ESET Endpoint Antivirus for Linux

Manual de usuario

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

ESET Endpoint Antivirus for Linux está desarrollado por ESET, spol. s r.o.

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

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

REV. 12/04/2024

Introducción

El avanzado motor de análisis de ESET tiene una velocidad de análisis y tasas de detección inigualables combinadas con un pequeño tamaño, lo que convierte a ESET Endpoint Antivirus for Linux (EEAU) en la opción ideal para cualquier escritorio Linux que cumpla los requisitos del sistema.

El Análisis a petición y el Análisis en el acceso cubren la funcionalidad principal.

El Análisis a petición puede iniciarlo un usuario con privilegios (normalmente un administrador del sistema) mediante la interfaz de línea de comandos, ESET PROTECT 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 cuando se intenta acceder a objetos del sistema de archivos.

Principales funciones del sistema

- Análisis en el acceso mediante el módulo ligero de ESET, integrado en el kernel.
- Completos registros de análisis.
- Configuración rediseñada y fácil de usar
- Cuarentena
- Notificaciones en el escritorio
- Se puede administrar mediante ESET PROTECT.
- Protección en la nube

Requisitos del sistema

Requisitos de hardware

Requisitos mínimos de hardware que se deben cumplir antes del proceso de instalación para ejecutar ESET Endpoint Antivirus for Linux correctamente:

- Procesador Intel/AMD x64
- 700 MB de espacio libres en el disco duro

Requisitos de software

El software es compatible de forma oficial y se ha probado con los siguientes sistemas operativos de 64 bits:

- Ubuntu Desktop 18.04 LTS 64-bit

- Ubuntu Desktop 20.04 LTS
- Red Hat Enterprise Linux 7 u 8 con un entorno de escritorio compatible instalado.
- SUSE Linux Enterprise Desktop 15

> **Kernel AWS**
> No se admiten las distribuciones Linux con kernel AWS.

Servidores de visualización compatibles:

- X11
- Wayland

Entornos de escritorio compatibles:

- GNOME 3.28.2 y versiones posteriores
- KDE
- XFCE

Cualquier configuración regional con codificación UTF-8.

La interfaz de usuario y la lista de comandos de la ventana de terminal están disponibles en los siguientes idiomas:

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

Si el SO host utiliza un idioma no compatible, se utiliza inglés de forma predeterminada.

Administración remota mediante ESET PROTECT

ESET Endpoint Antivirus for Linux también es compatible con ESET PROTECT v7.1 y posteriores.

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 Endpoint Antivirus for Linux (EEAU) debe estar firmado con una clave privada. La clave pública correspondiente debe importarse en UEFI. EEAU versión 8.1 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/eea/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.

Syntax: `/opt/eset/eea/lib/install_scripts/sign_modules.sh [OPTIONS]`

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/eea/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 EEAU 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 Endpoint Antivirus for Linux en el equipo de destino para actualizar la tabla de módulos.

Ejecute el siguiente comando como usuario con privilegios:

```
systemctl restart eea
```

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

Instalación

ESET Endpoint Antivirus for Linux se distribuye como un archivo binario (`.bin`).

> **Actualizar su sistema operativo**
> Antes de instalar ESET Endpoint Antivirus for Linux, asegúrese de que tiene instaladas las actualizaciones más recientes del sistema operativo.

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:

- `./eeau.x86_64.bin`
- `sh ./eeau.x86_64.bin`

Para mostrar los parámetros (argumentos) disponibles del archivo binario de ESET Endpoint Antivirus for Linux, ejecute el siguiente comando desde una ventana de terminal:
`./eeau.x86_64.bin -h`

Parámetros disponibles

Forma abreviada	Forma completa	Descripción
`-h`	`--help`	Mostrar los 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
`-u`	`--unpack-ertp-sources`	Desempaquetar fuentes del "Módulo de kernel de protección del sistema de archivos en tiempo real de ESET", no realizar instalación

> **Obtener el paquete de instalación .deb**
> Para obtener el paquete de instalación `.deb` adecuado para su sistema operativo, ejecute el script de distribución de ESET con el argumento de la línea de comandos "`-n`":
> `sudo ./eeau.x86_64.bin -n`
> o
> `sudo sh ./eeau.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 que aparecen en la pantalla. Acepte el acuerdo de licencia del producto para completar la instalación.

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

Instalación con ESET PROTECT

Si desea implementar ESET Endpoint Antivirus 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 Endpoint Antivirus for Linux.

> **Aplicaciones de terceros**
> Puede consultar un resumen de las aplicaciones de terceros que usa ESET Endpoint Antivirus for Linux en el archivo `NOTICE_mode` almacenado en `/opt/eset/eea/doc/modules_notice/`.

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 remove eea`

Distribuciones basadas en Red Hat:

- `yum remove eea`
- `rpm -e eea`

Implementación en bloque

En este tema se presenta una descripción general de alto nivel de la implementación en bloque de ESET Endpoint Antivirus 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 Endpoint Antivirus for Linux, tiene que decidir qué paquete desea usar. ESET Endpoint Antivirus 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/eea-8.0.1081.0.x86_64.bin":
           mode => "0700",
           owner => "root",
           group => "root",
           source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.bin"
         }
    exec {"Execute bin package installation":
           command => '/tmp/eea-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/eea-8.0.1081.0.x86_64.deb":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.deb"
             }
        package {"eea":
               ensure => "installed",
               provider => 'dpkg',
               source => "/tmp/eea-8.0.1081.0.x86_64.deb"
             }
}
if $osfamily == 'RedHat' {
        file {"/tmp/eea-8.0.1081.0.x86_64.rpm":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.rpm"
             }
        package {"eea":
               ensure => "installed",
               provider => 'rpm',
               source => "/tmp/eea-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/eea-8.0.1084.0.x86_64.bin' do
        source 'eea-8.0.1084.0.x86_64.bin'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
end

execute 'package_install' do
        command '/tmp/eea-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/eea-8.0.1084.0.x86_64.deb' do
        source 'eea-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/eea-8.0.1084.0.x86_64.rpm' do
                source 'eea-8.0.1084.0.x86_64.rpm'
                owner 'root'
                group 'root'
                mode '0700'
                action :create
                only_if { node['platform_family'] == 'rhel'}

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

rpm_package 'eea' do
        source '/tmp/eea-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: eea-8.0.1084.0.x86_64.bin
    dest: /home/ansible/

- name : "Install product bin package"
  shell: bash ./eea-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: ./eea-8.0.1085.0.x86_64.deb
          dest: /home/ansible/eea-8.0.1085.0.x86_64.deb
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "Debian"

      - name: "Copy rom package to VM"
        copy:
          src: ./eea-8.0.1085.0.x86_64.rpm
          dest: /home/ansible/eea-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/eea-8.0.1085.0.x86_64.deb
          state: present
        when:
          - ansible_os_family == "Debian"

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

Actualización

Acceso rápido a la actualización

Actualización de los módulos

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

Para iniciar manualmente la actualización del módulo de detección, ejecute el comando de actualización en una ventana de terminal o actualice mediante ESET PROTECT.

Si una actualización de ESET Endpoint Antivirus for Linux no resulta estable, revierta las actualizaciones de módulos a un estado anterior. Ejecute el comando adecuado en una ventana de terminal o revierta usando ESET PROTECT.

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

```
/opt/eset/eea/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
`-l`	`--list-modules`	Mostrar versión de los módulos usados
`-r`	`--rollback=VALUE`	Volver a la instantánea más antigua del módulo de análisis y bloquear todas las actualizaciones durante las horas indicadas en `VALOR`

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

EJEMPLO

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/eea/bin/upd --update --rollback=48
```

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

```
sudo /opt/eset/eea/bin/upd --update --cancel
```

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/eea/bin/upd --update --server=192.168.1.2:2221
```

Actualice ESET Endpoint Antivirus para Linux (EEAU) a una versión posterior

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

¿Qué versión del producto está instalada?

Tiene dos formas de saber la versión de EEAU que tiene instalada:

1. Ejecute /opt/eset/eea/lib/egui -v en una ventana de terminal.
2. Consulte ESET PROTECT (antes ESET PROTECT) en la sección Ordenadores.

Cómo actualizar

Para actualizar a una versión más reciente, ejecute un paquete de instalación del sistema operativo correspondiente, como se describe en el apartado Instalación.

Si administra ESET Endpoint Antivirus for Linux mediante ESET PROTECT , puede iniciar la actualización mediante la tarea Instalación de software o desde **Panel de control** > **Aplicaciones de ESET** > clic con el botón derecho en ESET Endpoint Antivirus for Linux > **Actualizar productos de ESET instalados**.

> **No es posible la actualización directa desde ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.**
> ESET Endpoint Antivirus for Linux es un producto totalmente nuevo y su configuración no es compatible con la configuración de ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.

Para actualizar de ESET NOD32 Antivirus 4 Business Edition for Linux Desktop a ESET Endpoint Antivirus for Linux, siga las instrucciones que se indican a continuación.

Entorno administrado de forma remota (ESET PROTECT)

Si gestiona ESET NOD32 Antivirus 4 Business Edition for Linux Desktop de forma remota, ESET PROTECT no le avisará de la actualización disponible.

1. Ejecute la tarea Desinstalación de software en las instalaciones existentes de ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.

2. Implemente ESET Endpoint Antivirus for Linux de forma remota en sus ordenadores con la tarea Instalación de software.

Entorno administrado personalmente

Si intenta instalar ESET Endpoint Antivirus for Linux antes de quitar ESET NOD32 Antivirus 4 Business Edition for Linux Desktop, la instalación falla con el siguiente mensaje:

```
"Error: Antes debe desinstalar el producto de seguridad de ESET anterior, el paquete no se instalará."
```

1. Desinstale ESET NOD32 Antivirus 4 Business Edition for Linux Desktop con el instalador descargado.

   i. Haga clic con el botón derecho del ratón en el archivo del instalador descargado (`eset_nod32av_64bit_<languge_code>.linux`), haga clic en la ficha **Propiedades** > **Permisos**, marque la opción **Permitir la ejecución de archivos como programa** y cierre la ventana.

   ii. Haga doble clic en el instalador para iniciar el **programa de instalación de ESET NOD32 Antivirus**.

   iii. Haga clic en **Siguiente**, seleccione **Desinstalar ESET NOD32 Antivirus del ordenador** y haga clic en **siguiente**.

   iv. En el cuadro de lista **Seleccione una de las opciones**, seleccione **Ninguna de las opciones mencionadas**.

   v. Escriba "*Actualizar a ESET Endpoint Antivirus for Linux*" en **Otros datos adicionales**, haga clic en **Siguiente** y, a continuación, en **Desinstalar**.

vi. Haga clic en **Finalizar** cuando termine y, a continuación, haga clic en **Sí** para reiniciar el ordenador.

2. Instale ESET Endpoint Antivirus for Linux.

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 Endpoint Antivirus for Linux para usar un mirror de actualización

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 Endpoint for Linux (V7+)** en el menú desplegable.

3. Haga clic en **Actualización** > **Servidor principal**.

4. En el apartado **Básico**, desactive el interruptor situado junto a **Elegir automáticamente**.

5. Escriba en el campo **Servidor de actualizaciones** la dirección URL del servidor Mirror en uno de los siguientes formatos:

   - `http://<IP>:<port>`
   - `http://<hostname>:<port>`

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

7. Haga clic en **Continuar** > **Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.

8. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

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

Activación de ESET Endpoint Antivirus for Linux

Active su ESET Endpoint Antivirus for Linux con una licencia adquirida a su distribuidor de ESET.

Activación desde una ventana de terminal

Use la utilidad `/opt/eset/eea/sbin/lic` con un usuario con privilegios para activar ESET Endpoint Antivirus

for Linux desde una ventana de terminal.

Sintaxis: `/opt/eset/eea/sbin/lic [OPTIONS]`

EJEMPLOS

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

Activación con una clave de licencia

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

o

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

donde XXXX-XXXX-XXXX-XXXX-XXXX representa su clave de licencia de ESET Endpoint Antivirus for Linux.

Activación con nombre de usuario y contraseña

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

```
/opt/eset/eea/sbin/lic -u <username> -p <public_id>
```

se pedirá al usuario que introduzca la contraseña. `public_id` representa el identificador público de la licencia.

Si el nombre de usuario, la contraseña y el ID público de la licencia están guardados en el archivo `password.txt`, ejecute lo siguiente como un usuario con privilegios:

```
cat password.txt | /opt/eset/eea/sbin/lic -u <nombre de usuario> -p <public_id> --stdin-pass
```

Activación con un archivo de licencia sin conexión

```
/opt/eset/eea/sbin/lic -f offline_license.lf
```

o

```
/opt/eset/eea/sbin/lic -FILE=offline_license.lf
```

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.

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:

https://eba.eset.com/LicenseConverter

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:

Sintaxis: `/opt/eset/eea/sbin/lic [OPTIONS]`

Los comandos indicados a continuación debe ejecutarlos un usuario con privilegios:
`/opt/eset/eea/sbin/lic -s`
o
`/opt/eset/eea/sbin/lic --status`

Ejemplo de 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 Endpoint Antivirus 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:

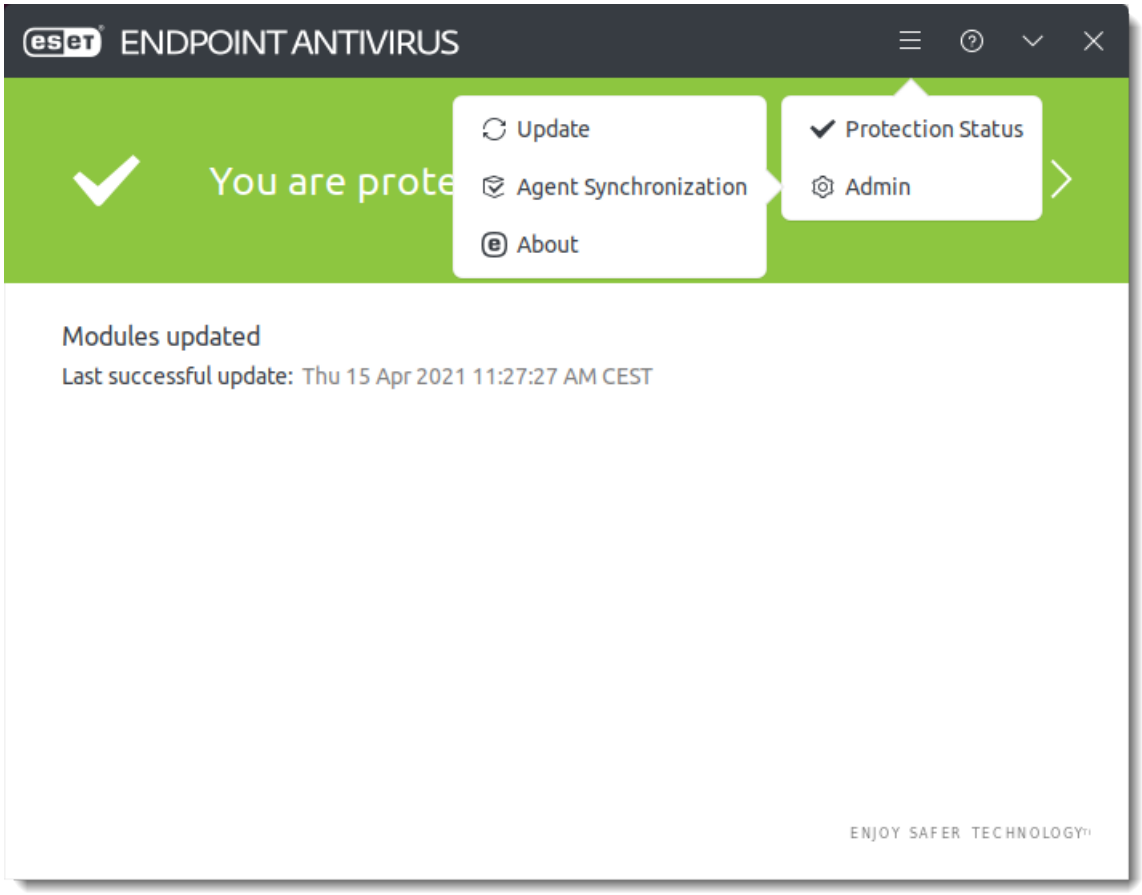
```
/opt/eset/efs/sbin/lic -s --with-details
```

Si se utiliza ESET Endpoint Antivirus for Linux

Si la instalación ha concluido, utilice una ventana de terminal o ESET PROTECT para ejecutar ESET Endpoint Antivirus for Linux.

Interfaz de usuario

ESET Endpoint Antivirus for Linux introduce una interfaz gráfica de usuario minimalista.



La pantalla de inicio ofrece un resumen del estado de la protección, las alertas y las notificaciones.

Si va a cualquier pantalla con el menú, haga clic en el botón Atrás para volver a la pantalla de inicio.

Estado de la protección

Cuando todo funciona sin problemas, el estado de la protección general (pantalla de inicio) es verde. Si hay opciones para mejorar el estado de la protección del sistema o se detecta un estado de la protección insuficiente, el color se vuelve rojo.

Para ver información más detallada sobre el estado de la protección, haga clic en el icono de menú > **Estado de la protección**.

Actualización

Para invocar manualmente actualizaciones de módulos, haga clic en el icono de menú > **Admin** > **Actualización**. En la pantalla se muestran la actualización correcta más reciente y la búsqueda de actualizaciones más reciente.

Módulos instalados

Hay dos formas de ver los módulos instalados:

1. Haga clic en el icono de menú > **Admin** > **Actualización** > **Mostrar todos los módulos**.
2. Haga clic en el icono de menú > **Admin** > **Acerca de** > **Mostrar todo**.

Sincronización del agente

Si administra ESET Endpoint Antivirus for Linux de forma remota, puede ver algunos detalles del agente de administración en el menú ☰ > **Admin** > **Sincronización del agente**.

Entre esos detalles se incluyen:

- Versión actual: versión del agente de administración remota instalado actualmente
- Última replicación: representa el último intento de sincronización entre el agente de administración remota y ESET PROTECT
- Última replicación correcta
- Último registro de estado generado: la última vez que el agente de administración generó un registro de estado. El archivo de registro está disponible en `/var/log/eset/RemoteAdministrator/Agent/status.html`

Acerca de

La pantalla **Acerca** de proporciona detalles acerca de la versión instalada de ESET Endpoint Antivirus for Linux, su sistema operativo y los recursos del sistema.

Haga clic en **Mostrar todo** para ver información acerca de la lista de módulos del programa instalados.

Escaneos

Vínculo rápido: Perfiles de análisis

Ejecución de un análisis a petición desde una ventana de terminal

Sintaxis: `/opt/eset/eea/bin/odscan [OPTIONS]`

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

Opciones: forma abreviada	Opciones: forma completa	Descripción
	`--profile-priority=PRIORITY`	La tarea se ejecutará con la prioridad especificada. La prioridad puede ser `normal`, `menor`, `más baja`, `inactividad`.
	`--readonly`	Analizar sin desinfectar
	`--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

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/eea/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/eea/bin/odscan --scan --profile="@Smart scan" /root/* /tmp/* /home/*
```

Enumerar todos los análisis en ejecución:

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

Códigos de salida

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	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

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.

Crear un perfil nuevo mediante 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 Endpoint for Linux (V7+)** en el menú desplegable.

3. Haga clic en **Análisis de malware > Análisis a petición** y haga clic en **Editar** junto a **Lista de perfiles**.

4. Introduzca el nombre deseado del nuevo perfil, haga clic en **Agregar** y luego en **Guardar**.

5. En el menú desplegable **Perfil seleccionado**, seleccione el nuevo perfil que ha creado y ajuste la configuración relacionada con el análisis en la sección **Análisis de malware**.

6. Diríjase a **Asignar**, haga clic en **Asignar** y seleccione el grupo deseado de ordenadores al que se aplicará la política.

7. Haga clic en **Aceptar** y luego en **Terminar**.

Exclusiones

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 ESET PROTECT, haga clic en **Políticas** > **Nueva política** y escriba un nombre para la política.
2. Haga clic en **Configuración** y seleccione **ESET Endpoint for Linux (V7+)** en el menú desplegable.
3. Diríjase a **Motor de detección** > **Básico** y haga clic en **Editar** junto a **Exclusiones de rendimiento**.
4. 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.
5. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
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**.

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.

Exclusiones de extensiones de archivo

Este tipo de exclusión se puede configurar para la **Protección del sistema de archivos en tiempo real**, el **Análisis a petición**.

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 Endpoint for Linux (V7+)** en el menú desplegable.
1. Diríjase al archivo:

- **Protección del sistema de archivos en tiempo real** > **Parámetros de ThreatSense**
- **Análisis de malware** > **Análisis a petición** > **Parámetros de ThreatSense**

2. Haga clic en **Editar** junto a **Extensiones de archivo excluidas del análisis**.

3. 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 que desee separadas por una línea nueva u otro separador que elija.

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

5. Haga clic en **Continuar** > **Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.

6. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

Cuarentena

La función principal de la cuarentena es almacenar de forma segura los archivos infectados. Los archivos deben ponerse en cuarentena si no se pueden desinfectar, si no es seguro o recomendable eliminarlos o si ESET Endpoint Antivirus for Linux los detecta como falsos positivos. Puede poner en cuarentena cualquier archivo, sobre todo si se comporta de forma sospechosa, pero el análisis antivirus no lo detecta.

Ruta de acceso al directorio de cuarentena: */var/opt/eset/eea/cache/quarantine/*

El directorio de cuarentena se crea la primera vez que hay un elemento que se debe poner en cuarentena.

Administrar elementos puestos en cuarentena desde una ventana de terminal

Sintaxis: `/opt/eset/eea/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`	Ruta en la que restaurar un elemento puesto en cuarentena
`-h`	`--help`	Mostrar ayuda y salir.
`-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/eea/bin/quar -d 0123456789
```

o

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

o

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

Restaurar un elemento puesto en cuarentena con el id "123456789" marcado con una "**x**" en la columna **excluible** en la carpeta *Descargas*:

```
/opt/eset/eea/bin/quar -e 9876543210 --restore-path=/home/$USER/Download/
```

o

```
/opt/eset/eea/bin/quar --restore-exclude=9876543210 --restore-
path=/home/$USER/Download/
```

Restaurar archivos puestos en cuarentena desde una ventana de terminal

1. Enumerar elementos puestos en cuarentena
   `/opt/eset/eea/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/eea/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-path=/final/path/of/restored/file`

Sucesos

Los comandos de ESET Endpoint Antivirus for Linux (EEAU) ejecutados mediante el terminal y algunos sucesos más se registran con EEAU.

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

Para mostrar los **Sucesos** registrados mediante una ventana de terminal, utilice la herramienta de línea de comandos `lslog` como usuario con privilegios.

Sintaxis: `/opt/eset/eea/sbin/lslog [OPTIONS]`

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
`-l`	`--device-control`	Mostrar registros de Control de dispositivos
`-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/eea/sbin/lslog -e
```

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

```
/opt/eset/eea/sbin/lslog -ec > /home/$USER/Documents/eventlogs.csv
```

Mostrar todas las amenazas detectadas y las acciones realizadas contra:

```
/opt/eset/eea/sbin/lslog -d
```

Notificaciones

EEAU muestra varias notificaciones para informarle sobre una actividad o una acción necesaria. Algunas de las notificaciones pueden activarse o desactivarse.

Las notificaciones están relacionadas con:

- Análisis a petición: por ejemplo, se ha iniciado o completado el análisis de un dispositivo extraíble.
- Control de dispositivos: un dispositivo se ha bloqueado o no se permite la escritura de datos en dicho dispositivo.
- Detecciones: por ejemplo, se ha encontrado o eliminado una amenaza, o se ha desinfectado un archivo.
- Sistema operativo: es necesario reiniciar el sistema o está programado un apagado.
- EDTD desde la versión 8.1 de EEAU: por ejemplo, se está analizando un archivo y, por lo tanto, no se puede abrir temporalmente.

Configuración

Para modificar la configuración de ESET Endpoint Antivirus 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 Endpoint 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 **Aceptar** y, a continuación, en **Terminar**.

> **Ajuste de la configuración de la política existente**
> Para ajustar la configuración de la política de ESET Endpoint Antivirus for Linux, haga clic en la política que desee cambiar en la lista de políticas y haga clic en **Editar**.

Puede ajustar el comportamiento de detección y modificar la configuración de conexión y actualización del producto.

Si ha configurado ESET Endpoint Antivirus for Linux según sus necesidades y desea guardar la configuración para usarla posteriormente (o para utilizarla con otra instancia de ESET Endpoint Antivirus 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/eea/lib/cfg --export-xml=/tmp/export.xml
```

Importación de la configuración

```
/opt/eset/eea/lib/cfg --import-xml=/tmp/export.xml
```

Opciones disponibles

Forma abreviada	Forma completa	Descripción
`-i`	`--json-rpc`	list of json-rpc files
	`--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, uso ESET PROTECT:

Para modificar la configuración de ESET Endpoint Antivirus 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 Endpoint 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 **Aceptar** y, a continuación, en **Terminar**.

> **Ajuste de la configuración de la política existente**
> Para ajustar la configuración de la política de ESET Endpoint Antivirus for Linux, haga clic en la política que desee cambiar en la lista de políticas y haga clic en **Editar**.

- 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.
- Active la caché local compartida.

Para mostrar todas las amenazas detectadas y las acciones realizadas contra ellas, utilice la utilidad lslog con el parámetro --detections.

Exclusiones

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 ESET PROTECT, haga clic en **Políticas** > **Nueva política** y escriba un nombre para la política.
2. Haga clic en **Configuración** y seleccione **ESET Endpoint for Linux (V7+)** en el menú desplegable.
3. Diríjase a **Motor de detección** > **Básico** y haga clic en **Editar** junto a **Exclusiones de rendimiento**.
4. 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.
5. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
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**.

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.

Exclusiones de extensiones de archivo

Este tipo de exclusión se puede configurar para la **Protección del sistema de archivos en tiempo real**, el **Análisis a petición**.

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 Endpoint for Linux (V7+)** en el menú desplegable.
1. Diríjase al archivo:

- **Protección del sistema de archivos en tiempo real** > **Parámetros de ThreatSense**
- **Análisis de malware** > **Análisis a petición** > **Parámetros de ThreatSense**

2. Haga clic en **Editar** junto a **Extensiones de archivo excluidas del análisis**.
3. 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 que desee separadas por una línea nueva u otro separador que elija.
4. Haga clic en **Aceptar** y, a continuación, haga clic en **Guardar** para cerrar el cuadro de diálogo.
5. Haga clic en **Continuar** > **Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.
6. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

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.

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.

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

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 Endpoint for Linux (V7+)** en el menú desplegable.
3. Haga clic en **Configuración > Motor de detección > Protección del sistema de archivos en tiempo real > Básico**.

4. Desactive **Activar la protección del sistema de archivos en tiempo real**.

5. Haga clic en **Continuar** > **Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.

6. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

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 al conectarse 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, usar 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 Endpoint for Linux (V7+)** en el menú desplegable.

3. Haga clic en **Motor de detección > Protección del sistema de archivos en tiempo real** > **Parámetros de ThreatSense**.

4. Active o desactive **Activar optimización inteligente**.

5. Haga clic en **Continuar** > **Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.

6. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

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:

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

Utilice ESET PROTECT para modificar la configuración. 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**: una heurística en un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la identificación de software malicioso que no existía o no estaba cubierto en la anterior base de datos de firmas de virus. La desventaja es una (pequeña) probabilidad 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 más 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 ThreatSense de los módulos donde se realiza 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.

Al implementar ESET Endpoint Antivirus for Linux de forma remota mediante ESET PROTECT, puede configurar una de las siguientes opciones en relación con la protección en la nube:

- La activación de ESET LiveGrid® no es obligatoria. El software no perderá funcionalidad, pero puede que ESET Endpoint Antivirus for Linux responda más lento a las nuevas amenazas que la actualización de la base de datos del motor de detección.
- Puede configurar ESET LiveGrid® para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso detectado. Este archivo se puede enviar a ESET para que realice un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar sus funciones de detección de amenazas.

De forma predeterminada, ESET Endpoint Antivirus for Linux 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.

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.

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 archivos ejecutables, como *.exe*, *.dll*, *.sys*.
- Archivos comprimidos: incluye tipos de archivo comprimidos, como *.zip*, *.rar*, *.7z*, *.arch*, *.arj*, *.bzip2*, *.gzip*, *.ace*, *.arc*, *.cab*.
- Scripts: incluye tipos de archivo de script, como *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.ps1*.
- Otros: incluye tipos de archivo como *.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 Endpoint Antivirus for Linux versión 8.1 o posterior se administra de forma remota.
> 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 acompaña del mensaje "Operación no permitida" o de un mensaje similar.

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

```
/opt/eset/eea/lib/cloud -e
o

/opt/eset/eea/lib/cloud --edtd-status
```

Para activar el servicio en EEAU:

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 Endpoint for Linux (V7+)** en el menú desplegable.
3. **Motor de detección** > **Protección en la nube**.
4. Active **Activar el sistema de respuesta ESET LiveGrid®, 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 deseado de ordenadores al que se aplica 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.

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 Endpoint Antivirus 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.

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 Endpoint Antivirus for Linux no resulta estable, revierta las actualizaciones de módulos a un estado anterior. Ejecute el comando adecuado en una ventana de terminal o revierta usando ESET PROTECT.

Puede definir dos fuentes de actualización alternativas, un servidor principal y uno secundario.

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 Endpoint Antivirus for Linux (EEAU) no actualiza los componentes del producto automáticamente.

Active las actualizaciones automáticas:

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 Endpoint for Linux (V7+)** en el menú desplegable.

3. Seleccione **Actualizar automáticamente** en el cuadro de lista **Modo de actualización**.

4. Haga clic en **Continuar** > **Asignar** y seleccione el grupo de ordenadores deseado al que se aplicará la política.

5. Haga clic en **Aceptar** y, a continuación, en **Terminar**.

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 EEAU 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.

Control del dispositivo

ESET Endpoint Antivirus for Linux proporciona el control automático de dispositivos (CD, DVD, USB, etc.). Este módulo le permite bloquear o ajustar los filtros y permisos ampliados, así como definir la capacidad de un usuario para acceder a un dispositivo dado y trabajar en él. Esta opción resulta útil cuando el administrador del ordenador quiere impedir el uso de dispositivos que contienen contenido no solicitado.

Posible daño en el sistema de archivos
La aplicación de una política con acción de bloquear o de solo lectura en dispositivos ya conectados mientras hay en curso una escritura o lectura de datos puede dañar su sistema de archivos, ya que el desmontaje se fuerza.

Sustituir política
Si se aplican en una instancia de EEAU varias políticas de reglas de control de dispositivos, la última política aplicada sustituye las reglas de las políticas anteriores.

Dispositivos externos admitidos:

- Dispositivos de almacenamiento conectados por USB
- Unidades de CD/DVD internas

El Cde dispositivos puede activarse y configurarse en ESET PROTECT desde la sección Políticas.

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 Endpoint for Linux (V7+)** en el menú desplegable.

3. Desplácese hasta **Control de dispositivos**.

4. Haga clic en el conmutador situado junto a **Integrar en el sistema**.

5. Para configurar Reglas y Grupos, haga clic en **Modificar** junto al elemento correspondiente.

6. Desplácese hasta **Asignar**, haga clic en **Asignar** y seleccione el grupo de ordenadores que desee.

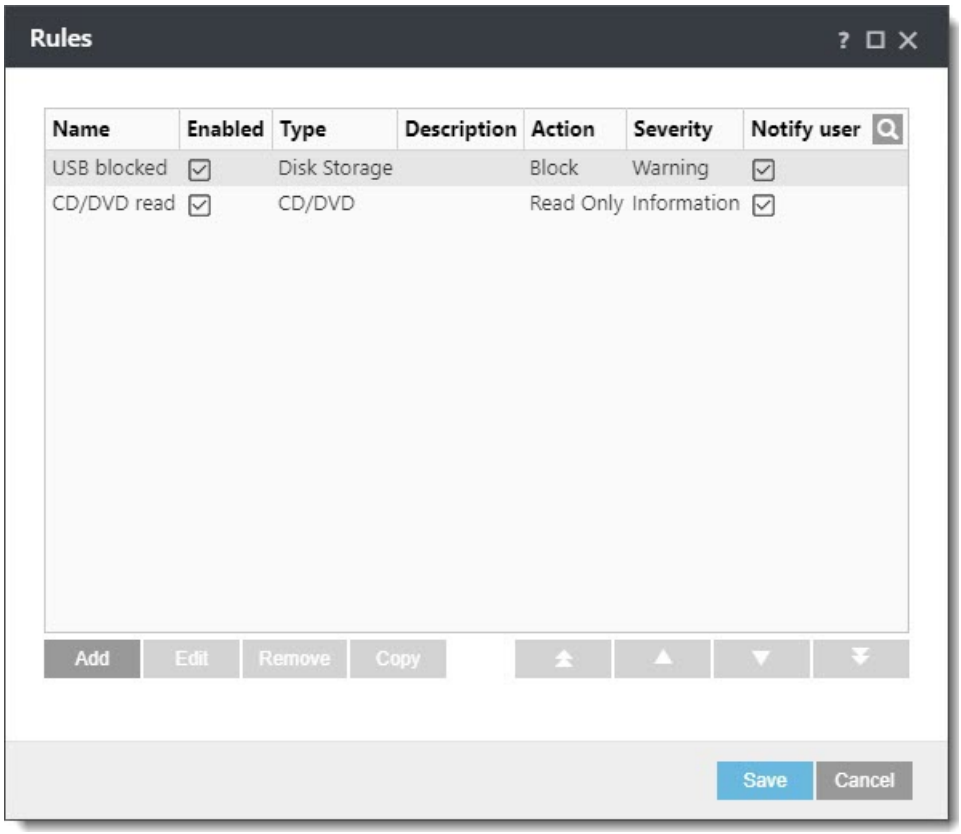
7. Haga clic en **Aceptar** y, a continuación, en **Finalizar**.

Consulte más información sobre la administración de productos de seguridad para equipos desde ESET PROTECT.

Si se conecta/inserta un dispositivo que está bloqueado por una regla existente, se mostrará una ventana de notificación y no se concederá el acceso al dispositivo.

Editor de reglas de control de dispositivos

En la ventana del **Editor de reglas de control de dispositivos** de ESET PROTECT se muestran las reglas existentes y se permite un control preciso de los dispositivos externos compatibles que los usuarios conectan al ordenador.



Se pueden permitir o bloquear dispositivos concretos en función de los parámetros definidos en la configuración de las reglas. La lista de reglas contiene varias descripciones de regla como el nombre, el tipo de dispositivo externo y la acción que debe realizarse tras conectar un dispositivo externo al ordenador.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Desactive la casilla **Activado** que aparece junto a la regla para desactivarla hasta que la quiera usar en el futuro. Seleccione una o más reglas y haga clic en **Eliminar**

para eliminar las reglas de forma permanente.

Haga clic en **Copiar** para crear una copia de la regla seleccionada.

Las reglas se muestran en orden de prioridad, con las reglas que tienen más prioridad más arriba en la lista. Para mover las reglas individualmente o en grupos, haga clic en los botones Superior/Arriba/Abajo/Inferior  .

El Registro de control de dispositivos anota todas las ocasiones en las que se activa el Control de dispositivos.

Atributos de los dispositivos conectados

Para ver una lista de los atributos de los dispositivos conectados al ordenador en el que ESET Endpoint Antivirus for Linux está instalado, utilice la utilidad `lsdev` en una ventana del terminal o ejecútelo desde ESET PROTECT.

Sintaxis: `/opt/eset/eea/bin/lsdev [OPTIONS]`

Opciones: forma abreviada	Opciones: forma completa	Descripción
`-l`	`--list`	Mostrar una lista de dispositivos conectados
`-c`	`--csv`	Usar formato CSV para ver una lista de dispositivos conectados
`-h`	`--help`	Mostrar ayuda y salir
`-v`	`--version`	Mostrar información sobre la versión y salir

Grupos de dispositivos

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo correspondiente, mientras que la parte izquierda contiene los grupos creados. Seleccione el grupo que contiene la lista de dispositivos que quiere ver en el panel de la derecha.

Cuando abra la ventana **Grupos de dispositivos** y seleccione un grupo, podrá agregar o quitar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo.

Elementos de control

Agregar: agregue un grupo escribiendo su nombre o un dispositivo al grupo existente (también puede especificar detalles como el nombre del proveedor, el modelo y el número de serie).

Modificar: modifique el nombre de un grupo seleccionado o los parámetros del dispositivo (proveedor, modelo, número de serie).

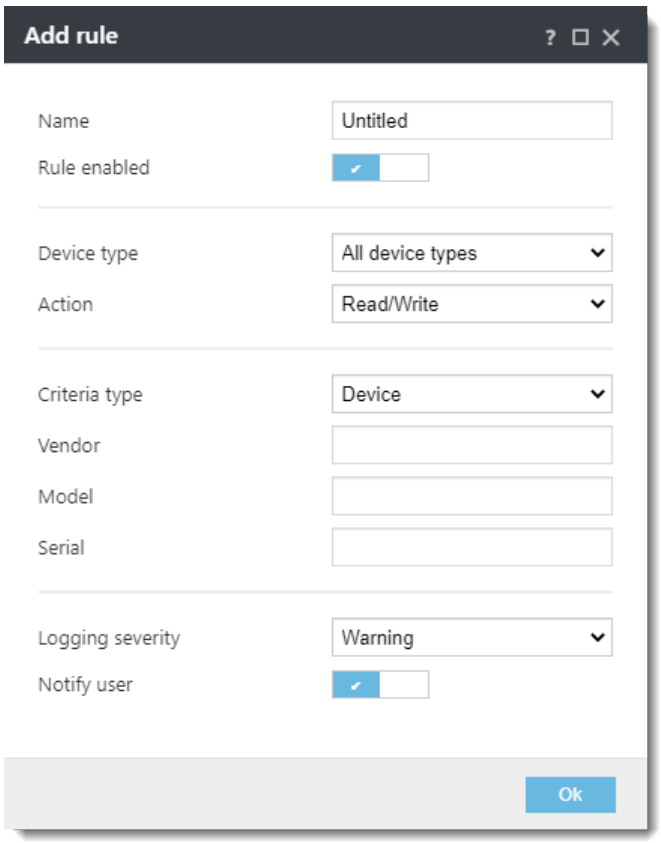
Eliminar: elimina el grupo o el dispositivo seleccionados.

Importar: importa una lista de dispositivos desde un archivo.

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** si desea cerrar la ventana **Grupos de dispositivos** sin guardar los cambios.

Adición de reglas de control de dispositivos

Una regla de control de dispositivos define la acción que se realiza cuando un dispositivo que cumple los criterios de la regla se conecta al ordenador.



Introduzca una descripción de la regla en el campo **Nombre** para facilitar la identificación. Haga clic en el conmutador situado junto a **Regla activada** para activar o desactivar esta regla, lo cual puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable:

- **Almacenamiento en disco** : se aplica a cualquier almacenamiento en disco conectado por USB, incluyendo unidades de CD/DVD externas y lectores de tarjetas de memoria convencionales.
- **CD/DVD** : se aplica a una unidad de CD/DVD interna conectada por IDE o SATA.
- **Todos los dispositivos** : incluye todos los tipos anteriores.

La información del tipo de dispositivo se recopila del sistema operativo. Utilice la utilidad lsdev para ver una lista de los dispositivos conectados y sus atributos.

Dado que estos dispositivos solo ofrecen información sobre sus acciones y no proporcionan información sobre los usuarios, solo se pueden bloquear de forma global.

Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/escritura**: acceso completo al dispositivo.
- **Bloquear**: el acceso al dispositivo está bloqueado.
- **Solo lectura**: acceso de solo lectura al dispositivo.

En **Tipo de criterios**, seleccione **Dispositivo** o **Grupo de dispositivos**.

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas y adaptarlas a dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas:

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

> **Parámetros sin definir**
> Si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).

> **Registro de control de dispositivo**
> Si desea ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo con la utilidad de línea de comandos lslog con el parámetro `-l` o `--device-control`.

Nivel de registro

- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta y los envía a ESET PROTECT.

Herramientas

En la sección **Herramientas** de la configuración de ESET Endpoint Antivirus for Linux mediante ESET PROTECT, puede modificar la configuración general de ESET Endpoint Antivirus for Linux.

- Especificar los datos de un servidor proxy para conectarse a Internet
- Configurar cómo se gestionan los archivos de registro

Servidor proxy

Configure ESET Endpoint Antivirus 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**.

Archivos de registro

Modifique la configuración del sistema de registro de ESET Endpoint Antivirus for Linux.

Detalle de registro mínimo

El nivel de detalle define los detalles que incluyen los archivos de registro relacionados con ESET Endpoint Antivirus 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 de la lista de registros entradas de registro anteriores al número de días especificado (`lslog`):

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 Endpoint for Linux (V7+)** en el menú desplegable.
3. Haga clic en **Herramientas** > **Archivos de registro**
4. Activar **Eliminar automáticamente los registros con una antigüedad de más de (días)**
5. Ajuste el día para especificar la antigüedad de los archivos que desea ocultar.
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**.

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. Haga clic en **Optimizar** para iniciar la desfragmentación de los archivos de registro. Se eliminan todas las entradas vacías del registro para mejorar el rendimiento y aumentar la velocidad del proceso de registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

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.

Interfaz de usuario

En esta sección de la configuración de ESET Endpoint Antivirus for Linux mediante ESET PROTECT, puede activar o desactivar las notificaciones en el escritorio y seleccionar las acciones y el estado de la aplicación sobre los que desee recibir notificaciones.

Notificaciones en el escritorio

Puede activar/desactivar notificaciones de escritorio alternando el interruptor situado junto a **Mostrar notificaciones en el escritorio**. Están activadas de forma predeterminada. Estas notificaciones contienen información que no requiere su intervención.

Configure las acciones sobre las que desee recibir notificación:

1. Haga clic en **Editar** junto a **Notificaciones de aplicaciones**.
2. Seleccione las acciones deseadas o anule la selección de las acciones no deseadas.
3. Haga clic en **Aceptar**.

Estado de la protección

Configure de qué estados de la aplicación se informa a ESET Endpoint Antivirus for Linux.

1. Haga clic en **Editar** junto a Estado de la aplicación.
2. En **Mostrado en equipo**, seleccione el estado de la aplicación sobre el que desee recibir notificación.
3. Haga clic en **Aceptar**.

Estado de la aplicación

Cada estado seleccionado en **Estado de la aplicación** > **Editar** > **Mostrado en equipo** mostrará una notificación en la pantalla inicial de ESET Endpoint Antivirus for Linux y el menú ☰ > **Estado de la protección**.

Administración remota

Para administrar ESET Endpoint Antivirus 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 Endpoint Antivirus for Linux.

Ejemplos de casos de uso

En este capítulo se tratan casos de uso comunes de ESET Endpoint Antivirus for Linux.

Recuperación de la información de módulos

Para ver una lista de todos los módulos de ESET Endpoint Antivirus for Linux y sus versiones, ejecute el siguiente comando en una ventana de terminal:

```
/opt/eset/eea/bin/upd --list-modules
```

```
/opt/eset/eea/bin/upd --list-modules
Salida:
EM000        1074.1 (20190925)        Módulo de actualización
EM001        1558.2 (20191218)        Módulo de análisis antivirus y antiespía
EM002         20708 (20200121)        Motor de detección
EM003          1296 (20191212)        Módulo de soporte de archivos comprimidos
EM004          1197 (20200116)        Módulo de heurística avanzada
EM005          1205 (20191209)        Módulo de desinfección
EM017          1780 (20191217)        Módulo de compatibilidad con traducción
EM022          1110 (20190827)        Módulo de base de datos
EM023         15605 (20200121)        Módulo de respuesta rápida
EM029          1026 (20191107)        Módulo de soporte de Mac/Linux
EM037         1833B (20191125)        Módulo de configuración
```

Programación de análisis

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 a. m.

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/eea/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/eea/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 Endpoint Antivirus 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 Endpoint Antivirus for Linux que contienen la base de firmas de virus.

`/var/opt/eset/eea/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 Endpoint Antivirus for Linux.

`/var/opt/eset/eea/cache`

Directorio de archivos binarios

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

`/opt/eset/eea/bin`

Aquí encontrará las siguientes utilidades:

- 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 Endpoint Antivirus for Linux.

`/opt/eset/eea/sbin`

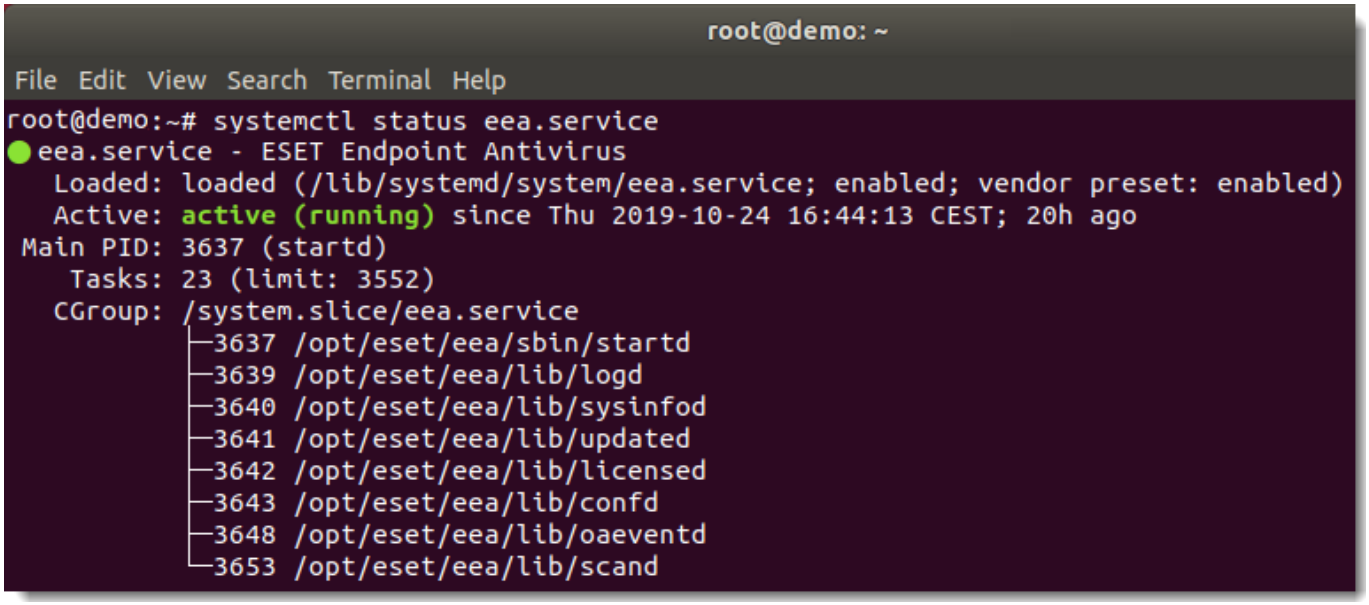
Aquí encontrará las siguientes utilidades:

- 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.
- ecp_logging.sh: utilícela para generar registros relacionados con la activación del producto.
- lic: utilícela para activar ESET Endpoint Antivirus for Linux con la clave de licencia adquirida o para comprobar el estado de activación y la validez de la licencia
- lslog: utilícela para mostrar los registros recopilados por ESET Endpoint Antivirus for Linux.
- startd: utilícela para iniciar el demonio de ESET Endpoint Antivirus for Linux de forma manual, en caso de que se haya detenido

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

```
systemctl status eea.service
```

Ejemplo de salida de `systemctl`:



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 + lib/odfeeder: asistentes del análisis a petición.
- lib/utild: servicio de utilidad.
- lib/sysinfod: servicio de detección de SO y medios.

Utilidades de línea de comandos

- sbin/lslog – Utilidad de enumeración de registros.
- bin/odscan: análisis a petición.
- lib/cfg: utilidad de configuración
- sbin/lic: utilidad de licencias
- bin/upd: utilidad de actualización de los módulos.

- bin/quar: utilidad de administración de la cuarentena.

- lib/cloud: permite enviar una muestra a ESET LiveGrid® o ESET Dynamic Threat Defense desde la línea de comandos (se requiere EEAU versión 8.1 o posterior).

Resolución de problemas

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

- Problemas de activación (solo en inglés)
- 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 Endpoint Antivirus for Linux, utilice el script *collect_logs.sh* disponible en */opt/eset/eea/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/eea/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. También recopila registros de activación si están disponibles. 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.

1. Active el servicio de registro de activación ejecutando el siguiente comando como un usuario con privilegios:

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -e
```

o bien

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -e -f
```

para reiniciar el producto, si es esencial, sin preguntar.

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

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

3. Envíe los registros recopilados al soporte técnico de ESET.

4. Desactive los registros de activación ejecutando el siguiente comando como un usuario con privilegios:

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -d
```

o bien

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -d -f
```

para reiniciar el producto, si es esencial, sin preguntar.

Uso del marcador noexec

Si tiene las rutas de acceso `/var` y `/tmp` montadas con el marcador `noexec`, la instalación de ESET Endpoint Antivirus 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/eea drwxrwxr-x. root eset-eea-daemons
```

2. Ejecute el siguiente comando:

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

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

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

3. Compile los módulos esenciales:

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

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

```
Environment=MODMAPDIR=/usr/lib/eea
```

5. Vuelva a cargar la configuración del servicio systemd:

```
# systemctl daemon-reload
```

6. Reinicie el servicio eea:

```
# systemctl restart eea
```

La protección en tiempo real no se puede iniciar

A continuación se presentan en Ubuntu un problema de muestra y una solución de muestra.

Problema

La protección en tiempo real no se puede iniciar porque faltan archivos del kernel.

En */var/log/messages* se muestra un error acerca de ESET Endpoint Antivirus for Linux:

15 de octubre, 15:42:30 localhost eea: Error de ESET Endpoint Antivirus error: no se puede encontrar el directorio de fuentes del kernel versión 3.10.0-957.el7.x86_64.

15 de julio, 15:42:30 localhost efs: Error de ESET Endpoint Antivirus compruebe si la versión del paquete kernel-devel (o linux-headers) coincide con la versión de kernel actual.

15 de octubre, 15:42:30 localhost oaeventd[31471]: Error de ESET Endpoint Antivirus: no se puede abrir el archivo /lib/modules/3.10.0-957.el7.x86_64/eset/eea/eset_rtp.ko: el archivo o el directorio no existe.

Solucion

Método 1: Requiere reiniciar el sistema operativo.

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

```
apt-get update
```

```
apt-get upgrade
```

2. Reinicie el sistema operativo.

Método 2

1. Instale los módulos kernel-headers más recientes en distribuciones Linux basadas en DEB. En Ubuntu, ejecute los siguientes comandos desde una ventana de terminal o como un usuario con privilegios:

```
apt update
apt install linux-headers-$(uname -r)
```

2. Reinicie el servicio EEA.

```
systemctl restart eea
```

Glosario

- **Demonio**: tipo de programa de los sistemas operativos similares a Unix que se ejecuta de forma no intrusiva en segundo plano. Lo activa la aparición de un suceso o una condición específicos.

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 SUJECIÓN A LOS TÉRMINOS Y CONDICIONES.

1. **Software**. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo (de aquí en adelante, la "Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. **Instalación, Ordenador y una Clave de licencia**. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (en adelante denominados "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (de aquí en adelante, “un AUC”) cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta,

notifíqueselo inmediatamente al Proveedor.

c) **Business Edition.** Debe obtener una versión Business Edition del Software para poder utilizarlo en servidores, relays abiertos y puertas de enlace de correo, así como en puertas de enlace a Internet.

d) **Vigencia de la licencia.** Tiene derecho a utilizar el Software durante un período de tiempo limitado.

e) **Software OEM.** El software OEM solo se puede utilizar en el ordenador con el que se le proporcionó. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR.** El Software cuya venta esté prohibida o de prueba no se puede pagar, y únicamente se debe utilizar para demostraciones o para probar las características del Software.

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la licencia, el usuario debe eliminar, destruir o devolver (a sus expensas) el software y todas las copias de seguridad del mismo a ESET o al lugar donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El Proveedor podrá publicar ocasionalmente actualizaciones del Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para suministrar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

b) **Envío de amenazas e información al proveedor**. El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet (de aquí en adelante “amenazas”) y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el ordenador o la plataforma en la que el Software está instalado o información sobre las operaciones y las funciones del Software e información sobre dispositivos de la red local como tipo, proveedor, modelo o nombre del dispositivo (de aquí en adelante “información”). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las Amenazas junto con los metadatos asociados.

La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La 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 regirá e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. En caso de discrepancia entre las versiones de este acuerdo en diferentes idiomas, prevalecerá la versión en inglés. Este acuerdo solo se puede modificar por escrito y con la firma de un representante autorizado del proveedor o una persona autorizada expresamente para este fin mediante un poder notarial.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

EULA ID: BUS-STANDARD-20-01

Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, número de registro de la empresa 31333532, como controlador de datos («ESET» o «Nosotros»), quiere ser transparente en cuanto al procesamiento de datos personales y la privacidad de sus clientes. Para alcanzar este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes («Usuario final» o «Usted») sobre los siguientes temas:

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

Los servicios prestados por ESET implementados en el producto se prestan de acuerdo con los términos del Acuerdo de licencia para el usuario final ("EULA"), pero algunos pueden requerir atención específica. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos diferentes servicios descritos en el EULA y en la documentación de producto, como el servicio de actualización, ESET LiveGrid®, protección contra mal uso de datos, soporte, etc. Para que todo funcione, debemos recopilar la siguiente información:

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Algoritmos hash unidireccionales relativos a infiltraciones que forman parte del sistema de reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones contra malware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.
- Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe
  - infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
  - información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;
  - información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;

- 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