pulse **Entrar**.
3. Cuando se le pida que genere nuevas claves, escriba **y** y, a continuación, pulse **Entrar**. El script firma el módulo del kernel con la clave privada generada.
4. Para inscribir la clave pública generada en UEFI semiautomáticamente, escriba **y** y, a continuación, pulse

Entrar. Para completar la inscripción manualmente, escriba **n**, pulse **Entrar** y siga las instrucciones que aparecen en la pantalla.

5. Cuando se le indique, introduzca una contraseña de su elección. Recuerde la contraseña; la necesitará al completar la inscripción (aprobación de la nueva clave de propietario del equipo [MOK]) en UEFI.

6. Para guardar las claves generadas en el disco duro para usarlas más adelante, escriba **y**, introduzca la ruta de acceso a un directorio y pulse **Entrar**.

7. Para reiniciar y acceder a UEFI, escriba **y** cuando se le indique y pulse **Entrar**.

8. Pulse cualquier tecla en un plazo de 10 segundos cuando se le pida para acceder a UEFI.

9. Seleccione **Inscribir MOK** y pulse **Entrar**.

10. Seleccione **Continuar** y pulse **Entrar**.

11. Seleccione **Sí** y pulse **Entrar**.

12. Para completar la inscripción y reiniciar el equipo, escriba la contraseña del paso 5 y pulse **Entrar**.

Modo no interactivo

Utilice este modo si tiene una clave privada y una clave pública disponibles en el equipo de destino.

Sintaxis: `/opt/eset/efs/lib/install_scripts/sign_modules.sh [OPCIONES]`

Opciones: forma abreviada	Opciones: forma completa	Descripción
-d	--public-key	Establecer la ruta de acceso a una clave pública con formato DER que se utilizará para firmar
-p	--private-key	Establecer la ruta de acceso a la clave privada que se utilizará para firmar
-k	--kernel	Establecer el nombre del kernel cuyos módulos deben firmarse. Si no se especifica, el kernel actual se selecciona de forma predeterminada
-a	--kernel-all	Firmar (y crear) módulos del kernel en todos los kernels existentes que contengan encabezados
-h	--help	Mostrar ayuda

1. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
/opt/eset/efs/lib/install_scripts/sign_modules.sh -p <path_to_private_key> -d <path_to_public_key>
```

Sustituya `<path_to_private_key>` y `<path_to_public_key>` por la ruta de acceso que lleva a una clave privada y a una clave pública, respectivamente.

2. Si la clave pública proporcionada aún no está inscrita en UEFI, ejecute el siguiente comando como usuario con privilegios:

```
mokutil --import <path_to_public_key>
```

<path_to_public_key> represents the provided public key.

3. Reinicie el equipo, acceda a UEFI, seleccione **Inscribir MOK > Continuar > Sí**.

Administración de varios dispositivos

Suponga que administra varios equipos que utilizan el mismo kernel Linux y tienen la misma clave pública inscrita en UEFI. En ese caso, puede firmar el módulo del kernel de ESSL en uno de esos equipos que contienen la clave privada y, a continuación, transferir el módulo del kernel firmado a los demás equipos. Cuando la firma se haya completado:

1. Copie el módulo del kernel firmado en `/lib/modules/<kernel-version>/eset/eea/eset_rtp` y péguelo en la misma ruta de acceso en los equipos de destino.
2. Llame a `depmod <kernel-version>` en los equipos de destino.
3. Reinicie ESET Server Security for Linux en el equipo de destino para actualizar la tabla de módulos. Ejecute el siguiente comando como usuario con privilegios:

```
systemctl restart efs
```

En todos los casos, sustituya `<kernel-version>` por la versión del kernel correspondiente.

Instalación

ESET Server Security for Linux (ESSL) [se distribuye como un archivo binario \(.bin\)](#).

Actualizar su sistema operativo

-  Antes de instalar ESET Server Security for Linux, asegúrese de que tiene instaladas las actualizaciones más recientes del sistema operativo.

Quitar

-  Si tiene ESET File Security for Linux 4.x instalado, quítelo primero. ESET Server Security for Linux x no es compatible con ESET File Security for Linux versión 4.x.
- Si ha utilizado ESET Remote Administrator para administrar ESET File Security for Linux versión 4, [actualice a ESET Security Management Center](#) y, a continuación, a [ESET PROTECT](#) para administrar la ESSL de forma remota.

Instalación desde ventana de terminal

Para instalar o actualizar su producto, ejecute el script de distribución de ESET con privilegios de usuario root para la distribución de SO correspondiente:

- `./efs.x86_64.bin`
- `sh ./efs.x86_64.bin`

 [Consulte los argumentos disponibles para la línea de comandos](#)

Para mostrar los parámetros (argumentos) disponibles del archivo binario de ESET Server Security for Linux, ejecute el siguiente comando desde una ventana de terminal:

```
bash ./efs.x86_64.bin -h
```

Parámetros disponibles

Forma abreviada	Forma completa	Descripción
-h	--help	Mostrar argumentos de la línea de comandos
-n	--no-install	No instalar tras desempaquetar
-y	--accept-license	No mostrar la licencia, la licencia se ha aceptado
-f	--force-install	Forzar la instalación mediante el sistema de gestión de paquetes sin preguntar
-g	--no-gui	No configurar o iniciar la interfaz gráfica de usuario tras la instalación
-u	--unpack-ertp-sources	Desempaquetar las fuentes de "Módulo del kernel de protección del sistema de archivos en tiempo real de ESET", no realizar instalación

Obtenga el paquete de instalación .deb o .rpm

Para obtener el paquete de instalación .deb o .rpm adecuado para su sistema operativo, ejecute el script de distribución de ESET con el argumento de la línea de comandos "-n":



```
sudo ./efs.x86_64.bin -n  
o  
sudo sh ./efs.x86_64.bin -n
```

Para ver las dependencias del paquete de instalación, ejecute uno de los siguientes comandos:

- `dpkg -I <deb package>`
- `rpm -qRp <rpm package>`

Siga las instrucciones de la pantalla. En cuanto acepte el Contrato de licencia del producto, la instalación finalizará y se mostrarán los detalles de inicio de sesión en la [Interfaz web](#).

Si existen problemas de dependencias, el instalador le informará de ello.

Instalación con ESET PROTECT

Si desea implementar ESET Server Security for Linux de forma remota en sus ordenadores, consulte el apartado [Instalación del software ESET PROTECT](#) de la ayuda en línea.

Para activar las actualizaciones periódicas de los módulos de detección, [active ESET Server Security for Linux](#).

Si es necesario, [active la interfaz web de forma remota](#).



Aplicaciones de terceros

Puede consultar un resumen de las aplicaciones de terceros que usa ESET Server Security for Linux en el archivo NOTICE_mode almacenado en `/opt/eset/efs/doc/modules_notice/`.

Reinstalar

Si la instalación se daña por cualquier motivo, [vuelva a ejecutar el instalador](#). Su configuración permanecerá intacta.

Desinstalar

Para desinstalar su producto ESET, utilice una ventana de terminal como superusuario para ejecutar el comando de supresión de paquetes correspondiente a su distribución Linux.

Distribuciones basadas en Ubuntu/Debian:

- `apt-get remove efs`
- `dpkg --purge efs`

Distribuciones basadas en Red Hat:

- `yum remove efs`
- `rpm -e efs`

Implementación en bloque

En este tema se presenta una descripción general de alto nivel de la implementación en bloque de ESET Server Security for Linux mediante [Puppet](#), [Chef](#) y [Ansible](#). Los bloques de código mostrados a continuación contienen únicamente ejemplos básicos de cómo pueden instalarse los paquetes. Pueden ser distintos según la distribución de Linux.

Selección del paquete

Antes de iniciar la implementación en bloque de ESET Server Security for Linux, tiene que decidir qué paquete desea usar. ESET Server Security for Linux se distribuye en forma de paquete `.bin`. Sin embargo, puede [obtener el paquete deb/rpm](#) mediante la ejecución del script de distribución de ESET con el argumento de línea de comandos `"-n"`.

Puppet

Condiciones previas

- Paquete `bin` o `deb/rpm` disponible en `puppet-master`
- `puppet-agent` conectado a `puppet-master`

Paquete `bin`

Pasos de implementación:

- Copie el paquete de instalación bin en los equipos que desee.
- Ejecute el paquete de instalación bin.

Ejemplo de manifiesto de Puppet

```
node default {  
  file {"/tmp/efs-8.0.1081.0.x86_64.bin":  
    mode => "0700",  
    owner => "root",  
    group => "root",  
    source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.bin"  
  }  
  exec {"Execute bin package installation":  
    command => '/tmp/efs-8.0.1081.0.x86_64.bin -y -f'  
  }  
}
```

Paquete deb/rpm

Pasos de implementación:

- Copie en las máquinas que desee el paquete de instalación deb/rpm según la familia de distribución.
- Ejecute el paquete de instalación deb/rpm.



Dependencias

Las dependencias se deben resolver antes de iniciar la instalación.

Ejemplo de manifiesto de Puppet

```
node default {
  if $osfamily == 'Debian' {
    file {"/tmp/efs-8.0.1081.0.x86_64.deb":
      mode => "0700",
      owner => "root",
      group => "root",
      source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.deb"
    }
    package {"efs":
      ensure => "installed",
      provider => 'dpkg',
      source => "/tmp/efs-8.0.1081.0.x86_64.deb"
    }
  }
  ✓ if $osfamily == 'RedHat' {
    file {"/tmp/efs-8.0.1081.0.x86_64.rpm":
      mode => "0700",
      owner => "root",
      group => "root",
      source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.rpm"
    }
    package {"efs":
      ensure => "installed",
      provider => 'rpm',
      source => "/tmp/efs-8.0.1081.0.x86_64.rpm"
    }
  }
}
```

Chef

Condiciones previas

- Paquete bin o deb/rpm disponible en el servidor de Chef
- Cliente de Chef conectado al servidor de Chef

Paquete bin

Pasos de implementación:

- Copie el paquete de instalación bin en los equipos que desee.
- Ejecute el paquete de instalación bin.

Ejemplo de receta de Chef

```
cookbook_file '/tmp/efs-8.0.1084.0.x86_64.bin' do
  source 'efs-7.0.1084.0.x86_64.bin'
  owner 'root'
  group 'root'
  mode '0700'
  action :create
end

execute 'package_install' do
  command '/tmp/efs-8.0.1084.0.x86_64.bin -y -f'
end
```

Paquete deb/rpm

Pasos de implementación:

- Copie en las máquinas que desee el paquete de instalación deb/rpm según la familia de distribución.
- Ejecute el paquete de instalación deb/rpm.



Dependencias

Las dependencias se deben resolver antes de iniciar la instalación.

Ejemplo de receta de Chef

```
cookbook_file '/tmp/efs-8.0.1084.0.x86_64.deb' do
  source 'efs-8.0.1084.0.x86_64.deb'
  owner 'root'
  group 'root'
  mode '0700'
  action :create
  only_if { node['platform_family'] == 'debian' }
end

cookbook_file '/tmp/efs-8.0.1084.0.x86_64.rpm' do
  source 'efs-8.0.1084.0.x86_64.rpm'
  owner 'root'
  group 'root'
  mode '0700'
  action :create
  only_if { node['platform_family'] == 'rhel' }
end

dpkg_package 'efsu' do
  source '/tmp/efs-8.0.1084.0.x86_64.deb'
  action :install
  only_if { node['platform_family'] == 'debian' }
end

rpm_package 'efsu' do
  source '/tmp/efs-8.0.1084.0.x86_64.rpm'
  action :install
  only_if { node['platform_family'] == 'rhel' }
end
```

Ansible

Condiciones previas

- Paquete bin o deb/rpm disponible en el servidor de Ansible
- Acceso mediante ssh a los equipos de destino

Paquete bin

Pasos de implementación:

- Copie el paquete de instalación bin en los equipos que desee.
- Ejecute el paquete de instalación bin.

Ejemplo de tarea de Playbook

```
.....  
- name: "INSTALL: Copy configuration json files"  
  copy:  
    src: efs-8.0.1084.0.x86_64.bin  
    dest: /home/ansible/  
  
- name : "Install product bin package"  
  shell: bash ./efs-8.0.1084.0.x86_64.bin -y -f -g  
.....
```

Paquete deb/rpm

Pasos de implementación:

- Copie en las máquinas que desee el paquete de instalación deb/rpm según la familia de distribución.
- Ejecute el paquete de instalación deb/rpm.

Ejemplo de tarea de Playbook

```
....
- name: "Copy deb package to VM"
  copy:
    src: ./efs-8.0.1085.0.x86_64.deb
    dest: /home/ansible/efs-8.0.1085.0.x86_64.deb
    owner: ansible
    mode: a+r
  when:
    - ansible_os_family == "Debian"

- name: "Copy rpm package to VM"
  copy:
    src: ./efs-8.0.1085.0.x86_64.rpm
    dest: /home/ansible/efs-8.0.1085.0.x86_64.rpm
    owner: ansible
    mode: a+r
  when:
    - ansible_os_family == "RedHat"

- name: "Install deb package"
  apt:
    deb: /home/ansible/efs-8.0.1085.0.x86_64.deb
    state: present
  when:
    - ansible_os_family == "Debian"

- name: "Install rpm package"
  yum:
    name: /home/ansible/efs-8.0.1085.0.x86_64.rpm
    state: present
  when:
    - ansible_os_family == "RedHat"
....
```

Actualización

Actualizar módulos

Los módulos del producto, incluidos los módulos de detección, se actualizan automáticamente.

Para actualizar manualmente los módulos de detección, haga clic en **Actualización de los módulos > Comprobar y actualizar**.

Si una actualización de ESET Server Security for Linux no resulta estable, revierta la actualización del módulo al estado anterior. Haga clic en **Panel de control > Actualización de los módulos > Reversión de módulos**, seleccione el periodo que desee y haga clic en **Revertir**.

Si desea actualizar todos los módulos del producto desde una ventana de terminal, ejecute el siguiente comando:

```
/opt/eset/efs/bin/upd -u
```

Actualización y reversión desde una ventana de terminal

Opciones: forma abreviada	Opciones: forma completa	Descripción
-u	--update	Actualizar módulos
-c	--cancel	Cancelar la descarga de módulos
-e	--resume	Desbloquear actualizaciones
-r	--rollback=VALUE	Volver a la instantánea más antigua del módulo de análisis y bloquear todas las actualizaciones durante las horas indicadas en VALOR
-l	--list-modules	Mostrar la lista de módulos de productos
	--check-app-update	Comprobar la disponibilidad de una versión nueva del producto en el repositorio
	--download-app-update	Descargar la versión nueva del producto si está disponible
	--perform-app-update	Descargar e instalar la versión nueva del producto si está disponible
	--accept-license	Aceptar los cambios en la licencia



Limitación de upd

La utilidad upd no se puede usar para realizar cambios en la configuración del producto.

Para detener las actualizaciones durante 48 horas y volver a la instantánea más antigua del módulo de análisis, ejecute el siguiente comando con un usuario con privilegios:

```
sudo /opt/eset/efs/bin/upd --rollback=48
```

Para reanudar las actualizaciones automáticas del módulo de análisis, ejecute el siguiente comando con un usuario con privilegios:

```
sudo /opt/eset/efs/bin/upd --resume
```

Para actualizar desde un servidor Mirror disponible en la dirección IP "192.168.1.2" y el puerto "2221", ejecute el siguiente comando con un usuario con privilegios:

```
sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221
```

Actualización de ESET Server Security for Linux a una versión posterior

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

Sin actualización directa desde ESET File Security for Linux versión 4



No puede actualizar de ESET File Security for Linux versión 4 a la ESET Server Security for Linux versión 8 y posteriores. Es necesaria una nueva instalación. La configuración de la versión 4 no se puede importar a la versión 8 y posteriores.

Determinar la versión del producto instalada

Hay dos métodos para determinar la versión del producto de ESET Server Security for Linux:

- En la [interfaz web](#), haga clic en **Ayuda > Acerca de**.
- Ejecute `/opt/eset/efs/sbin/setgui -v` en una ventana de terminal.

Actualización local de ESET Server Security for Linux

- Ejecute un paquete de instalación del sistema operativo correspondiente, como se describe en el apartado [Instalación](#).
- En la interfaz web, haga clic en **Panel > Actualización de componentes de los programas > Buscar actualizaciones**.
- Use la utilidad `upd` con el parámetro `--perform-app-update`
- [Configuración de las actualizaciones automáticas](#).

Actualización remota de ESET Server Security for Linux

Si utiliza ESET PROTECT para administrar ESET Server Security for Linux, puede iniciar una actualización de las siguientes formas:

- [Software install](#) task.
- En la interfaz web, diríjase a **Panel > Aplicaciones de ESET > clic con el botón derecho en ESET Server Security for Linux > Actualizar productos de ESET instalados**
- [Configuración de las actualizaciones automáticas](#).

Mirror de actualización

Son varios los productos de seguridad de ESET ([ESET PROTECT](#), [ESET Endpoint Antivirus](#), etc.) que le permiten crear copias de los archivos de actualización que puede utilizar para actualizar otras estaciones de trabajo de la red. El uso de un "Mirror" (una copia de los archivos de actualización en el entorno de la LAN) resulta práctico, dado que evita tener que descargar los archivos de actualización del servidor de actualizaciones del proveedor varias veces en cada estación de trabajo. Las actualizaciones se descargan de manera centralizada en el servidor Mirror 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.

Configure ESET Server Security for Linux para usar un mirror de actualización

1. En la [Interfaz web](#), diríjase a **Configuración > Actualización > Servidor principal**.
2. En el apartado **Básico**, desactive el interruptor situado junto a **Elegir automáticamente**.
3. Escriba en el campo **Servidor de actualizaciones** la dirección URL del servidor Mirror en uno de los siguientes formatos:

a. `http://<IP>:<port>`

b. `http://<hostname>:<port>`

4. Escriba el nombre de usuario y la contraseña correspondientes.

5. Haga clic en **Guardar**.

Si hay más servidores Mirror disponibles en la red, repita los pasos anteriores para configurar los servidores de actualizaciones secundarios.

Actualización desde un directorio local

i Para actualizar desde un directorio local, por ejemplo, `/updates/eset` escriba en el campo **Servidor de actualización**:
`file:///updates/eset/`

Actualización automático de componentes de los programas

Activar las actualizaciones automáticas del componente del producto, incluidas las actualizaciones a versiones posteriores del producto.

1. En la Interfaz web, haga clic en **Configuración > Actualizar**.
2. En la sección **Actualización de programa**, seleccione **Actualizar automáticamente** en el cuadro de lista **Modo de actualización**.
3. Si prefiere usar un servidor de actualizaciones personalizado para las actualizaciones del componente del producto:
 - a. Defina la dirección del servidor en el campo **Servidor personalizado**.
 - b. Escriba el **Nombre de usuario** y la **Contraseña** en los campos correspondientes.
4. Haga clic en **Guardar**.

Si administra ESET Server Security for Linux mediante ESET PROTECT, configure las actualizaciones automáticas mencionadas anteriormente mediante [Políticas](#).

Para modificar la configuración de ESET Server Security for Linux:

1. En ESET PROTECT, haga clic en **Políticas > Nueva política** y escriba un nombre para la política.
2. Haga clic en **Configuración** y seleccione **ESET Server/File Security for Linux (V7+)** en el menú desplegable.
3. Configure los ajustes deseados.
4. Haga clic en **Continuar > Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.
5. Haga clic en **Finalizar**.

Se recomienda reiniciar

i Si un ordenador administrado de forma remota tiene las actualizaciones automáticas activadas y el nuevo paquete se descarga automáticamente, el estado de la protección en ESET PROTECT será **Se recomienda reiniciar**.

Modo de actualización

Actualizar automáticamente: los paquetes nuevos se descargan e instalan automáticamente tras el siguiente reinicio del SO. Si se han realizado modificaciones del Acuerdo de licencia para el usuario final, el usuario debe aceptar el Acuerdo de licencia para el usuario final para poder descargar el paquete nuevo.

No actualizar nunca: los paquetes nuevos no se descargan, pero el producto indica en el **Panel** que hay nuevos paquetes disponibles.

Activación de ESET Server Security for Linux

Active su ESET Server Security for Linux (ESSL) con una [licencia](#) adquirida a su distribuidor de ESET.

Activación con la Interfaz web

1. Inicio de sesión en la Interfaz web.
2. Haga clic en **Panel** > **Licencia**.
3. Seleccione el método de activación que desee:
 - [Activar con clave de licencia](#): para usuarios que han comprado una clave de licencia de ESET Server Security for Linux.
 - [ESET Business Account](#): para usuarios de [ESET Business Account \(EBA\)](#) registrados que tienen una licencia de ESET Server Security for Linux importada en EBA. Son necesarios su nombre de usuario y su contraseña de EBA (o de ESET MSP Administrator [EMA]).
 - [Licencia sin conexión](#): utilice esta opción si el ESET Server Security for Linux no se puede conectar a Internet y ESSL se utilizará en un entorno sin conexión.
 - [ESET PROTECT](#)

Si la licencia caduca, puede cambiarla a otra distinta en la misma ubicación.

Uso de las credenciales de inicio de sesión de EBA o EMA para activar ESSL

1. Inicio de sesión en la Interfaz web.
2. Haga clic en **Panel** > **Licencia** y seleccione **ESET Business Account**.
3. Introduzca sus credenciales de inicio de sesión en EBA o EMA.
4. Si solo hay una licencia de ESSL (o ESET File Security for Linux) en su cuenta de EBA o EMA y no se crea ningún sitio, la activación se completará al instante. De lo contrario, tendrá que seleccionar una licencia o un sitio concretos ([grupo de licencias](#)) para activar ESSL.
5. Haga clic en **Activar**.

Activación desde una ventana de terminal

Use la utilidad `/opt/eset/efs/sbin/lic` con un usuario con privilegios para activar ESET Server Security for Linux desde una ventana de terminal.

Syntax: `/opt/eset/efs/sbin/lic[OPCIONES]`

EJEMPLOS

Los comandos indicados a continuación se deben ejecutar con un usuario con privilegios.

Activación mediante clave de licencia

```
/opt/eset/efs/sbin/lic -k XXXX-XXXX-XXXX-XXXX-XXXX
```

o

```
/opt/eset/efs/sbin/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
```

donde XXXX-XXXX-XXXX-XXXX-XXXX representa su clave de licencia de ESET Server Security for Linux.

Activación con una cuenta de EBA o EMA

1. Ejecute

```
/opt/eset/efs/sbin/lic -u your@username
```

donde `your@username` representa el nombre de usuario de su cuenta de EBA o EMA.



2. Escriba su contraseña y pulse **Entrar**.

3. Si solo hay una licencia de ESSL en su cuenta de EBA o EMA y no se crea ningún sitio, la activación se completará al instante. De lo contrario, se mostrará una lista de licencias y sitios de ESSL disponibles ([grupo de licencias](#)).

4. Ejecute uno de los siguientes comandos:

```
/opt/eset/efs/sbin/lic -u your@username -p XXX-XXX-XXX
```

donde XXX-XXX-XXX representa un ID de licencia público entre corchetes junto a cada licencia de la lista mostrada anteriormente

```
/opt/eset/efs/sbin/lic -u your@username -i site_ID
```

donde `site_ID` representa una cadena alfanumérica mostrada entre corchetes junto a cada sitio de la lista mostrada anteriormente

5. Introduzca su contraseña y pulse **Entrar**.

Activación de mediante ESET PROTECT

Inicie sesión en la Interfaz web de ESET PROTECT, diríjase a **Tareas del cliente > Activación del producto** y siga las [instrucciones de activación de productos](#).

Tras completar la activación, acceda a la [Interfaz web](#) para realizar el [análisis](#) inicial del sistema o [configurar](#) ESET Server Security for Linux.

Dónde está mi licencia

Si ha comprado una licencia, debe haber recibido dos mensajes de correo electrónico de ESET. El primero contiene información sobre el portal ESET Business Account. El segundo contiene la información de su clave de licencia (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) o nombre de usuario (EAV-xxxxxxxxxx) y contraseña cuando proceda, el ID público de la licencia (xxx-xxx-xxx), el nombre del producto (o la lista de productos) y la cantidad.

Tengo un nombre de usuario y una contraseña

Si tiene un nombre de usuario y una contraseña, conviértalos en una clave de licencia en la página de conversión de licencias de ESET Business Account:

Comprobar el estado de activación

Para ver el estado de activación y la validez de la licencia, utilice la utilidad `lic`. Ejecute los siguientes comandos como usuario con privilegios:

Syntax: `/opt/eset/efs/sbin/lic[OPCIONES]`

Los comandos indicados a continuación debe ejecutarlos un usuario con privilegios:

```
/opt/eset/efs/sbin/lic -s
```

o

```
/opt/eset/efs/sbin/lic --status
```

✓ Salida cuando el producto está activado:

```
Estado: activado
```

```
ID público: ABC-123-DEF
```

```
Validez de la licencia: 29-03-2020
```

Salida cuando el producto no está activado:

```
Estado: no activado
```

Si [ESET Dynamic Threat Defense](#) está activado para la instancia específica de ESET Server Security for Linux, la salida muestra los detalles de la licencia relacionada.

En la versión 8.1 o posterior, para mostrar el ID del puesto si lo solicita el servicio de atención al cliente de ESET, ejecute:

```
/opt/eset/efs/sbin/lic -s --with-details
```

Si se utiliza ESET Server Security for Linux

Acceder a la interfaz web

Si la instalación ha concluido, inicie sesión en la Interfaz web en la dirección URL que mostró el instalador junto con las credenciales de inicio de sesión.

La Interfaz web está disponible en los siguientes idiomas:

- Inglés
- Francés
- Español
- Español de Latinoamérica
- Alemán
- Japonés

- Polaco

certificado ssl

ESET Server Security for Linux Certificado de la Interfaz web

ESET Server Security for Linux Web Console usa un certificado autofirmado. Al acceder por primera vez a la Interfaz web, se mostrará un mensaje de problema con el certificado, a menos que agregue una [excepción de certificado](#).

- Para agregar una excepción de certificado a Mozilla Firefox:

1. Haga clic en **Configuración avanzada > Agregar excepción**.
2. Compruebe que la opción **Almacenar esta excepción de forma permanente** está marcada en la ventana **Agregar excepción de seguridad**.
3. Haga clic en **Confirmar excepción de seguridad**.

- Para agregar una excepción de certificado a Google Chrome:

1. Haga clic en **Configuración avanzada**.
2. Haga clic en **Ir a <web address of ESSL Web interface> (no seguro)**.
3. A partir de ahora, Google Chrome recuerda la excepción.

Si desea usar un certificado SSL para la interfaz web, genere un certificado e impórtelo en ESET Server Security for Linux.

1. Para generar un certificado SSL:

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout privatekey.pem -out certificate.pem
```

2. Para importar el certificado SSL en ESET Server Security for Linux:

```
sudo /opt/eset/efs/sbin/setgui -c certificate.pem -k privatekey.pem -e
```

Activar la interfaz web de forma remota

Si instala ESET Server Security for Linux de forma remota mediante ESET PROTECT, la Interfaz web no se activa. Si desea acceder a la Interfaz web desde un equipo concreto, ejecute el siguiente comando desde una ventana de terminal:

```
sudo /opt/eset/efs/sbin/setgui -gre
```

En la salida final se mostrarán la dirección URL de la Interfaz web y las credenciales de acceso.

Para que la Interfaz web esté disponible en una dirección IP y un puerto personalizados, por ejemplo 10.1.184.230:9999, ejecute el siguiente comando desde una ventana de terminal:

```
sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999
```

Para activar la interfaz web con ESET PROTECT, utilice la [tarea Ejecutar comando](#) para ejecutar el siguiente comando:

```
/opt/eset/efs/sbin/setgui -re --password=<password>
```

donde <password> representa la contraseña deseada definida por usted.

[Opciones disponibles para el comando setgui](#)

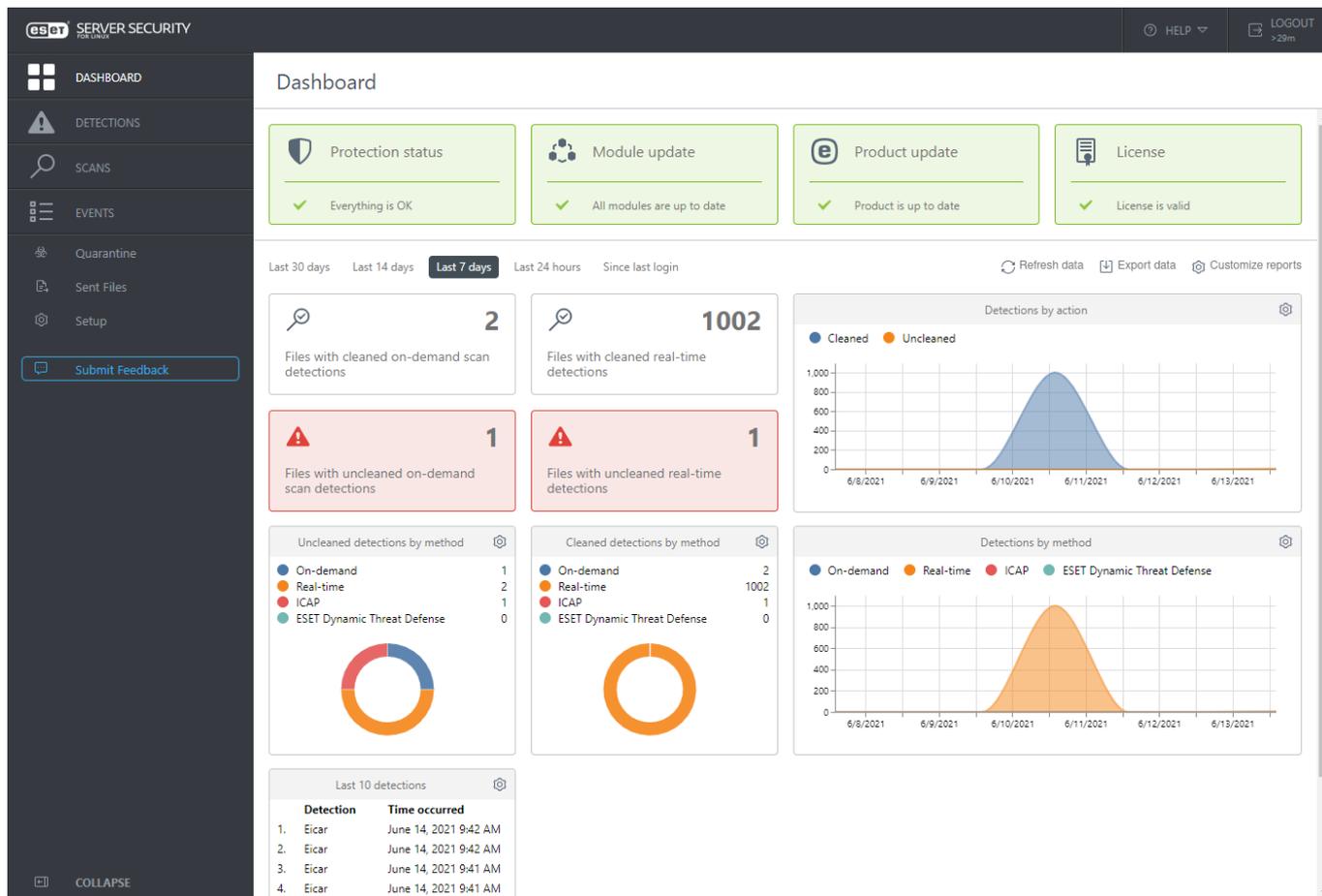
Opciones: forma abreviada	Opciones: forma completa	Descripción
-g	--gen-password	Generar una contraseña nueva para acceder a la Interfaz web
-p	--password=PASSWORD	Definir una contraseña nueva para acceder a la Interfaz web
-f	--passfile=FILE	Definir una contraseña nueva leída de un archivo para acceder a la Interfaz web
-r	--gen-cert	Generar una clave privada y un certificado nuevos
-a	--cert-password=PASSWORD	Establecer la contraseña del certificado
-l	--cert-passfile=FILE	Establecer la contraseña del certificado leída de un archivo
-i	--ip-address=IP:PORT	Dirección del servidor (IP y número de puerto)
-c	--cert=FILE	Importar certificados
-k	--key=FILE	Importar la clave privada
-d	--disable	Desactivar la Interfaz web
-e	--enable	Activar la Interfaz web

Activación del producto y análisis inicial

Si [activó](#) su instancia de ESET Server Security for Linux, actualice los módulos de detección (haga clic en **Panel de control** > **Actualización de los módulos** > **Comprobar y actualizar**) y ejecute un [análisis](#) inicial del sistema de archivos.

Panel

El **Panel de control** ofrece una descripción general del estado de protección, las [actualizaciones de los módulos](#), información sobre la licencia y las [opciones de activación del producto](#), además de mostrar un resumen de las notificaciones. A partir de la versión 8.1, también ofrece [estadísticas de análisis](#) sencillas.



Estado de la protección

Cuando todo está en funcionamiento y sin ningún tipo de problema, el estado de protección aparece en color verde. Si existen opciones para mejorar el estado de protección de su sistema o se detecta un estado de protección insuficiente, verá "Atención necesaria" en la ventana **Estado de la protección**. Para ver más información, haga clic en la ventana.

Silenciar o desactivar el silencio de las alertas de estado de protección

Las alertas de estado de protección que no estén en verde pueden silenciarse con la opción **Silenciar esta alerta**. El estado del módulo de protección cambiará a gris, y la ventana del módulo de protección se trasladará al final de la lista. Haga clic en **Desactivar el silencio de esta alerta** para activar la notificación de estado.

Si el [estado de protección se desactiva](#) mediante ESET PROTECT, ni **Desactivar el silencio de esta alerta** ni **Activar** estarán disponibles en el **Panel de control**.

Actualización de los módulos

Si todos los módulos están actualizados, la ventana **Actualizaciones del módulo** aparece de color verde. Si las actualizaciones de los módulos están suspendidas de manera temporal, la ventana cambia a color naranja. Si la actualización falla, el color de la ventana cambia a rojo. Para ver más información, haga clic en la ventana.

Para ejecutar una actualización manual de los módulos de detección, haga clic en **Actualización de los módulos > Comprobar y actualizar** y espere a que la actualización concluya.

Actualización de componentes de los programas

Si todos los componentes del producto están actualizados, la ventana **Actualización del producto** será de color verde. Haga clic en la ventana para ver más detalles de la versión actual y la última búsqueda de actualizaciones.

Si hay una nueva versión del producto disponible, la ventana será de azul claro. Para ver el registro de cambios o actualizar a la versión nueva, haga clic en **Actualización del producto** y, a continuación, haga clic en **Ver registro de cambios** o **Aceptar & actualizar ahora**.

Para comprobar la disponibilidad de actualizaciones nuevas manualmente, haga clic en **Actualización del producto > Buscar actualizaciones**.

Consulte más información sobre la configuración de las [actualizaciones automáticas del producto](#).

Licencia

Si la fecha de caducidad de la licencia está próxima, la ventana **Licencia** cambia a color naranja. Si la licencia ya ha caducado, la ventana cambia a color rojo. Haga clic en la ventana para ver las opciones de cambio de licencia disponibles.

Estadísticas de análisis

ESET Server Security for Linux versión 8.1 y posteriores proporcionan estadísticas de análisis sencillas a través de gráficos o tablas:

- **Detecciones por acción**
- **Detecciones por método**
- **Detecciones sin desinfectar por método**
- **Detecciones desinfectadas por método**
- **Últimas 10 detecciones**
- **Los 10 usuarios con más detecciones de acceso**
- **Últimos 10 análisis a petición con detecciones**

y en forma de ventanas dinámicas:

- **Archivos con detecciones del análisis a petición desinfectadas**
- **Archivos con detecciones en tiempo real desinfectadas**
- **Archivos con detecciones del análisis a petición sin desinfectar**
- **Archivos con detecciones en tiempo real sin desinfectar**

Haga clic en una ventana dinámica de estadísticas o un gráfico para ir a la pantalla [Análisis](#) o [Detecciones](#). Utilice preajustes de periodos para filtrar las estadísticas.

Si el número de detecciones sin desinfectar es superior a 0, el color de fondo de las estadísticas "sin desinfectar" cambia a color rojo.

Estadísticas que se mostrarán

1. Haga clic en  **Personalizar informes**.
2. Seleccione las acciones deseadas o anule la selección de las estadísticas no deseadas.
3. Haga clic en **Guardar**.

Para eliminar estadísticas individuales, haga clic en su botón de configuración  y seleccione **Quitar**.

La configuración de las estadísticas permanece intacta, a menos que elimine la memoria caché del navegador.

Descargar estadísticas de análisis

Para descargar todas las estadísticas de análisis del periodo seleccionado como un archivo comprimido .zip, haga clic en  **Exportar datos**. El archivo comprimido .zip contiene las estadísticas en los archivos .csv.

Para descargar estadísticas de análisis específicas, haga clic en su botón de configuración , seleccione **Descargar** y, a continuación, seleccione **CSV** o **PDF**.

Escaneos

Ejecute un nuevo análisis de todas las unidades locales de forma manual desde **Análisis > Nuevo análisis > Analizar todas las unidades locales**.

Seleccione **Análisis personalizado**, donde puede elegir el [perfil de análisis](#), y defina la ubicación que desee analizar. Si selecciona **Análisis con desinfección**, el [nivel de desinfección](#) del perfil de análisis seleccionado se aplicará a cada amenaza detectada. Para analizarlo todo, incluidas las [exclusiones](#) configuradas, seleccione **Exclusiones de análisis**.

Objetos del análisis personalizado

- Unidades locales
- Unidades de red
- Medios extraíbles
- Sectores de arranque: se analizará el sector de arranque de todas las unidades o soportes montados.
- Objeto personalizado: escriba la ruta de acceso que desee analizar y pulse la tecla **Tabulador** del teclado.

Todos los análisis ejecutados se registran en la pantalla **Análisis**, incluida la información sobre el número de amenazas detectadas y desinfectadas. Si la columna **Desinfectado** aparece en rojo, algunos archivos infectados no se han desinfectado o eliminado. Para ver más detalles de una entrada, haga clic en ella y, a continuación, haga

clic en **Mostrar detalles**.

En la pantalla **Detalle del análisis** se incluyen tres fichas:

- **Información general:** muestra la misma información que aparece en la pantalla **Análisis**, más el número de discos analizados.
- [Detecciones](#): muestra los detalles de la amenaza detectada y la acción emprendida contra ella.
- **Archivos no analizados:** muestra los detalles y el motivo de los archivos que no se pudieron analizar.

Perfiles de análisis

Es posible guardar los parámetros de análisis que desee ([Parámetros de ThreatSense](#)) para futuros análisis. Se recomienda crear un perfil distinto (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada análisis que use con frecuencia.

Para crear un perfil nuevo, haga clic en **Configuración > Motor de detección > Análisis de malware > Análisis a petición > Lista de perfiles**.

Análisis a petición desde una ventana de terminal

Para ejecutar un análisis a petición desde una ventana de terminal, use el comando [/opt/eset/efs/bin/odscan](#).

Ejecución de un análisis a petición desde una ventana de terminal

Sintaxis: `/opt/eset/efs/bin/odscan [OPCIONES..]`

Opciones: forma abreviada	Opciones: forma completa	Descripción
-l	--list	Mostrar análisis que se están ejecutando
	--list-profiles	Mostrar todos los perfiles de análisis disponibles
	--all	Muestra también los análisis ejecutados por otro usuario (requiere privilegios de usuario root)
-r	--resume=session_id	Reanudar un análisis puesto anteriormente en pausa identificado mediante session_id
-p	--pause=session_id	Poner en pausa un análisis identificado mediante session_id
-t	--stop=session_id	Detener un análisis identificado mediante session_id
-s	--scan	Iniciar análisis
	--profile=PROFILE	Análisis con el PERFIL seleccionado
	--profile-priority=PRIORITY	La tarea se ejecutará con la prioridad especificada. La prioridad puede ser normal, menor, más baja, inactividad.
	--readonly	Analizar sin desinfectar

Opciones: forma abreviada	Opciones: forma completa	Descripción
	--local	Analizar las unidades locales
	--network	Analizar las unidades de red
	--removable	Analizar los medios extraíbles
	--boot-local	Analizar los sectores de arranque de la unidad local
	--boot-removable	Analizar los sectores de arranque de los medios extraíbles
	--boot-main	Analizar el sector de arranque principal
	--exclude=FILE	Omitir el archivo o el directorio seleccionados
	--ignore-exclusions	Analizar también las rutas de acceso y extensiones excluidas

La utilidad `odscan` finaliza con un código de salida cuando concluye el análisis. Ejecute `echo $?` en la ventana de terminal cuando haya finalizado el análisis para mostrar el código de salida.

Códigos de salida

Código de salida	Significado
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

EJEMPLO

Ejecutar un análisis a petición del directorio `/root/` de forma recursiva con el perfil de análisis "@Análisis inteligente" como un proceso en segundo plano:

```
/opt/eset/efs/bin/odscan --scan --profile="@Smart scan" /root/ &
```

Ejecutar un análisis a petición con el perfil de análisis "@Análisis inteligente" en varios destinos de forma recursiva:

```
/opt/eset/efs/bin/odscan --scan --profile="@Smart scan" /root/ /tmp/ /home/
```

Enumerar todos los análisis en ejecución

```
/opt/eset/efs/bin/odscan -l
```

Pausar el análisis con el session-id "15" (cada análisis tiene su propio session-id, que se genera al comenzar)

```
/opt/eset/efs/bin/odscan -p 15
```

Detener el análisis con el session-id "15" (cada análisis tiene su propio session-id, que se genera al comenzar)

```
/opt/eset/efs/bin/odscan -t 15
```

Ejecutar un análisis a petición con el directorio */root/exc_dir* excluido y el archivo */root/eicar.com* excluido

```
/opt/eset/efs/bin/odscan --scan --profile="@In-depth scan" --  
exclude=/root/exc_dir/ --exclude=/root/eicar.com /
```

Analizar el sector de arranque de las unidades extraíbles (ejecute el siguiente comando con un usuario con privilegios)

```
sudo /opt/eset/efs/bin/odscan --scan --profile="@In-depth scan" --boot-removable
```

Exclusiones

Exclusiones de extensiones de archivo

Este tipo de exclusión se puede configurar para la protección del sistema de archivos en tiempo real, para análisis a petición y para el análisis remoto.

1. En la [Interfaz web](#), haga clic en **Configuración > Motor de detección**.
2. Haga clic en:
 - **Protección del sistema de archivos en tiempo real > Parámetros de ThreatSense** para modificar las exclusiones relacionadas con [Protección del sistema de archivos en tiempo real](#)
 - **Análisis de malware > Análisis a petición > Parámetros de ThreatSense** para modificar las exclusiones relacionadas con [Análisis a petición \(análisis personalizado\)](#)
 - **Análisis remoto > Parámetros de ThreatSense** para modificar exclusiones relacionadas con el [análisis remoto](#)
3. Junto a **Extensiones de archivo excluidas del análisis**, haga clic en **Editar**.
4. Haga clic en **Agregar** y escriba la extensión que desea excluir. Para definir varias extensiones a la vez, haga clic en **Escribir varios valores** y escriba las extensiones aplicables separadas por una línea nueva u otro separador que elija.
5. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
6. Haga clic en **Guardar** para guardar los cambios.

Exclusiones de rendimiento

Al excluir las rutas de acceso (carpetas) del análisis, el tiempo necesario para analizar el sistema de archivos para detectar malware puede reducirse significativamente.

1. En la [Interfaz web](#), haga clic en **Configuración > Motor de detección > Básico**.
2. Junto a **Exclusiones de rendimiento**, haga clic en **Editar**.
3. Haga clic en **Agregar** y defina la **ruta de acceso** que va a omitir el explorador. Si lo desea, agregue un comentario para su información.
4. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
5. Haga clic en **Guardar** para guardar los cambios.

Ruta de exclusión

*/root/**: el directorio "root", todos sus subdirectorios y el contenido que incluyen.

/root: solo el archivo "root".

/root/file.txt: solo file.txt en el directorio "root".

Comodines en el medio de una ruta de acceso

Le recomendamos encarecidamente no usar comodines en el medio de una ruta de acceso (por ejemplo */home/user/*/data/file.dat*) a menos que la infraestructura de su sistema lo requiera. Consulte el siguiente [artículo de la base de conocimiento](#) para obtener más información.

Cuando se utilizan [exclusiones de detección](#), no hay restricciones en lo que respecta al uso de comodines en el medio de una ruta de acceso.

Criterios de exclusiones de detección

- **Ruta de acceso**: exclusión de detección para una ruta de acceso especificada (o para cualquiera si se deja en blanco)
- **Nombre de la detección**: un objeto detectado se excluirá si coincide con el nombre de la detección definido. Si más tarde el archivo se infecta con otro malware, el nombre de la detección cambiará; así, se detectará como amenaza, y se realizará la acción adecuada contra ella. Si se define **Ruta de acceso**, solo se excluirán de la detección los archivos situados en esa ruta de acceso que coincidan con el **Nombre de la detección**. Para agregar dichas detecciones a la lista de exclusiones, utilice el [asistente de exclusión de detecciones](#). También puede ir a **Cuarentena**, hacer clic en un archivo en cuarentena y seleccionar **Restaurar y excluir**. Esta opción solo se muestra para los elementos evaluados como aptos para exclusión por el motor de detección.
- **Hash**: excluye un archivo según el hash especificado (SHA1), sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.

Detecciones

Las amenazas detectadas por el análisis en el acceso y las medidas tomadas contra ellas se registran en la pantalla **Detecciones**.

Las amenazas detectadas por el análisis a petición y las medidas tomadas se registran en **Análisis** > seleccione un análisis completado > **Mostrar detalles** > **Detecciones**.

Si se ha detectado una amenaza, pero no se ha desinfectado, toda la fila se resaltará en color rojo.

Acciones disponibles

- Para intentar desinfectar un archivo malicioso detectado, haga clic en la fila en concreto y seleccione **Analizar de nuevo con desinfección**.
- Para localizar el archivo que se ha detectado como malicioso pero no se ha eliminado, haga clic en la fila correspondiente, seleccione **Copiar ruta de acceso** y use un explorador de archivos para acceder al archivo.
- Para crear una [exclusión de detecciones](#) basada en el hash SHA-1 manualmente, seleccione **Copiar hash**.
- Para invocar el [asistente de exclusión](#), seleccione **Crear exclusión**.

Para aplicar **Analizar de nuevo con desinfección** o **Crear exclusión** en varias detecciones a la vez:

1. Marque la casilla de verificación de las detecciones correspondientes.
2. Haga clic en Acciones y seleccione la acción deseada.

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 ni aconsejable eliminarlos o si ESET Server Security for Linux los detecta incorrectamente como infectados. Es posible poner en cuarentena cualquier archivo. La cuarentena se recomienda cuando el comportamiento de un archivo es sospechoso y el análisis antivirus no lo ha detectado. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.

Administración de los elementos en cuarentena mediante la Interfaz web

En la pantalla **Cuarentena** se muestra una lista de los archivos almacenados en la carpeta de cuarentena. En la lista se muestran:

- La fecha y la hora de la cuarentena.
- La ruta de acceso a la ubicación original del archivo en cuarentena.
- El nombre de la detección (vacío para elementos puestos en cuarentena manualmente).
- El motivo de mover el archivo a la cuarentena (vacío para elementos puestos en cuarentena manualmente).

- El número de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias amenazas).
- El tamaño y el hash del elemento puesto en cuarentena.

Haga clic en el elemento puesto en cuarentena para mostrar las acciones disponibles:

- **Restaurar:** restaure el elemento puesto en cuarentena en su ubicación original
- **Restaurar y excluir:** restaure el elemento puesto en cuarentena en su ubicación original y cree una [exclusión de detección](#) que coincida con la ruta de acceso y el nombre de la detección
- **Copiar ruta de acceso:** copie la ruta de acceso original del archivo en el portapapeles
- **Copiar hash:** copie el hash SHA-1 del archivo en el portapapeles
- **Descargar:** descargue el elemento puesto en cuarentena en su disco duro
- **Eliminar de la cuarentena:** elimine de forma permanente el elemento puesto en cuarentena
- **Enviar para su análisis:** envíe una copia del elemento puesto en cuarentena para su análisis a ESET

La opción **Restaurar y excluir** solo se muestra para los elementos evaluados como susceptibles de exclusión por el motor de detección.

Ruta de acceso al directorio de cuarentena: `/var/opt/eset/efs/cache/quarantine/root/`

Para enviar un archivo en cuarentena para su análisis:

1. Seleccione un elemento y seleccione **Enviar para su análisis**.
2. Seleccione un **Motivo de envío de la muestra** adecuado.
 - **Archivo sospechoso:** un archivo que no se puede desinfectar durante un análisis o que tiene características inusuales
 - **Archivo de falso positivo:** un archivo identificado falsamente como malware
 - **Otros**
3. Introduzca su dirección de correo electrónico o seleccione **Enviar de forma anónima**.
4. Haga clic en **Siguiente**.
5. Facilite cualquier información adicional.
6. Haga clic en **Enviar**.

Administrar elementos puestos en cuarentena desde una ventana de terminal

Syntax: `/opt/eset/efs/bin/quar [OPTIONS]`

Opciones: forma abreviada	Opciones: forma completa	Descripción
-i	--import	Importar archivo en la cuarentena
-l	--list	Mostrar la lista de los archivos puestos en cuarentena
-r	--restore=id	Restaurar el elemento en cuarentena identificado por el id en la ruta definida por --restore-path
-e	--restore-exclude=id	Restaurar un elemento puesto en cuarentena identificado mediante su id y marcado con "x" en la columna excluible
-d	--delete=id	Eliminar un elemento puesto en cuarentena identificado mediante su id
-f	--follow	Esperar a los nuevos elementos y anexarlos a la salida
	--restore-path=path	Nueva ruta de acceso en la que restaurar un elemento puesto en cuarentena
-h	--help	Mostrar ayuda
-v	--version	Mostrar información sobre la versión y salir



Restaurar

La restauración no está disponible si el comando no se ejecuta con un usuario con privilegios.

EJEMPLO

Eliminar un elemento puesto en cuarentena con el "0123456789"

```
/opt/eset/efs/bin/quar -d 0123456789
```

o

```
/opt/eset/efs/bin/quar --delete=0123456789
```

Restaurar el elemento puesto en cuarentena con el id "9876543210" en la carpeta *Descargas* del usuario conectado y renombrarlo a *restoredFile.test*

```
/opt/eset/efs/bin/quar -r 9876543210 --restore-  
path=/home/$USER/Download/restoredFile.test
```

o

```
/opt/eset/efs/bin/quar --restore=9876543210 --restore-  
path=/home/$USER/Download/restoredFile.test
```

Restaurar un elemento puesto en cuarentena con el id "9876543210" marcado con una "x" en la columna

excluíble en la carpeta *Descargas*:

```
/opt/eset/efs/bin/quar -e 9876543210 --restore-  
path=/home/$USER/Download/restoredFile.test
```

o

```
/opt/eset/efs/bin/quar --restore-exclude=9876543210 --restore-  
path=/home/$USER/Download/restoredFile.test
```

Restaurar archivos puestos en cuarentena desde una ventana de terminal

1. Enumerar elementos puestos en cuarentena

```
/opt/eset/efs/bin/quar -l
```

2. Consulte el ID y el nombre del objeto puesto en cuarentena que desea restaurar y ejecute el siguiente comando:

```
/opt/eset/efs/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-  
path=/final/path/of/restored/file
```

Archivos enviados

ESET Server Security for Linux versión 8.1 y posteriores contiene información general sobre los archivos enviados para su análisis a ESET LiveGrid® o [ESET Dynamic Threat Defense](#).

Los archivos sospechosos se envían automáticamente para su análisis a ESET LiveGrid®. Si activa ESET Dynamic Threat Defense, los archivos enviados manualmente para su análisis se enviarán únicamente a EDTD. Sin embargo, es posible que algunos archivos enviados automáticamente se envíen a ESET LiveGrid®.

También puede [enviar archivos o sitios sospechosos para su análisis manualmente](#). Los archivos enviados manualmente tardan unos minutos en mostrarse en la lista.

Para ver la lista de archivos enviados para su análisis, inicie sesión en la [Interfaz web](#) y haga clic en **Archivos enviados**. También puede ejecutar cualquiera de los siguientes comandos desde una ventana de terminal como usuario con privilegios:

```
/opt/eset/efs/bin/lslog -n
```

```
/opt/eset/efs/bin/lslog --sent-files
```

Si desea crear una [exclusión de detección](#) temporal para un archivo enviado para su análisis, haga clic en el archivo para copiar su ruta de acceso o su hash.

Enviar muestra para el análisis

Si encuentra un archivo sospechoso en su ordenador o un sitio sospechoso en Internet, puede enviarlos al laboratorio de investigación de ESET para que los analicen.

ESET LiveGrid® El sistema de respuesta debe estar activado

1. En la [Interfaz web](#), haga clic en **Configuración > Motor de detección > Protección en la nube**.
2. Active **Activar sistema de respuesta ESET LiveGrid®** y haga clic en **Guardar**.

Para enviar una muestra para su análisis:

1. Haga clic en **Ayuda** o **Archivos enviados** y, a continuación, en **Enviar muestra para su análisis**.
2. Seleccione un **Motivo de envío de la muestra**.
 - **Archivo sospechoso**: un archivo que no se puede desinfectar durante un análisis o que tiene características inusuales
 - **Sitio sospechoso**: un sitio web infectado por malware
 - **Sitio de falso positivo**: un sitio web identificado falsamente como infectado por malware
 - **Archivo de falso positivo**: un archivo identificado falsamente como malware
 - **Otros**
3. Agregue la dirección del sitio o la ruta de acceso del archivo.
4. Introduzca su dirección de correo electrónico o seleccione **Enviar de forma anónima**.
5. Haga clic en **Siguiente**.
6. Proporcione información adicional.
7. Haga clic en **Enviar**.

También puede enviar [archivos en cuarentena](#) para su análisis.

Sucesos

Las acciones importantes realizadas en la Interfaz web de ESET Server Security for Linux, los intentos de inicio de sesión en la Interfaz web fallidos, los comandos relacionados con ESET Server Security for Linux ejecutados mediante una ventana de terminal y otra información se registran en la pantalla **Sucesos**.

Con cada acción registrada se incluye la siguiente información: hora a la que se produjo el suceso, componente (si está disponible), suceso y usuario

Visualización de sucesos en una ventana de terminal

Si desea visualizar el contenido de la pantalla **Sucesos** en una ventana de terminal, utilice la herramienta de línea de comandos `lslog`.

Syntax: `/opt/eset/efs/bin/lslog[OPCIONES]`

Opciones: forma abreviada	Opciones: forma completa	Descripción
-f	--follow	Esperar a los nuevos registros y anexarlos a la salida
-o	--optimize	Optimizar los registros
-c	--csv	Mostrar los registros en formato CSV
-e	--events	Enumerar los registros de sucesos
-n	--sent-files	Mostrar una lista de los archivos enviados para su análisis
-s	--scans	Enumerar los registros de análisis a petición
	--with-log-name	Mostrar también columna Nombre del registro
	--ods-details=log-name	Mostrar detalles de un análisis a petición identificado mediante el nombre del registro
	--ods-detections=log-name	Mostrar detecciones de un análisis a petición identificado mediante el nombre del registro
	--ods-notscanned=log-name	Mostrar elementos no analizados de un análisis a petición identificados mediante el nombre del registro
-d	--detections	Enumerar las entradas del registro de detección

EJEMPLOS

Mostrar todos los registros de sucesos

```
/opt/eset/efs/bin/lslog -e
```

Guardar todos los registros de sucesos en formato CSV en un archivo en el directorio *Documents* del usuario actual

```
/opt/eset/efs/bin/lslog -ec > /home/$USER/Documents/eventlogs.csv
```

Configuración

Si desea modificar la configuración predeterminada de ESET Server Security for Linux, diríjase a la pantalla **Configuración**. Puede ajustar el [comportamiento de detección](#), modificar la configuración de conexión y actualización del producto o cambiar la contraseña y el certificado de la [Interfaz web](#). Para aplicar los cambios, haga clic en **Guardar** en la pantalla **Configuración**.

Si ha configurado ESET Server Security for Linux según sus necesidades y desea guardar la configuración para usarla posteriormente (o para utilizarla con otra instancia de ESET Server Security for Linux), puede exportarla a un archivo *.xml*.

Ejecute los siguientes comandos desde una ventana de terminal con privilegios de usuario root.

Exportación de la configuración

```
/opt/eset/efs/sbin/cfg --export-xml=/tmp/export.xml
```

Importación de la configuración

```
/opt/eset/efs/sbin/cfg --import-xml=/tmp/export.xml
```

Opciones disponibles

Forma abreviada	Forma completa	Descripción
	--import-xml	import settings
	--export-xml	export settings
-h	--help	show help
-v	--version	show version information

Motor de detección

La configuración predeterminada del comportamiento de detección ofrece el nivel de seguridad básico, que incluye:

- [Protección del sistema de archivos en tiempo real](#)
- Optimización inteligente (la combinación más eficiente de protección del sistema y la velocidad de análisis)
- Sistema de reputación [ESET LiveGrid](#)

Para activar funciones de protección adicionales, haga clic en **Configuración > Motor de detección**:

- Detección de [aplicaciones potencialmente indeseables](#)
- Detección de [aplicaciones potencialmente peligrosas](#) (por ejemplo, registradores de pulsaciones de teclado, herramientas para averiguar contraseñas).
- Active el envío de muestras sospechosas o infectadas.
- Configure las [exclusiones](#) (archivos, directorios no incluidos en el análisis) para agilizar el análisis.
- Ajuste el [nivel de desinfección](#).
- Active la [caché local compartida](#).

Todas las amenazas detectadas y las acciones realizadas para resolverlas se registran en la pantalla **Detecciones**.

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 for Linux 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.

Exclusiones

Exclusiones de extensiones de archivo

Este tipo de exclusión se puede configurar para la protección del sistema de archivos en tiempo real, para análisis a petición y para el análisis remoto.

1. En la [Interfaz web](#), haga clic en **Configuración > Motor de detección**.
2. Haga clic en:
 - **Protección del sistema de archivos en tiempo real > Parámetros de ThreatSense** para modificar las exclusiones relacionadas con [Protección del sistema de archivos en tiempo real](#)
 - **Análisis de malware > Análisis a petición > Parámetros de ThreatSense** para modificar las exclusiones relacionadas con [Análisis a petición \(análisis personalizado\)](#)
 - **Análisis remoto > Parámetros de ThreatSense** para modificar exclusiones relacionadas con el [análisis remoto](#)
3. Junto a **Extensiones de archivo excluidas del análisis**, haga clic en **Editar**.
4. Haga clic en **Agregar** y escriba la extensión que desea excluir. Para definir varias extensiones a la vez, haga clic en **Escribir varios valores** y escriba las extensiones aplicables separadas por una línea nueva u otro separador que elija.
5. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
6. Haga clic en **Guardar** para guardar los cambios.

Exclusiones de rendimiento

Al excluir las rutas de acceso (carpetas) del análisis, el tiempo necesario para analizar el sistema de archivos para detectar malware puede reducirse significativamente.

1. En la [Interfaz web](#), haga clic en **Configuración > Motor de detección > Básico**.
2. Junto a **Exclusiones de rendimiento**, haga clic en **Editar**.
3. Haga clic en **Agregar** y defina la **ruta de acceso** que va a omitir el explorador. Si lo desea, agregue un

comentario para su información.

4. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.

5. Haga clic en **Guardar** para guardar los cambios.

Ruta de exclusión

`/root/*`: el directorio "root", todos sus subdirectorios y el contenido que incluyen.

`/root`: solo el archivo "root".

`/root/file.txt`: solo file.txt en el directorio "root".

Comodines en el medio de una ruta de acceso

✓ Le recomendamos encarecidamente no usar comodines en el medio de una ruta de acceso (por ejemplo `/home/user/*/data/file.dat`) a menos que la infraestructura de su sistema lo requiera. Consulte el siguiente [artículo de la base de conocimiento](#) para obtener más información.

Cuando se utilizan [exclusiones de detección](#), no hay restricciones en lo que respecta al uso de comodines en el medio de una ruta de acceso.

Exclusiones de procesos

La función Exclusiones de procesos le permite excluir procesos de aplicación de la [protección del sistema de archivos en tiempo real](#).

Las soluciones de copia de seguridad buscan mejorar la velocidad, la integridad de los procesos y la disponibilidad de los servicios. Suelen utilizar técnicas que se sabe que entran en conflicto con la protección contra malware a nivel de archivo para conseguirlo. Al intentar completar una migración en tiempo real de máquinas virtuales pueden producirse problemas similares. Normalmente, la única forma eficaz de evitar estas situaciones es desactivar el software antimalware.

Al excluir procesos específicos (por ejemplo, los de la solución de copia de seguridad), todas las operaciones de archivo atribuidas a dichos procesos excluidos se ignoran y se consideran seguras, lo que reduce al mínimo la interferencia con el proceso de copia de seguridad. Recomendamos tener precaución al crear exclusiones: una herramienta de copia de seguridad excluida puede acceder a archivos infectados sin desencadenar una alerta, por lo que los permisos ampliados solo se permiten en el módulo de protección en tiempo real.

Esta función se ha diseñado para excluir herramientas de copia de seguridad. Excluir el proceso de análisis de la herramienta de copia de seguridad garantiza la estabilidad del sistema y no afecta al rendimiento de la copia de seguridad, pues la copia de seguridad no se ralentiza mientras se ejecuta. En último término, reduce al mínimo el riesgo de posibles conflictos.

Agregar binarios a la lista de procesos excluidos

1. Haga clic en **Configuración** > **Motor de detección** > **Protección del sistema de archivos en tiempo real**.

2. En la sección **Básico** > **Exclusiones de procesos**, haga clic en **Editar** junto a **Procesos que se excluirán del análisis**.

3. Haga clic en **Agregar**.
4. Introduzca la ruta de acceso absoluta del binario.
5. Haga clic en **Guardar** dos veces.
6. En la pantalla **Configuración**, haga clic en **Guardar**.

En cuanto se agrega un binario a las exclusiones, ESET Server Security for Linux deja de supervisar su actividad. Los análisis no se ejecutan en ninguna operación de archivo realizada por ese binario.

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

Exportar/importar exclusiones de detección

Para compartir las exclusiones de procesos configuradas con otra instancia de ESET Server Security for Linux no administrada de forma remota, exporte la configuración:

1. Haga clic en **Configuración > Motor de detección > Protección del sistema de archivos en tiempo real**.
2. En la sección **Básico > Exclusiones de procesos**, haga clic en **Editar** junto a **Procesos que se excluirán del análisis**.
3. Haga clic en **Exportar**.
4. Haga clic en el icono de descarga  junto a **Descargar los datos exportados**.
5. Si el navegador le pide que abra o guarde el archivo, seleccione **Guardar**.

Para importar el archivo de exclusiones de procesos exportado:

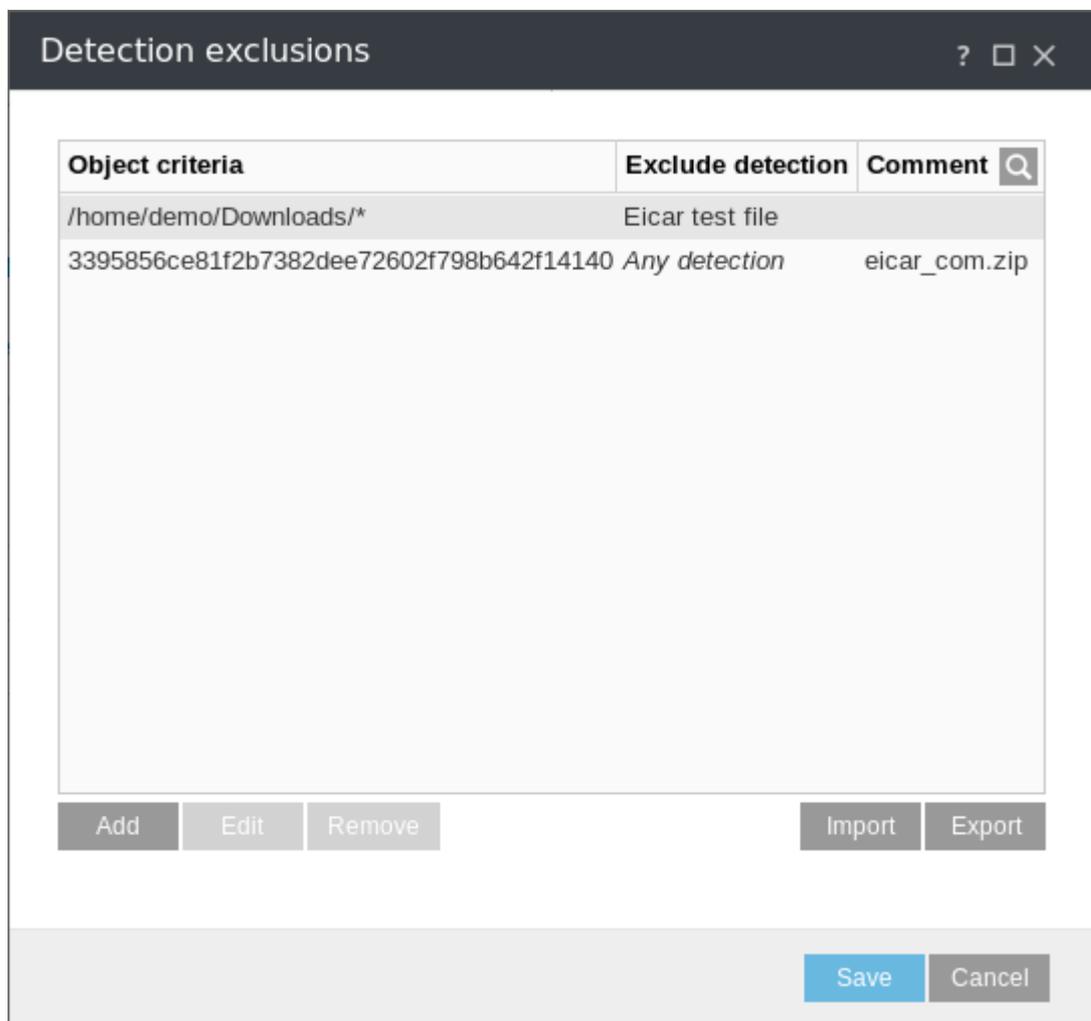
1. Haga clic en **Configuración > Motor de detección > Protección del sistema de archivos en tiempo real**.
2. En la sección **Básico > Exclusiones de procesos**, haga clic en **Editar** junto a **Procesos que se excluirán del análisis**.
3. Haga clic en **Importar** y, a continuación, en el icono de buscar  para buscar el archivo exportado y haga clic en **Abrir**.
4. Haga clic en **Importar > Aceptar > Guardar**.
5. En la pantalla **Configuración**, haga clic en **Guardar**.

Exclusiones de detección

Las exclusiones de detección le permiten excluir objetos de la desinfección (eliminación o traslado a cuarentena) filtrando el nombre de detección, la ruta de acceso del objeto o su hash.

Cómo funcionan las exclusiones de detección

Las exclusiones de detección no excluyen archivos y carpetas del análisis como las **Exclusiones de rendimiento**. Las exclusiones de detección solo evitan que se pongan en cuarentena o se eliminen objetos cuando los detecta el motor de detección y existe una regla apropiada en la lista de exclusiones. Consulte las reglas de muestra en la imagen siguiente. La regla de la primera fila excluirá un objeto que se detecte como *Eicar test file* y se encuentre en */home/demo/Download/some.file*. La regla de la segunda fila excluirá todos los objetos detectados que tengan el hash SHA-1 correspondiente, sea cual sea el nombre de la detección.



Criterios del objeto de exclusiones de detección

- **Ruta de acceso:** exclusión de detección para una ruta de acceso especificada (o para cualquiera si se deja en blanco)
- **Nombre de la detección:** un objeto detectado se excluirá si coincide con el nombre de la detección definido. Si más tarde el archivo se infecta con otro malware, el nombre de la detección cambiará; así, se detectará como amenaza, y se realizará la acción adecuada contra ella. Si se define **Ruta de acceso**, solo se excluirán de la detección los archivos situados en esa ruta de acceso que coincidan con el **Nombre de la detección**. Para agregar dichas detecciones a la lista de exclusiones, utilice el [asistente de exclusión de detecciones](#). También puede ir a **Cuarentena**, hacer clic en un archivo en cuarentena y seleccionar **Restaurar y excluir**. Esta opción solo se muestra para los elementos evaluados como aptos para exclusión por el motor de detección.
- **Hash:** excluye un archivo según el hash especificado (SHA1), sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.

Agregar o editar una exclusión de detección

Definir manualmente exclusiones de detección

1. Haga clic en **Configuración > Motor de detección**.
2. Haga clic en **Editar** junto a **Exclusiones de detección** y haga clic en **Agregar**.
3. Defina los criterios de exclusión:
 - **Ruta de acceso:** exclusión de detección para una ruta de acceso especificada (o para cualquiera si se deja en blanco)
 - **Nombre de la detección:** un objeto detectado se excluirá si coincide con el nombre de la detección definido. Si más tarde el archivo se infecta con otro malware, el nombre de la detección cambiará; así, se detectará como amenaza, y se realizará la acción adecuada contra ella. Si se define **Ruta de acceso**, solo se excluirán de la detección los archivos situados en esa ruta de acceso que coincidan con el **Nombre de la detección**. Para agregar dichas detecciones a la lista de exclusiones, utilice el [asistente de exclusión de detecciones](#). También puede ir a **Cuarentena**, hacer clic en un archivo en cuarentena y seleccionar **Restaurar y excluir**. Esta opción solo se muestra para los elementos evaluados como aptos para exclusión por el motor de detección.
 - **Hash:** excluye un archivo según el hash especificado (SHA1), sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.
4. Haga clic en **Aceptar** y, a continuación, en **Guardar**.
5. En la pantalla **Configuración**, haga clic en **Guardar**.

Utilizar el asistente de exclusión de detecciones

1. Haga clic en una [detección](#) y seleccione **Crear exclusión**.
2. Seleccione los criterios de exclusión adecuados:
 - **Archivo exacto:** excluir un archivo por hash SHA-1
 - **Detección:** excluir un archivo por nombre de detección
 - **Ruta de acceso y Detección:** excluir un archivo que coincida con la ruta de acceso y el nombre de detección
3. Escriba un comentario si corresponde. Aparece en la lista de exclusiones de detección en **Configuración > Motor de detección >** haga clic en **Editar** junto a **Exclusiones de detección**.
4. Haga clic en **Crear exclusión**.

Editar o quitar una exclusión de detección

1. Haga clic en **Configuración > Motor de detección**.

2. Haga clic en **Editar** junto a **Exclusiones de detección**.
3. Seleccione una exclusión y haga clic en **Editar** o en **Quitar**.
4. Guarde los cambios.

Exportar/importar exclusiones de detección

Para compartir las exclusiones de detección configuradas con otra instancia de ESET Server Security for Linux no administrada de forma remota, exporte la configuración:

1. Haga clic en **Configuración > Motor de detección**.
2. Haga clic en **Editar** junto a **Exclusiones de detección** y haga clic en **Exportar**.
3. Haga clic en el icono de descarga  junto a **Descargar los datos exportados**.
4. Si el navegador le pide que abra o guarde el archivo, seleccione **Guardar**.

Para importar el archivo de exclusiones de detección exportado:

1. Haga clic en **Configuración > Motor de detección**.
2. Haga clic en **Editar** junto a **Exclusiones de detección** y haga clic en **Importar**.
3. Haga clic en el icono de buscar  para buscar el archivo exportado y haga clic en **Abrir**.
4. Haga clic en **Importar > Aceptar > Guardar**.
5. En la pantalla **Configuración**, haga clic en **Guardar**.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con el antivirus en el sistema. Todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. De forma predeterminada, la protección del sistema de archivos en tiempo real se inicia al arrancar el sistema y proporciona análisis ininterrumpido.

i La protección del sistema de archivos en tiempo real no analiza el contenido de los archivos comprimidos. Analiza el contenido de determinados archivos comprimidos de autoextracción cuando se descargan en el disco duro.

No se admite el análisis en el acceso remoto de una carpeta compartida NFS montada localmente

i Supongamos que tiene el servidor del kernel de NFS instalado en un equipo protegido por ESET Server Security for Linux (ESSL); si su carpeta compartida está montada a nivel local en un equipo remoto no protegido por ESSL, el análisis en el acceso de ESSL no funcionaría ahí.

En casos excepcionales (por ejemplo, si hay un conflicto con otro análisis en tiempo real), la protección en tiempo

real se puede desactivar:

1. Haga clic en **Configuración > Motor de detección > Protección del sistema de archivos en tiempo real > Básico**.
2. Desactive **Activar la protección del sistema de archivos en tiempo real**.

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 :** activa o desactiva el análisis al abrir archivos.
- **Crear el archivo:** activa o desactiva el análisis durante la creación de archivos.
- **Acceder a medios extraíbles:** activa o desactiva el análisis automático de medios extraíbles cuando está conectado al ordenador.

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. Si se utilizan métodos de detección con la tecnología ThreatSense (tal como se describe en la sección [Parámetros de ThreatSense](#)), 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 de la base de datos 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 esta configuración:

1. En la [interfaz web](#), haga clic en **Configuración > Motor de detección > Protección del sistema de archivos en tiempo real > Parámetros de ThreatSense**.
2. Active o desactive **Activar optimización inteligente**.
3. Haga clic en **Guardar**.

Parámetros de ThreatSense

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 eficazmente los programas peligrosos (rootkits).

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

- Tipos y extensiones de archivo que se analizarán
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **Configuración > Motor de detección**, seleccione uno de los módulos mencionados a continuación y haga clic en **Parámetros de ThreatSense**. Cada contexto de seguridad puede requerir su propia configuración y, por ello, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- **Protección del sistema de archivos en tiempo real**
- **Análisis de malware**
- **Análisis remoto**

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 ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados).

Objetos a analizar

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

- **Sectores de inicio/UEFI:** analiza los sectores de inicio o UEFI para detectar virus en el registro de inicio principal
- **Archivos de correo:** el programa admite las extensiones DBX (Outlook Express) y EML
- **Archivos comprimidos:** el programa admite las 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 autoextraíbles:** los archivos comprimidos de autoextracción (SFX) son archivos comprimidos que pueden extraerse por sí solos
- **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



La protección del sistema de archivos en tiempo real no analiza el contenido de los archivos comprimidos. Analiza el contenido de determinados archivos comprimidos de autoextracción cuando se descargan en el disco duro.

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 la base de firmas de virus anterior no cubría. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas
- **Heurística avanzada/Firmas de ADN:** la heurística avanzada es un algoritmo heurístico único desarrollado por ESET 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)

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 haciéndose 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
- **Activar 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 el apartado **Límites** puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Para modificar la configuración de los objetos, desactive **Usar parámetros predeterminados del objeto**.

- **Tamaño máximo del objeto:** define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado
- **Tiempo máximo de análisis para el objeto (seg.):** define el tiempo máximo asignado para analizar un objeto. Si se especifica un valor definido por el usuario, el módulo antivirus detendrá el análisis de un objeto cuando se haya agotado el tiempo, independientemente de si el análisis ha finalizado o no. Valor predeterminado: ilimitado

Configuración del análisis de archivos comprimidos

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

- **Nivel de anidamiento de archivos:** especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10
- **Tamaño máx. de archivo en el archivo comprimido:** esta opción 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

Valores predeterminados



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

Parámetros adicionales de ThreatSense

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. 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.

Protección en la nube

Vínculos rápidos: [Protección en la nube](#), [Envío de muestras](#), [ESET Dynamic Threat Defense](#)

[ESET LiveGrid®](#) es un sistema avanzado de alerta temprana compuesto por varias tecnologías en la nube. Ayuda a detectar amenazas emergentes basadas en la reputación y mejora el rendimiento del análisis mediante la creación de listas blancas.

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

Modifique la configuración en **Configuración > Motor de detección > Protección en la nube**.

Protección en la nube

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.

Activar ESET Dynamic Threat Defense

Disponible a partir de ESET Server Security for Linux versión 8.1. Los datos se enviarán a [ESET Dynamic Threat Defense](#).

Enviar informes de bloqueo y datos de diagnóstico

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

Ayudar a mejorar el producto enviando estadísticas de uso 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 detectadas

De acuerdo con la opción seleccionada, puede enviar muestras infectadas a ESET 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 todos los archivos en formato PE (por ejemplo, *.exe*, *.dll*, *.sys*) y los archivos ELF (por ejemplo, *.axf*, *.bin*, *.elf*). También archivos de texto con el indicador "x" (ejecutable).
- 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*, *.ps1*, *.sh*, *.py*, *.pl*)
- Otros: incluye otros tipos de archivos (*.jar*, *.reg*, *.msi*, *.swf*, *.lnk*)
- Documentos - Incluye documentos creados con Microsoft Office, Libre Office u otra herramienta de oficina, o archivos PDF con contenido activo.

Exclusiones

Haga clic en **Editar** junto a **Exclusiones** para configurar cómo se envían las amenazas a los laboratorios 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

[ESET Dynamic Threat Defense](#) (EDTD) es un servicio de pago prestado por ESET. Su finalidad es agregar una capa de protección diseñada específicamente para mitigar las nuevas amenazas en el mundo.

Disponibilidad

El servicio solo está disponible si ESET Server Security for Linux versión 8.1 o posterior se [administra de forma remota](#). [Active EDTD antes de usarlo](#).



Según la [configuración de la protección proactiva de EDTD](#), un archivo enviado para su análisis puede bloquearse de la ejecución hasta que se reciba un resultado. Este bloqueo va acompañado del mensaje "Operación no permitida" o de un mensaje similar.

Para ver el estado del servicio EDTD en su instancia de ESSL, ejecute uno de los siguientes comandos en una ventana de terminal con un usuario con privilegios:

```
/opt/eset/efs/sbin/cloud -e
```

o

```
/opt/eset/efs/sbin/cloud --edtd-status
```

Para activar el servicio en ESSL:

1. [Active EDTD](#).
2. En la [Interfaz web](#), haga clic en **Configuración > Motor de detección > Protección en la nube**.
3. Active **Activar el sistema de reputación ESET LiveGrid® (recomendado)**, **Activar el sistema de respuesta ESET LiveGrid®** y **Activar ESET Dynamic Threat Defense**.
4. Para modificar la configuración predeterminada de EDTD, haga clic en ESET Dynamic Threat Defense y ajuste las opciones disponibles. Para obtener más información sobre estos ajustes de EDTD, consulte la tabla con el encabezado "Sección: ESET Dynamic Threat Defense" en la [documentación de EDTD](#).
5. Haga clic en **Guardar**.

[Instrucciones de activación de EDTD de forma remota a través de ESET PROTECT](#)

1. En ESET PROTECT, haga clic en **Políticas > Nueva política** y escriba un nombre para la política.
2. Haga clic en **Configuración** y seleccione **ESET Server/File Security for Linux (V7+)** en el menú desplegable.
3. **Motor de detección > Protección en la nube**.
4. Active **Activar el sistema de reputación ESET LiveGrid® (recomendado)**, **Activar el sistema de respuesta ESET LiveGrid®** y **Activar ESET Dynamic Threat Defense**.
5. Para modificar la configuración predeterminada de EDTD, haga clic en ESET Dynamic Threat Defense y ajuste las opciones disponibles. Para obtener más información sobre estos ajustes de EDTD, consulte la tabla con el encabezado "Sección: ESET Dynamic Threat Defense" en la [documentación de EDTD](#).
6. Haga clic en **Continuar > Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.
7. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

Análisis de malware

En esta sección se ofrecen opciones para seleccionar los parámetros del **Análisis a petición**.

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.

Análisis remoto (análisis ICAP)

Para proteger de forma remota los dispositivos y el software compatible con ICAP externos, active y configure el **Análisis remoto**.

1. En la Interfaz web, **diríjase a Configuración > Motor de detección > Análisis remoto**.
2. Active el interruptor situado junto a **Activar el análisis remoto con el servicio ICAP**.
3. Haga clic en **Editar** junto a **Direcciones y puertos de recepción de conexiones**, haga clic en **Agregar** y defina la dirección y el puerto del servidor ICAP. Haga clic en **Aceptar** y, a continuación, en **Guardar**.
4. Si lo desea, revise y modifique los [parámetros de ThreatSense](#).
5. Haga clic en **Guardar**.

[Vea cómo integrar el servidor de ICAP con EMC Isilon](#).

Clientes de ICAP compatibles

- Dell EMC Isilon
- Citrix ShareFile
- EFT Enterprise
- Nutanix

Niveles de desinfección

- **Sin desinfección:** los archivos infectados no se desinfectan automáticamente. El número de amenazas detectadas se resalta en color rojo en la columna **Detecciones realizadas**. La columna **Desinfectado** se resalta en color rojo, pero muestra 0.
- **Desinfección normal:** el programa intentará desinfectar o eliminar automáticamente los archivos infectados, excepto aquellos que podrían causar la pérdida de datos útiles, como en un archivo comprimido que contiene una mezcla de archivos infectados y desinfectados. El número de archivos detectados en este archivo comprimido se contará en las **Detecciones realizadas**, y la columna **Desinfectado** aparecerá en rojo.

- **Desinfección estricta:** el programa desinfectará o eliminará todos los archivos infectados. Las únicas excepciones son los archivos del sistema.
- **Desinfección rigurosa:** el programa desinfecta o elimina todos los archivos infectados, sin excepción.
- **Eliminar:** el programa elimina todos los archivos infectados, sin excepción.

Actualización

De forma predeterminada, el **Tipo de actualización** está configurado como **Actualización normal**. Este ajuste garantiza que la base de firmas de detección y los módulos del producto se actualizan automáticamente a diario desde los [servidores de actualización de ESET](#).

Las actualizaciones previas a su lanzamiento incluyen las correcciones de errores más recientes o los métodos de detección que estarán disponibles próximamente para el público general. No obstante, pueden no ser estables en todo momento, y por tanto no se recomienda su uso en un entorno de producción.

Actualizaciones 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).

Si una actualización de ESET Server Security for Linux no resulta estable, revierta la actualización del módulo al estado anterior. Haga clic en **Panel de control > Actualización de los módulos > Reversión de módulos**, seleccione el periodo que desee y haga clic en **Revertir**.

De forma predeterminada, solo se almacena una instantánea de los módulos de forma local. Para almacenar más instantáneas, aumente el **Número de instantáneas almacenadas localmente** hasta el número deseado.

Actualización de componentes de los programas

De forma predeterminada, ESET Server Security for Linux (ESSL) no actualiza los componentes del producto automáticamente. Para activar las actualizaciones automáticas, seleccione **Actualizar automáticamente** en el cuadro de lista **Modo de actualización**.

Modo de actualización

Actualizar automáticamente: los paquetes nuevos se descargan e instalan automáticamente tras el siguiente reinicio del SO. Si se han realizado modificaciones del Acuerdo de licencia para el usuario final, el usuario debe aceptar el Acuerdo de licencia para el usuario final para poder descargar el paquete nuevo.

No actualizar nunca: los paquetes nuevos no se descargan, pero el producto indica en el **Panel** que hay nuevos paquetes disponibles.

Servidor personalizado, Nombre de usuario, Contraseña

Si administra varias instancias de ESSL y prefiere actualizar desde una ubicación personalizada, defina la dirección y las credenciales de acceso aplicables de un servidor HTTP(S), una unidad local o una unidad extraíble.

Herramientas

En el apartado **Configuración > Herramientas** de la Interfaz web de ESET Server Security for Linux puede modificar la configuración general de ESET Server Security for Linux.

- Especificar los datos de un [servidor proxy](#) para conectarse a Internet
- Cambiar la contraseña o el certificado de la [Interfaz web](#)
- Configurar cómo se gestionan los [archivos de registro](#)

También puede [programar](#) el análisis a petición.

Servidor proxy

Configure ESET Server Security for Linux para usar su servidor proxy para conectarse a Internet o los servidores de actualizaciones definidos (Mirror). Para modificar los parámetros, haga clic en **Configuración > Herramientas > Servidor proxy**.

Interfaz web

Para cambiar la dirección IP y el puerto de la Interfaz web de ESET Server Security for Linux o agregar más direcciones en las que se desea que la Interfaz web esté disponible, haga clic en **Editar** junto a **Direcciones y puertos de recepción de conexiones**. Haga clic en **Agregar**, escriba la dirección y el puerto correctos, haga clic en **Aceptar** y, a continuación, haga clic en **Guardar**. Haga clic en **Guardar** en la pantalla **Configuración**.

Para actualizar la contraseña de la Interfaz web, haga clic en **Cambiar contraseña**. Escriba una contraseña nueva y haga clic en **Guardar**.

Para importar un certificado nuevo y la clave privada correspondiente, utilice los botones **Certificado** y **Clave privada**. Si el certificado está protegido mediante contraseña, escriba la contraseña en el campo **Contraseña de los certificados**. Haga clic en **Guardar** en la pantalla **Configuración**.

Desactivación y activación de la Interfaz web

Si desactiva el interruptor situado junto a **Activar la Interfaz web** y hace clic en **Guardar** en la pantalla Configuración, se cerrará su sesión automáticamente y la Interfaz web dejará de estar disponible.

 [Podrá volver a activar la Interfaz web desde una ventana de terminal.](#)

Si instala ESET Server Security for Linux de forma remota mediante ESET PROTECT, la Interfaz web no se activa.

Si desea acceder a la Interfaz web desde un equipo concreto, ejecute el siguiente comando desde una ventana de terminal:

```
sudo /opt/eset/efs/sbin/setgui -gre
```

En la salida final se mostrarán la dirección URL de la Interfaz web y las credenciales de acceso.

Para que la Interfaz web esté disponible en una dirección IP y un puerto personalizados, por ejemplo 10.1.184.230:9999, ejecute el siguiente comando desde una ventana de terminal:

```
sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999
```

Para activar la interfaz web con ESET PROTECT, utilice la [tarea Ejecutar comando](#) para ejecutar el siguiente comando:

```
/opt/eset/efs/sbin/setgui -re --password=<password>
```

donde <password> representa la contraseña deseada definida por usted.

[Opciones disponibles para el comando setgui](#)

Opciones: forma abreviada	Opciones: forma completa	Descripción
-g	--gen-password	Generar una contraseña nueva para acceder a la Interfaz web
-p	--password=PASSWORD	Definir una contraseña nueva para acceder a la Interfaz web
-f	--passfile=FILE	Definir una contraseña nueva leída de un archivo para acceder a la Interfaz web
-r	--gen-cert	Generar una clave privada y un certificado nuevos
-a	--cert-password=PASSWORD	Establecer la contraseña del certificado
-l	--cert-passfile=FILE	Establecer la contraseña del certificado leída de un archivo
-i	--ip-address=IP:PORT	Dirección del servidor (IP y número de puerto)
-c	--cert=FILE	Importar certificados
-k	--key=FILE	Importar la clave privada
-d	--disable	Desactivar la Interfaz web
-e	--enable	Activar la Interfaz web

Dirección y puerto de recepción de conexiones

ESET Server Security for Linux le permite configurar una dirección IP y un puerto personalizados para la [Interfaz web](#) y el [servidor de ICAP](#).

Archivos de registro

Modifique la [configuración](#) del sistema de registro de ESET Server Security for Linux.

Detalle de registro mínimo

El nivel de detalle define los detalles que incluyen los archivos de registro relacionados con ESET Server Security for Linux.

- **Alertas críticas:** incluye solo los errores críticos (por ejemplo, no se ha podido iniciar la protección antivirus).
- **Errores:** se registran los errores del tipo "Error al descargar el archivo", además de las **alertas críticas**.
- **Alertas:** se registran los errores críticos y los mensajes de advertencia, además de los **errores**.
- **Registros informativos:** registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Registros de diagnóstico:** incluye la información necesaria para ajustar el programa y todos los registros anteriores.

Eliminar automáticamente los registros con una antigüedad de más de (días)

Para ocultar entradas de registro anteriores al número de días especificado desde la pantalla **Sucesos**, **Detecciones** o **Archivos enviados**, o la lista de registros (**LSLog**):

1. Active **Eliminar automáticamente los registros con una antigüedad de más de (días)**.
2. Ajuste el día para especificar la antigüedad de los archivos que desea ocultar.
3. Haga clic en **Guardar**.

Los registros ocultados no pueden volver a mostrarse. Las entradas en el registro relativas al análisis a petición se eliminan directamente. Para evitar que se acumulen los registros ocultos, active la optimización automática de los archivos de registro.

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 (%)**. Los registros no utilizados representan las entradas en el registro ocultas. 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.

Utilidad syslog

[Utilidad syslog](#) es un parámetro de registro syslog que se usa para agrupar los mensajes de registro similares. Por ejemplo, las entradas en el registro correspondientes a demonios (que recopilan archivos de registro mediante el demonio de la utilidad syslog) se pueden enviar a `/var/log/daemon.log` si así se configura. Con el cambio reciente a systemd y su diario, la función syslog tiene menos importancia, pero se puede seguir usando para el filtrado de registros.

Planificador de tareas

ESET Server Security for Linux v8 y posteriores permite realizar [análisis personalizados](#) periódicos semanales en días y horas definidos.

Programar un análisis

1. En la [Interfaz web](#), haga clic en **Configuración > Herramientas > Tareas programadas**.
2. Junto a **Tareas**, haga clic en **Editar**.
3. Haga clic en **Agregar**.
4. Asigne un nombre a la programación, defina una hora y seleccione los días en los que se desencadenará el análisis personalizado de forma automática. Haga clic en **Siguiente**.
5. Seleccione [Perfil de análisis](#).
6. Seleccione **Objetos de análisis** o objetos personalizados definidos separados por una línea nueva.
7. Seleccione o anule la selección de las **Opciones** disponibles ([Análisis con desinfección](#), [exclusiones](#) de análisis).
8. Haga clic en **Finalizar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
9. Haga clic en **Guardar** para guardar todos los cambios.

Para modificar una tarea programada, en el paso 3 anterior, seleccione la tarea en cuestión y haga clic en **Editar**. Continúe con el resto de pasos.

Para quitar una tarea programada, en el paso 3 anterior, seleccione la tarea en cuestión y haga clic en **Quitar**. Continúe con los pasos 8 y 9.

Ejecución de tareas programadas

- ✓ El planificador de tareas utiliza [cron](#) y se ejecuta si el ordenador correspondiente está activo. Si el ordenador está apagado, la tarea se ejecutará a la siguiente hora programada en que el ordenador esté encendido.

Interfaz de usuario

Para configurar notificaciones de [estado de la protección](#):

1. En la [interfaz web](#), haga clic en **Configuración > Interfaz de usuario > Elementos de la interfaz de usuario**.
2. Haga clic en **Editar** junto a **Mostrar en Estado de la protección**.
3. Seleccione el [estado de la aplicación](#) correspondiente.
4. Haga clic en **Aceptar** y, a continuación, en **Guardar**.

Notas

- i** El estado no seleccionado está silenciado en [Estado de la protección](#). Los cambios solo se aplican localmente.

Si administra ESET Server Security for Linux de forma remota, consulte [Mostrar estados en ESET PROTECT](#).

Estados

Cada estado seleccionado en **Configuración > Interfaz de usuario > Mostrar en Estado de la protección > Editar** muestra una notificación en **Panel > Estado de la protección** si el módulo relacionado está desactivado, no es funcional o falta.

Notas

- i** El estado no seleccionado está silenciado en [Estado de la protección](#). Los cambios solo se aplican localmente.

Mostrar estados en ESET PROTECT

Para mostrar estados en ESET PROTECT al administrar ESET Server Security for Linux de forma remota:

1. En ESET PROTECT, haga clic en **Políticas > Nueva política** y escriba un nombre para la política.
2. Haga clic en **Configuración** y seleccione **ESET Server/File Security for Linux (V7+)** en el menú desplegable.
3. Haga clic en **Interfaz de usuario > Elementos de la interfaz de usuario**.
4. Haga clic en **Editar** junto a **Enviar a ESET PROTECT**.
5. Seleccione los estados adecuados y haga clic en **Aceptar**.
6. Haga clic en **Guardar** en cada cuadro de diálogo en el que haya realizado un cambio y, a continuación, haga clic en **Finalizar**.

Administración remota

Para administrar ESET Server Security for Linux de forma remota, conecte el ordenador en el que se aloja su producto de seguridad ESET a ESET PROTECT.

1. [Implemente ESET Management Agent](#).
2. [Agregue el ordenador a ESET PROTECT](#).

A partir de este momento, podrá ejecutar las [tareas del cliente](#) correspondientes relacionadas con ESET Server Security for Linux.

A partir de la versión 8.1, ESSL permite la fusión [de listas locales y remotas de políticas](#).

Seguridad de contenedor

Los servidores Linux suelen ser la base sobre la que se ejecutan contenedores Docker y herramientas de orquestación Docker. La función de seguridad de contenedor forma parte de la [protección del sistema de archivos en tiempo real](#) de ESET Server Security for Linux (ESSL).

ESSL v8.1 puede detectar amenazas o actividades sospechosas en un contenedor y bloquearlas, pero no las puede eliminar, lo que significa que se bloqueará la ejecución de un script sospechoso, pero no se eliminará. Puede eliminarla manualmente.

La [protección del sistema de archivos en tiempo real](#) de ESET puede analizar el contenedor en las siguientes fases:

- Proceso de construcción de la imagen del contenedor
- Implementación de la imagen del contenedor en un equipo protegido por ESSL

La actividad dentro del contenedor también se analiza en tiempo real en busca de comportamiento sospechoso.

En ESET probamos la versión 20.10.7 de [Docker CE](#) (Community Edition).

Ejemplos de casos de uso

En este capítulo vamos a tratar los casos de uso más habituales de ESET Server Security for Linux.

Integración del servidor de ICAP con EMC Isilon

Visión general

Puede analizar los archivos que almacena en un clúster de Isilon en busca de virus informáticos, malware y otras amenazas para la seguridad gracias a la integración con ESET Server Security for Linux (ESSL) mediante Internet Content Adaptation Protocol (ICAP).

Requisitos previos

1. ESSL está instalado y su Interfaz web está activada.
2. Isilon OneFS está instalado.

Activación del servidor de ICAP en ESSL

En este ejemplo, el servidor de ICAP recibirá conexiones en la dirección IP 10.1.169.28 y en el puerto 1344.

1. Haga clic en **Configuración** > **Motor de detección** > **Análisis remoto** y active las opciones **Activar análisis remoto mediante el servicio ICAP** y **Compatibilidad con Dell EMC Isilon**.
2. Haga clic en **Editar** junto a **Direcciones y puertos de recepción de conexiones**.
3. Haga clic en **Agregar**.

4. Escriba la dirección IP y el puerto correspondientes. En nuestro ejemplo, la dirección IP es 10.1.168.28 y el puerto es 1344.

5. Haga clic en **Guardar**.

Activación del servidor de ICAP en OneFS

1. Inicie sesión en el panel de administración de OneFS, haga clic en **Protección de datos > Antivirus > Servidores de ICAP > Agregar un servidor de ICAP**.

2. Seleccione **Activar servidor de ICAP** e introduzca la dirección URL del servidor de ICAP en el campo **URL del servidor de ICAP** utilizando el siguiente patrón: `icap://<IP_ADDRESS>:<PORT>/scan`
En nuestro ejemplo: `icap://10.1.168.28:1344/scan`

3. Haga clic en **Agregar servidor**.

4. Haga clic en **Configuración** y seleccione **Activar servicio antivirus**.

5. Escriba en **Prefijos de la ruta** la ruta de acceso que desea analizar. Para analizar todas las rutas, escriba `/ifs` (sin comillas).

6. Haga clic en **Guardar cambios**.

Ajustes relacionados con el análisis en EMC Isilon

- [Restricciones de tamaño de archivo, nombre de archivo o extensión de archivo](#)
- [Análisis en el acceso](#) o [análisis a petición mediante política](#)
- [Configuración de amenaza a respuesta](#)

¿Cómo funciona?

Cuando se escribe un archivo (o se accede a él) en el clúster de EMC Isilon, OneFS agrega a la cola el archivo que se debe analizar y lo envía al servidor de ICAP configurado en OneFS y ESSL. ESSL analiza el archivo y envía a EMC Isilon comentarios sobre el archivo analizado. OneFS decide cómo gestionar los archivos analizados según la [configuración de respuesta a amenazas](#).

Prueba de la configuración

Para probar su configuración, debe tener acceso desde su ordenador al clúster de OneFS mediante uno de los protocolos compatibles. En nuestro ejemplo vamos a usar el protocolo NFS.

1. Configure NFS:

a. Inicie sesión en el panel de administración de OneFS y haga clic en **Protocolos > UNIX Sharing (NFS) > Crear un export**.

b. Mantenga la configuración predeterminada, compruebe que la ruta de acceso es `/ifs` y haga clic en **Guardar**.

2. Monte el recurso compartido NFS en su equipo Linux:

```
mkdir isilon
```

```
sudo mount -t nfs <IP address of OneFS cluster>:/ifs isilon
```

3. Realice un análisis de prueba:

a. Descargue el archivo de prueba de antivirus de eicar de la URL www.eicar.org, cópielo en el recurso compartido NFS de Isilon e intente leer su contenido.

```
wget www.eicar.org/download/eicar.com
```

```
cp eicar.com isilon
```

```
cat isilon/eicar.com
```

b. Según la configuración de su antivirus de OneFS, el resultado será denegar el permiso para ese archivo (predeterminado), o el archivo se truncará o eliminará. Por ejemplo:

```
cat: isilon/eicar.com: Permiso denegado
```

c. Para comprobar la amenaza detectada, inicie sesión en el panel de administración de OneFS y haga clic en **Protección de datos > Antivirus**.

Recuperación de la información de módulos

Utilice la utilidad `upd` con el parámetro `-l` en una ventana de terminal para mostrar todos los módulos y sus versiones.

```
/opt/eset/efs/bin/upd -l
```

Programación de análisis

ESET Server Security for Linux v8 tiene [tareas programadas](#) integradas para ejecutar análisis personalizados periódicos en días y horas definidos. Para configurar un análisis personalizado periódico sin [tareas programadas](#) integradas, siga las instrucciones que se indican a continuación.

En los sistemas basados en Unix, utilice **cron** para programar un análisis a petición en un periodo personalizado.

Para configurar una tarea programada, edite la tabla cron (crontab) desde una ventana de terminal.

Si es la primera vez que edita la tabla cron, se le ofrecerá la posibilidad de elegir un editor pulsando el número correspondiente. Seleccione un editor que conozca; por ejemplo, a continuación hacemos referencia al editor

Nano al guardar los cambios.

Programación de un análisis exhaustivo del disco completo todos los domingos a las 2 de la mañana

1. Para editar la tabla cron, ejecute el siguiente comando desde una ventana de terminal con un usuario con privilegios que disponga de acceso a las carpetas que desea analizar:

```
sudo crontab -e
```

2. Utilice las teclas de flecha para desplazarse debajo del texto en crontab y escriba el siguiente comando:

```
0 2 * * 0 /opt/eset/efs/bin/odscan --scan --profile="@In-depth scan" / &>/dev/null
```

3. Para guardar los cambios, pulse CTRL + X, escriba Y y pulse **Entrar**.

Programación de un análisis inteligente de una carpeta concreta todos los días a las 11 de la noche

En este ejemplo, programamos el sistema para analizar la carpeta `/var/www/download/` todas las noches.

1. Para editar la tabla cron, ejecute el siguiente comando desde una ventana de terminal con un usuario con privilegios que disponga de acceso a las carpetas que desea analizar:

```
sudo crontab -e
```

2. Utilice las teclas de flecha para desplazarse debajo del texto que se muestra en crontab y escriba el siguiente comando:

```
0 23 * * 0 /opt/eset/efs/bin/odscan --scan --profile="@Smart scan" /var/www/download/ &>/dev/null
```

3. Para guardar los cambios, pulse CTRL + X, escriba Y y pulse **Entrar**.

Estructura de archivos y carpetas

En este tema se detalla la estructura de archivos y carpetas de ESET Server Security for Linux, en caso de que el Soporte técnico de ESET le pida acceder a los archivos para resolver algún problema. A continuación se muestra la [lista de demonios y utilidades de línea de comandos](#).

Directorio base

El directorio en el que se almacenan los módulos cargables por ESET Server Security for Linux que contienen la base de firmas de virus.

/var/opt/eset/efs/lib

Directorio de caché

El directorio en el que se almacenan la caché y los archivos temporales (como informes o archivos de cuarentena) de ESET Server Security for Linux.

/var/opt/eset/efs/cache

Directorio de archivos binarios

El directorio en el que se almacenan los archivos binarios correspondientes de ESET Server Security for Linux.

/opt/eset/efs/bin

Aquí encontrará las siguientes utilidades:

- [lslog](#): utilícela para mostrar los registros recopilados por ESET Server Security for Linux.
- [odscan](#): utilícela para ejecutar un análisis a petición desde una ventana de terminal.
- [quar](#): utilícela para administrar elementos puestos en cuarentena.
- [upd](#): utilícela para administrar actualizaciones de módulos o para modificar la configuración de actualización.

Directorio de archivos binarios del sistema

El directorio en el que se almacenan los archivos binarios correspondientes del sistema ESET Server Security for Linux.

/opt/eset/efs/sbin

Aquí encontrará las siguientes utilidades:

- [cfg](#): utilícela para importar/exportar configuraciones de ESET Server Security for Linux.
- [cloud](#): utilícela para comprobar el estado de ESET Dynamic Threat Defense.
- [collect_logs.sh](#): utilícela para generar todos los registros esenciales como un archivo comprimido en la carpeta de inicio del usuario que ha iniciado sesión.
- [lic](#): utilícela para activar ESET Server Security for Linux con la clave de licencia adquirida o para comprobar el estado de activación y la validez de la licencia.
- [setgui](#): utilice esta opción para activar o desactivar la Interfaz web de ESET Server Security for Linux y gestionar las operaciones relacionadas.
- [startd](#): utilícela para iniciar el demonio de ESET Server Security for Linux de forma manual, en caso de que se haya detenido

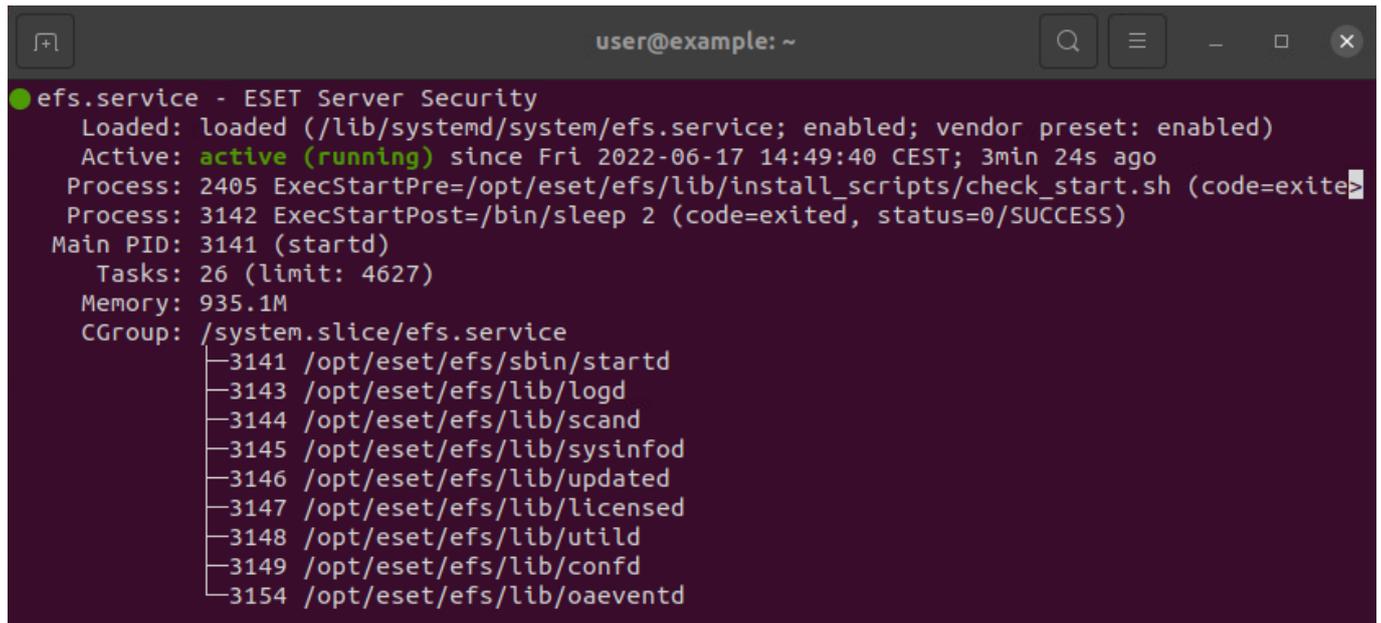
Si desea comprobar si el servicio ESET Server Security for Linux se encuentra activo, ejecute el siguiente comando desde una ventana de terminal con privilegios de usuario root:

```
systemctl status efs.service
```

o

```
/etc/init.d/efs status
```

Ejemplo de salida de systemctl:



```
user@example: ~
● efs.service - ESET Server Security
   Loaded: loaded (/lib/systemd/system/efs.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-06-17 14:49:40 CEST; 3min 24s ago
     Process: 2405 ExecStartPre=/opt/eset/efs/lib/install_scripts/check_start.sh (code=exite>
     Process: 3142 ExecStartPost=/bin/sleep 2 (code=exited, status=0/SUCCESS)
    Main PID: 3141 (startd)
       Tasks: 26 (limit: 4627)
      Memory: 935.1M
     CGroup: /system.slice/efs.service
            └─3141 /opt/eset/efs/sbin/startd
              └─3143 /opt/eset/efs/lib/logd
                └─3144 /opt/eset/efs/lib/scand
                  └─3145 /opt/eset/efs/lib/sysinfod
                    └─3146 /opt/eset/efs/lib/updated
                      └─3147 /opt/eset/efs/lib/licensed
                        └─3148 /opt/eset/efs/lib/utild
                          └─3149 /opt/eset/efs/lib/confd
                            └─3154 /opt/eset/efs/lib/oaeventd
```

Demonios

- sbin/startd: demonio principal, inicia y gestiona otros demonios.
- lib/scand: demonio de análisis.
- lib/oaeventd: servicio de intercepción de sucesos en el acceso (utiliza el módulo del kernel eset_rtp).
- lib/confd: servicio de administración de la configuración.
- lib/logd: servicio de administración de registros.
- lib/licensed: servicio de activación y licencias.
- lib/updated: servicio de actualización de módulos.
- lib/execd+odfeeder: asistentes del análisis a petición.
- lib/utild: servicio de utilidad.

- lib/syinfod: servicio de detección de SO y medios.
- lib/icapd: servicio ICAP para el análisis de NAS.
- lib/webd: servidor https e Interfaz web.

Utilidades de línea de comandos

- bin/[lslog](#): utilidad de enumeración de registros.
- bin/[odscan](#): análisis a petición.
- sbin/[cfg](#): utilidad de configuración.
- sbin/[lic](#): utilidad de licencias
- bin/[upd](#): utilidad de actualización de los módulos.
- bin/[guar](#): utilidad de administración de la cuarentena.
- sbin/[setgui](#): configuración básica de la Interfaz web.
- sbin/[collect_logs.sh](#): script para generar registros esenciales como un archivo comprimido si lo solicita el servicio de atención al cliente de ESET.

Resolución de problemas

En este apartado se describe cómo resolver los diversos problemas indicados a continuación.

- [Problemas de activación \(solo en inglés\)](#)
- [Contraseña olvidada](#)
- [Actualización fallida](#)
- [La actualización falla debido a una política de SELinux personalizada](#)
- [Uso del marcador noexec](#)
- [No se puede iniciar el demonio de la protección en tiempo real](#)
- [Recopilación de registros](#)

Recopilación de registros

Si el Soporte técnico de ESET le pide los archivos de registro de ESET Server Security for Linux, utilice el script `collect_logs.sh` disponible en `/opt/eset/efs/sbin/` para generarlos.

Ejecute el script desde una ventana de terminal con privilegios de usuario root. Por ejemplo, en Ubuntu, ejecute el siguiente comando:

```
sudo /opt/eset/efs/sbin/collect_logs.sh
```

El script genera todos los registros esenciales como un archivo comprimido en la carpeta de inicio del usuario que ha iniciado sesión y muestra la ruta de acceso al archivo. Envíe dicho archivo al Soporte técnico de ESET por correo electrónico.

Registros de activación

Para ayudarle a resolver problemas de activación del producto, el soporte técnico de ESET podría solicitar registros relacionados.

Para activar los registros de activación:

1. Detenga el servicio `efs`. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
sudo systemctl stop efs
```

2. Abra `/var/opt/eset/efs/licensed/license_cfg.json` para su edición. En el siguiente ejemplo se utiliza el editor `nano`. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
sudo nano -w /var/opt/eset/efs/licensed/license_cfg.json
```

3. Cambie `"Logging":false` por `"Logging":true`.
4. Para guardar los cambios, pulse `Ctrl+X`, escriba `Y` y pulse **Entrar**.
5. Inicie el servicio `efs`. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
sudo systemctl start efs
```

6. Vuelva a intentar el proceso de activación. Si falla, ejecute el script de recopilación de registros como un usuario con privilegios:

```
sudo /opt/eset/efs/sbin/collect_logs.sh
```

7. Repita los pasos n.º 1 y 2.
8. Cambie `"Logging":true` por `"Logging":false`.
9. Para guardar los cambios, pulse `Ctrl+X`, escriba `Y` y pulse **Entrar**.
10. Inicie el servicio `efs`. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
sudo systemctl start efs
```

Contraseña olvidada

Para restablecer la contraseña de la Interfaz web, abra una ventana de terminal en el equipo en el que está instalado ESET Server Security for Linux.

- Si desea generar una contraseña nueva, ejecute el siguiente comando con privilegios de usuario root:
`/opt/eset/efs/sbin/setgui -g`
- Si desea definir una contraseña nueva, ejecute el siguiente comando con privilegios de usuario root:
`/opt/eset/efs/sbin/setgui --password=PASSWORD`
donde PASSWORD se debe sustituir por la contraseña que desee.

En la salida final se mostrarán la dirección URL de la Interfaz web y las credenciales de acceso.

Actualización fallida

Si, por algún motivo, los módulos del producto no se actualizan, la información se mostrará en el Panel de control.

Intentos de actualización fallidos recientes: ESET Server Security for Linux no ha podido conectarse hace poco al servidor de actualizaciones para comprobar las actualizaciones de la firma de virus más recientes. Revise su conectividad de red y, a continuación, intente actualizar los módulos de nuevo; para ello, haga clic en **Comprobar y actualizar**.

Motor de detección obsoleto: hace tiempo que no se actualiza el Motor de detección. Compruebe la conectividad de red y, a continuación, intente actualizar los módulos de nuevo; para ello, haga clic en **Comprobar y actualizar**.

La actualización falla debido a políticas de SELinux personalizadas

Al intentar actualizar ESET Server Security for Linux (ESSL) en un [SO compatible](#) utilizando políticas de SELinux personalizadas se produce un error similar al siguiente:

```
Error: la política selinux eset_efs la usa otra política, intente quitarla con "semodule -r eset_efs".
```

```
El paquete no se actualizará.
```

A partir de ahora:

- Se ha quitado ESSL versión 8.1.685.0 (o inferior)
- ESSL 8.1.813 se conserva, pero se detiene. Para actualizar ESSL, continúe con los pasos indicados a continuación; de lo contrario, inicie el servicio `efs.service`.

Si intenta utilizar el comando `semodule -r eset_efs` sugerido para quitar la política `eset_efs`, se produce un fallo y se muestra un mensaje de error similar al siguiente:

```
libsemanage.semanage_direct_remove_key: quitando el último módulo eset_efs (no existe ningún otro módulo eset_efs con otra prioridad).
```

```
Error al resolver la declaración typeattributeset en /var/lib/selinux/targeted/tmp/modules/400/my-gdb/cil:2
```

```
semodule: ierror!
```

En nuestro ejemplo, primero debe quitarse la política personalizada `my-gdb`. Ejecute el siguiente comando en una ventana de terminal con un usuario con privilegios:

```
semodule -r my-gdb
```

La salida será:

```
libsemanage.semanage_direct_remove_key: quitando el último módulo my-gdb (no existe ningún otro módulo my-gdb con otra prioridad).
```

Quite la política `eset_efs` ejecutando el comando que se indica a continuación en una ventana de terminal con un usuario con privilegios:

```
semodule -r eset_efs
```

y ejecute el [instalador de ESSL](#) de nuevo para completar la actualización.

i La política `eset_efs` no se quita después de desinstalar ESSL
Tras desinstalar ESSL en el entorno mencionado anteriormente, la política `eset_efs` no se quita. Quítela manualmente como se indica anteriormente.

Uso del marcador noexec

Si tiene las rutas de acceso `/var` y `/tmp` montadas con el marcador `noexec`, la instalación de ESET Server Security for Linux falla con el siguiente mensaje de error:

```
Invalid value of environment variable MODMAPDIR. Modules cannot be loaded.
```

Solución

Los siguientes comandos se ejecutan en una ventana de terminal.

1. Cree una carpeta en la que `exec` esté activado con el siguiente propietario y conjunto de permisos:

```
/usr/lib/efs drwxrwxr-x. root eset-efs-daemons
```
2. Ejecute el siguiente comando:

```
# mkdir /usr/lib/efs
# chgrp eset-efs-daemons /usr/lib/efs
# chmod g+w /usr/lib/efs/
```

a.Si está activado SELinux, establezca el contexto para esta carpeta:

```
# semanage fcontext -a -t tmp_t /usr/lib/efs
# restorecon -v /usr/lib/efs
```

3. Compile los módulos esenciales:

```
# MODMAPDIR=/usr/lib/efs /opt/eset/efs/bin/upd --compile-nups
```

4. Configure MODMAPDIR en `/usr/lib/systemd/system/efs.service`; para ello, agregue una línea al bloque [Service]:

```
Environment=MODMAPDIR=/usr/lib/efs
```

5. Vuelva a cargar la configuración del servicio systemd:

```
# systemctl daemon-reload
```

6. Reinicie el servicio efs:

```
# systemctl restart efs
```

La protección en tiempo real no se puede iniciar

Problema

La protección en tiempo real no se puede iniciar porque faltan archivos del kernel o porque está activada la opción Arranque seguro.

En la pantalla **Sucesos** de la interfaz web de ESET Server Security for Linux (ESSL) versión 8 se muestra un mensaje de error.

TIME	COMPONENT	EVENT
November 30, 2020 3:47 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
November 30, 2020 3:47 PM	Real-time protection service	If you are running UEK kernel, make sure you have kernel-uek-devel installed
November 30, 2020 3:47 PM	Real-time protection service	Cannot open file /lib/modules/5.4.17-2036.100.6.1.el8uekx86_64/eset/efs/eset_rtp.ko: No such file or directory

Archivos del kernel que faltan

TIME	COMPONENT	EVENT
February 5, 2021 2:58 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
February 5, 2021 2:58 PM	Real-time protection service	Secure Boot is enabled. Please sign the kernel module /lib/modules/5.8.0-41-generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.

La opción Arranque seguro está activada

En los registros del sistema se muestra el mensaje de error correspondiente:

```
Nov 30 15:47:02 localhost.localdomain efs[373639]: ESET File Security error: cannot find kernel sources directory for kernel version 5.4.17-2036.100.6.1.el8uek.x86_64
Nov 30 15:47:02 localhost.localdomain efs[373641]: ESET File Security error: please check if kernel-devel (or linux-headers) package version matches the current kernel version
Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: Cannot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/efset/efs/eset_rtp.ko: No such file or directory
Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Warning: If you are running UEK kernel, make sure you have kernel-uek-devel installed
Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
```

Archivos del kernel que faltan

```
Feb 05 14:58:47 ubuntu2004 efs[52262]: ESET File Security Error: Secure Boot requires signed kernel modules. Please run "/opt/eset/efs/lib/install_scripts/sign_modules.sh" to sign our modules.
Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Secure Boot is enabled. Please sign the kernel module /lib/modules/5.8.0-41-generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.
Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
```

La opción Arranque seguro está activada

Solución

Si el equipo con la instalación de ESSL tiene la opción Arranque seguro activada, consulte la [sección Arranque seguro](#).

Método 1: requiere reiniciar el sistema operativo

1. Actualice los paquetes del sistema operativo a la versión más reciente. En CentOS 7, ejecute el siguiente comando desde una ventana de terminal con un usuario con privilegios:

```
yum upgrade
```

2. Reinicie el sistema operativo.

Método 2

1. Instale los módulos kernel-devel más recientes (en distribuciones Linux basadas en RPM) o los módulos linux-headers más recientes (en distribuciones Linux basadas en DEB). En Ubuntu Linux, ejecute el siguiente

comando desde una ventana de terminal o con un usuario con privilegios:

```
apt-get install linux-headers-`uname -r`
```

2. Reinicie el servicio de ESSL. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
systemctl restart efs
```

Método 3: sistema operativo con Unbreakable Enterprise Kernel

Si se utiliza [Unbreakable Enterprise Kernel](#), el paquete [kernel-uek-devel](#) se debe instalar manualmente.

1. En Oracle Linux, ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
yum install kernel-uek-devel-`uname -r` kernel-headers
```

2. Reinicie el servicio de ESSL. Ejecute el siguiente comando desde una ventana de terminal como usuario con privilegios:

```
systemctl restart efs
```

Desactivar protección en tiempo real al arrancar

Si la máquina protegida por ESET Server Security for Linux tarda en responder y la CPU está sobrecargada constantemente, puede desactivar la protección en tiempo real al arrancar para solucionar estos problemas.

1. Inicie el ordenador y espere a que aparezca el menú del GRUB.
2. Resalte el kernel que desea usar y pulse la tecla **e**.
3. Vaya a la línea que comienza con `linux` y agregue el parámetro `eset_rtp=0` al final de la línea.
4. Pulse CTRL + X para arrancar.

i NOTA

La modificación del GRUB puede ser ligeramente diferente en algunas distribuciones de Linux.

Glosario

- **Demonio:** un tipo de programa de los sistemas operativos basados en Unix que se ejecutan de forma no intrusiva en segundo plano, en lugar de bajo el control directo de un usuario, que espera que se den un suceso o una condición concretos para activarse.

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, 851 01 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 SUJECCIÓN 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, notifíquesele 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 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.. 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, 851 01 Bratislava, Slovak Republic.

21. Legislación aplicable. Este acuerdo se registrará 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

o 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;

o información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;

o información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;

o archivos 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