ESET Endpoint Antivirus for Linux

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

ESET Endpoint Antivirus for Linux was developed by ESET, spol. s r.o.

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 4/12/2024

1 Introduction 1
1.1 Key features of the system 1
2 Release notes 1
3 System requirements 1
3.1 Secure boot 4
4 Installation 6
4.1 Uninstall 7
4.2 Mass deployment 7
5 Activate ESET Endpoint Antivirus for Linux 12
5.1 Where can I find my license 13
5.2 Activation status 13
6 Update, upgrade 14
6.1 Update mirror 16
7 Using ESET Endpoint Antivirus for Linux 17
7.1 User interface 17
7.2 Scans 20
7.2 Exclusions 22
7.3 Quarantine 23
7.4 Events 25
7.5 Notifications 26
8 Configuration 26
8.1 Detection engine 27
8.1 Exclusions 27
8.1 Cloud-based protection 29
8.1 Malware scans 31
8.2 Update 32
8.3 Protections 33
8.3 Real-time file system protection 34
8.3 ThreatSense parameters 36
8.3 Additional ThreatSense parameters 38
8.3 Web access protection 38
8.3 Excluded applications 40
8.3 Excluded IPs 40
8.3 URL address management 41
8.3 Create new list 42
8.3 HTTPS traffic scanning 45
8.3 List of SSL/TLS filtered applications 46
8.3 List of known certificates 47
8.3 Network access protection 48
8.3 Device control 48
8.3 Device control rules editor 49
8.3 Device groups 50
8.3 Adding Device control rules 50
8.4 Tools 52
8.4 Proxy Server 52
8.4 Log files 52
8.5 User interface 54
8.5 Application status 54
9 Remote Management 54
10 Use case examples 55

10.1 Retrieve module information 55
10.2 Schedule scan 55
11 File and folder structure 56
12 Troubleshooting 59
12.1 Collect logs 59
12.2 Using the noexec flag 61
12.3 Realtime protection cannot start 62
12.4 NFS mount fails 63
12.5 Using WireGuard with Web access protection 63
13 Glossary 64
14 End User License Agreement 64
15 Privacy Policy 71

Introduction

ESET's state-of-the-art scanning engine has unsurpassed scanning speed and detection rates combined with a tiny footprint that makes ESET Endpoint Antivirus for Linux (EEAU) the ideal choice for any Linux desktop meeting the system requirements.

The On-demand scanner and On-access scanner cover the main functionality.

The On-demand scanner can be started through the command-line interface, ESET PROTECT, or by the operating system's automatic scheduling tool (for example, `cron`). The term On-demand refers to file system objects being scanned by either user or system demand.

The On-access scanner is invoked by any attempt to access file system objects.

Key features of the system

- On-access scan by ESET's lightweight in-kernel module
- Comprehensive scan logs
- Redesigned, easy-to-use setup
- Automatic product updater
- Quarantine
- Desktop notifications
- Manageable via ESET PROTECT
- Cloud-based protection
- Web access protection
- Device control
- ESET Inspect support

Release notes

System requirements

Hardware requirements

Minimum hardware requirements to be met before the installation process to run ESET Endpoint Antivirus for Linux properly:

- processor Intel/AMD x64
- 700MB of free hard disk space

Software requirements

The following operating systems of 64-bit architecture are officially supported and tested:

- Ubuntu Desktop 18.04 LTS 64-bit
- Ubuntu Desktop 20.04 LTS
- Ubuntu Desktop 22.04 LTS
- Red Hat Enterprise Linux 8, 9 with supported desktop environment installed.
- Linux Mint 20, 21

The latest Linux kernel for Ubuntu Desktop 22.04 LTS/Linux Mint 21 requires gcc-12 for kernel modules compilation. See our Knowledgebase article for more information on this issue.

AWS kernel
Linux distributions with AWS kernel are not supported.

Supported display servers:

- X11
- Wayland

Supported desktop environments:

- Cinnamon 5.0 and later
- GNOME 3.28.2 and later
- KDE
- MATE
- XFCE

Any locale with UTF-8 encoding.

The user interface and command list in the Terminal window are available in the following languages:

- English
- German

- Spanish
- Spanish Latin America
- French
- Polish
- Ukrainian
- Japanese

If the host OS uses an unsupported language, English is used by default.

Network prerequisites

To ensure the proper functioning of the ESET Endpoint Antivirus for Linux allow the network prerequisites listed in the Knowledgebase article.

Supported filesystems

The following filesystems are officially supported and tested:

Filesystem	Local devices	Removable devices	Network
Btrfs	✔		
FAT		✔	
VFAT	✔	✔	
exFAT	✔	✔	
F2FS		✔	
ext4 (version 2, version 3)	✔	✔	
JFS	✔		
NTFS	✔	✔	
UDF		✔	
XFS	✔		
ZFS	✔		
EncFS	✔		
FUSE (snap, appimage)	✔		
tmpfs	✔		
NFS client (version 3, version 4)			✔
SMB (GVfs, CIFS)			✔
SSHFS			✔

Remote management via ESET PROTECT

Secure boot

To use real-time file system protection and web access protection on a machine with Secure boot enabled, the ESET Endpoint Antivirus for Linux (EEAU) kernel modules must be signed with a private key. The corresponding public key must be imported to UEFI. EEAU comes with a built-in signing script, that operates in interactive or non-interactive mode.

Use the `mokutil` utility to verify Secure boot is enabled on the machine. Execute the following command from a Terminal window as a privileged user:

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

Interactive mode

If you do not have a public and private key to sign the kernel modules, Interactive mode can generate new keys and sign the kernel modules. It also helps enroll the generated keys in UEFI.

1. Execute the following command from a Terminal window as a privileged user:

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

2. When the script prompts you for keys, type N, then press **Enter**.

3. When prompted to generate new keys, type Y, then press **Enter**. The script signs the kernel modules with the generated private key.

4. To enroll the generated public key to UEFI semiautomatically, type Y, then press **Enter**. To complete the enrollment manually, type N, press **Enter**, and follow the on-screen instructions.

5. When prompted, type a password of your choice. Remember the password; you will need it when completing enrollment (approval of new Machine Owner Key [MOK]) in UEFI.

6. To save the generated keys to your hard drive for later use, type Y, type the path to a directory, press **Enter**.

7. To reboot and access UEFI, type Y when prompted, and press **Enter**.

8. Press any key within 10 seconds when prompted to access UEFI.

9. Select **Enroll MOK**, press **Enter**.

10. Select **Continue**, press **Enter**.

11. Select **Yes**, press **Enter**.

12. To complete the enrollment and reboot the machine, type the password from step 5 and press **Enter**.

Non-interactive mode

Use this mode if you have a private and public key available on the target machine.

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

Options - short form	Options - long form	Description
`-d`	`--public-key`	Set the path to a DER format public key to use for signing
`-p`	`--private-key`	Set the path to the private key to use for signing
`-k`	`--kernel`	Set the name of the kernel whose modules have to be signed. If not specified, the current kernel is selected by default
`-a`	`--kernel-all`	Sign (and build) kernel modules on all existing kernels containing headers
`-h`	`--help`	Show help

1. Execute the following command from a Terminal window as a privileged user:

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

Replace `<path_to_private_key>` and `<path_to_public_key>` with the path leading to a private key and public key respectively.

2. If the provided public key is not enrolled in UEFI yet, execute the following command as a privileged user:

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

`<path_to_public_key>` represents the provided public key.

3. Reboot the machine, access UEFI, select **Enroll MOK** > **Continue** > **Yes**.

Managing several devices

Suppose you manage several machines that use the same Linux kernel and have the same public key enrolled in UEFI. In that case, you can sign the EEAU kernel modules on one of those machines containing the private key and then transfer the signed kernel modules to the other machines. When the signing is complete:

1. Copy/paste the signed kernel modules from `/lib/modules/<kernel-version>/eset/eea/eset_rtp` and `eset_wap` to the same path on the target machines.

2. Call `depmod <kernel-version>` on the target machines.

3. Restart ESET Endpoint Antivirus for Linux on the target machine to update the modules table. Execute the following command as a privileged user:

```
systemctl restart eea
```

In all cases, replace `<kernel-version>` with the corresponding kernel version.

Installation

ESET Endpoint Antivirus for Linux is distributed as a binary file (`.bin`).

ESET Endpoint Antivirus for Linux may not work properly in case some other security product is installed and running on the system.
In case of any (unknown) problems, please try to install ESET Endpoint Antivirus for Linux on clean machine, without any other security or third-party products.

Update your OS
If your OS is supported, ensure it has the most recent updates installed before installation of ESET Endpoint Antivirus for Linux.

Installation via Terminal

The commands below are valid if you are at the location of the mentioned files in the Terminal window.

To install or upgrade your product, run the ESET distribution script with root privileges for the appropriate OS distribution that you have:

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

See the available command-line arguments

To display the available parameters (arguments) of ESET Endpoint Antivirus for Linux binary file, run the following command from a terminal window:
`./eeau.x86_64.bin -h`

Available parameters

Short form	Long form	Description
`-h`	`--help`	Display command-line arguments
`-n`	`--no-install`	Do not perform installation after unpacking
`-y`	`--accept-license`	Do not show the license, license has been accepted
`-f`	`--force-install`	Force installation via package manager without asking
`-u`	`--unpack-ertp-sources`	Unpack "ESET Real-time file system protection kernel module" sources, do not perform installation

Gain .deb installation package
To gain `.deb` installation package suitable for your OS, run ESET distribution script with "`-n`" command-line argument:
`sudo ./eeau.x86_64.bin -n`
or
`sudo sh ./eeau.x86_64.bin -n`

To see the dependencies of the installation package, run one of the following commands:

- `dpkg -I <deb package>`

- `rpm -qRp <rpm package>`

Follow the on-screen instructions. Accept the product License Agreement to complete the installation.

The installer would inform you of any dependency problems.

Installation via ESET PROTECT

To deploy ESET Endpoint Antivirus for Linux remotely on your computers, refer to the ESET PROTECT Software Install online help section.

Activate ESET Endpoint Antivirus for Linux

To enable regular updates of detection modules, activate ESET Endpoint Antivirus for Linux.

> **Third-party apps**
> A summary of third-party apps used by ESET Endpoint Antivirus for Linux can be found in the `NOTICE_mode` file stored at `/opt/eset/eea/doc/modules_notice/`.

Uninstall

To uninstall your ESET product, use the terminal window as a superuser to execute the command of removing packages corresponding to your Linux distribution.

Ubuntu/Debian based distributions:

- `apt remove eea`
- `dpkg remove eea`

Red Hat based distributions:

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

Mass deployment

This topic provides a high-level overview of mass deployment of ESET Endpoint Antivirus for Linux via Puppet, Chef and Ansible. The code blocks below contain only basic examples of how packages could be installed. They might differ per linux distribution.

Package selection

Before you start the mass deployment of ESET Endpoint Antivirus for Linux, you have to decide which package to use. ESET Endpoint Antivirus for Linux is distributed as a `.bin` package. However, you can obtain deb/rpm package by running the ESET distribution script with "`-n`" command-line argument.

Puppet

Precondition

- bin or deb/rpm package available on puppet-master
- puppet-agent connected to puppet-master

Bin package

Deployment steps:

- copy the bin installation package to the desired machines
- run the bin installation package

Puppet manifest sample

```
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'
         }
}
```

Deb/rpm package

Deployment steps:

- copy deb/rpm installation package according to distribution family to the desired machines
- run the deb/rpm installation package

Dependencies
Dependencies have to be resolved before starting the installation

Puppet manifest sample

```
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

Precondition

- bin or deb/rpm package available on Chef server
- Chef client connected to Chef server

Bin package

Deployment steps:

- copy the bin installation package to the desired machines
- run the bin installation package

Chef recipe sample

```
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
```

Deb/rpm package

Deployment steps:

- copy deb/rpm installation package according to distribution family to the desired machines
- run the deb/rpm installation package

Dependencies

Dependencies have to be resolved before starting the installation

Chef recipe sample

```
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

Precondition

- bin or deb/rpm package available on Ansible server
- ssh access to target machines

Bin package

Deployment steps:

- copy the bin installation package to the desired machines
- run the bin installation package

Playbook task sample

```
....
- 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
.....
```

Deb/rpm package

Deployment steps:

- copy deb/rpm installation package according to distribution family to the desired machines
- run the deb/rpm installation package

Playbook task sample

```
....
      - 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"
....
```

Activate ESET Endpoint Antivirus for Linux

Activate your ESET Endpoint Antivirus for Linux using a license obtained from your ESET distributor.

Activate using Terminal

Use the `/opt/eset/eea/sbin/lic` utility as a privileged user to activate ESET Endpoint Antivirus for Linux from a Terminal window.

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

Examples

The commands below have to be executed as a privileged user.

Activation via a license key

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

or

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

while XXXX-XXXX-XXXX-XXXX-XXXX represents your ESET Endpoint Antivirus for Linux License Key.

Activation using an EBA or EMA account

1. Execute:

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

where your@username represents your EBA or EMA account username.

2. Type in your password, and press **Enter**.

3. If there is only a single EEAU license in your EBA or EMA account and no sites are created, the activation will complete instantly. Otherwise, a list of available EEAU licenses and sites (license pool) will display.

4. Execute one of the following commands:

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

while `XXX-XXX-XXX` represents a public license ID enclosed in square brackets next to each license in the list displayed earlier.

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

while `site_ID` represents an alphanumeric string displayed in square brackets next to each site in the list displayed earlier.

5. Type in your password, and press **Enter**.

If the username, password and public license ID are stored in a `password.txt` file, execute the following as a privileged user:

```
cat password.txt | /opt/eset/eea/sbin/lic -u your@username -p XXX-XXX-XXX --stdin-pass
```

Activation via an offline license file

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

or

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

Activate using ESET PROTECT

Log in to ESET PROTECT Web interface, navigate to **Client Tasks** > **Product Activation**, and follow the instructions on product activation.

Where can I find my license

If you purchased a license, you should have received two emails from ESET. The first email contains information about the ESET Business Account portal. The second email contains details about your License Key (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) or Username (EAV-xxxxxxxxxx) and Password when applicable, Public License ID (xxx-xxx-xxx), product name (or list of products), and quantity.

For free trial license refer to free trial license in ESET Business Account.

Check the activation status

To see the activation status and license validity, use the `lic` utility. Execute the following commands as a privileged user:

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

The commands below must be executed as a privileged user:
`/opt/eset/eea/sbin/lic -s`
or
`/opt/eset/eea/sbin/lic --status`

Sample output when the product is activated:
```
Status: Activated
Public Id: ABC-123-DEF
License Validity: 2020-03-29
```

Output when the product is not activated:
```
Status: Not activated
```

If ESET LiveGuard Advanced is activated for the specific instance of ESET Endpoint Antivirus for Linux, the output displays the related license details.

In version 8.1 or later, to display the Seat ID if requested by ESET customer care, execute:

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

Update, upgrade

Quick jump to upgrade

Update of modules

Product modules, including detection modules, are updated automatically.

To launch the detection module update manually, execute the update command via a Terminal window, or update using ESET PROTECT.

If an ESET Endpoint Antivirus for Linux update was not stable, roll back the module updates to a previous state. Execute the appropriate command from a Terminal window, or roll back using ESET PROTECT.

To update all product modules from a Terminal window, execute the following command:

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

Update and rollback via Terminal

Options - short form	Options - long form	Description
`-u`	`--update`	Update modules
`-c`	`--cancel`	Cancel downloading modules
`-e`	`--resume`	Unblock updates
`-l`	`--list-modules`	Show version of used modules
`-r`	`--rollback=VALUE`	Rolls back to the oldest snapshot of the scanner module and blocks all updates for `VALUE` hours

The upd utility cannot be used to make changes in product configuration.

Example

To stop updates for 48 hours and roll back to the oldest snapshot of the scanner module, execute the following command as a privileged user:

```
sudo /opt/eset/eea/bin/upd --update --rollback=48
```

To resume automatic updates of the scanner module, execute the following command as a privileged user:

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

To update from a mirror server available at IP address "192.168.1.2" and port "2221", execute the following command as a privileged user:

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

Upgrade ESET Endpoint Antivirus for Linux (EEAU) to a later version

New versions of EEAU are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules.

Which product version is currently installed?

To determine the product version of EEAU, you have two options:

1. Execute /opt/eset/eea/lib/egui -v in a Terminal window.
2. Check in ESET PROTECT in the Computers section.

How to upgrade?

To upgrade to a more recent version, run an OS-related installation package as described in the Installation section.

If managing ESET Endpoint Antivirus for Linux through ESET PROTECT , you can initiate upgrade via Software install task, or via **Dashboard** > **ESET applications** > click ESET Endpoint Antivirus > **Update installed ESET products**.

Direct upgrade from ESET NOD32 Antivirus 4 Business Edition for Linux Desktop is not possible

ESET Endpoint Antivirus for Linux is a completely new product and its configuration is not compatible with the configuration of ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.

To upgrade from ESET NOD32 Antivirus 4 Business Edition for Linux Desktop to ESET Endpoint Antivirus for Linux,

follow the instructions below.

Remotely managed environment (ESET PROTECT)

If you manage ESET NOD32 Antivirus 4 Business Edition for Linux Desktop remotely, ESET PROTECT will not notify about available upgrade.

1. Execute Software uninstall task on existing installations of ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.

2. Deploy ESET Endpoint Antivirus for Linux remotely on your computers using the Software Install task.

Personally managed environment

If you try to install ESET Endpoint Antivirus for Linux before removing ESET NOD32 Antivirus 4 Business Edition for Linux Desktop, the installation fails with the following message:

```
"Error: Previous ESET Security product must be uninstalled first, package won't be installed."
```

1. Uninstall ESET NOD32 Antivirus 4 Business Edition for Linux Desktop using the downloaded installer.

   i. Right-click the downloaded installer file (`eset_nod32av_64bit_<language_code>.linux`), click **Properties** > **Permissions** tab, check the **Allow executing file as program** option and close the window.

   ii. Double-click the installer to launch **ESET NOD32 Antivirus Setup**.

   iii. Click **Next**, select **Uninstall ESET NOD32 Antivirus from your computer**, click **Next**.

   iv. From the **Please select one of the options** list-box, select **None of the listed**.

   v. Type "*Upgrade to ESET Endpoint Antivirus for Linux*" to **Other additional data**, click **Next**, then **Uninstall**.

   vi. Click **Finish** when complete, then click **Yes** to restart the computer.

2. Install ESET Endpoint Antivirus for Linux.

Update mirror

Several ESET security products (ESET PROTECT, ESET Endpoint Antivirus, etc.) allow you to create copies of the update files to update other workstations on the network. The use of a mirror— a copy of the update files in the LAN environment—is convenient because the update files do not need to be downloaded from the vendor update server repeatedly by each workstation. Updates are downloaded to the local mirror server and then distributed to all workstations to avoid the risk of network traffic overload. Updating client workstations from a mirror optimizes network load balance and saves internet connection bandwidth.

Configure ESET Endpoint Antivirus for Linux to use an update mirror

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.

2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.

3. Click **Update** > **Primary Server**.

4. In the **Basic** section, click the toggle next to **Choose automatically** to turn it off.

5. In the **Update server** field, type the URL address of the mirror server in one of the following forms:

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

6. Type the applicable username and password.

7. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

8. Click **OK**, then click **Finish**.

If there are more mirror servers available in your network, repeat the steps above to configure the secondary update servers.

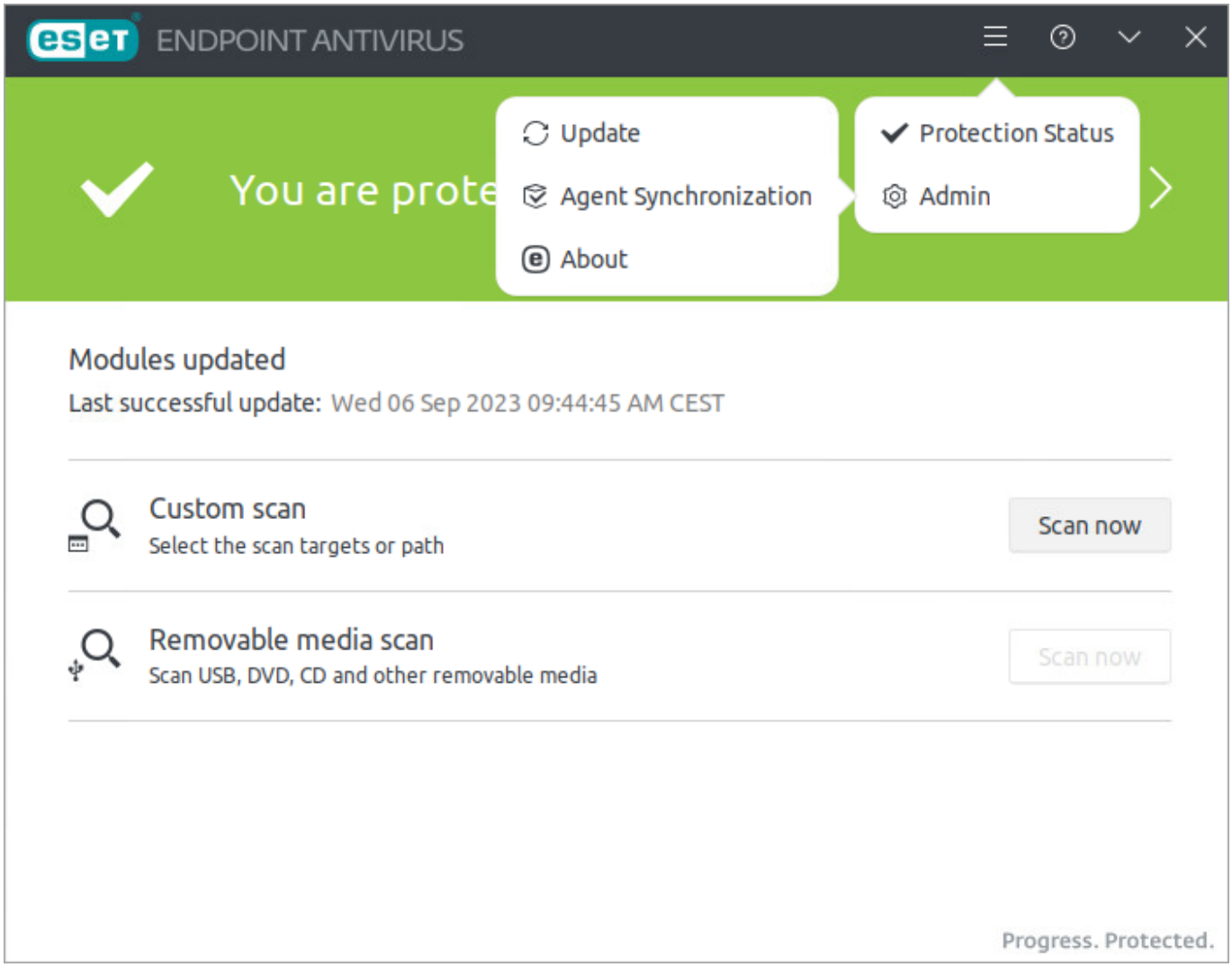
Using ESET Endpoint Antivirus for Linux

If the installation is complete, use a Terminal window or ESET PROTECT to operate ESET Endpoint Antivirus for Linux.

The user interface also enables the execution of some actions.

User interface

ESET Endpoint Antivirus for Linux introduces a minimalistic graphical user interface.



The home screen provides an overview of protection status, alerts, notifications and enables starting On-demand scans of a custom path.

Scans

To scan a custom path:

1. Click **Scan now** in the **Custom scan** section.
2. Type a valid path to scan.
3. Click **Scan**.

If a removable media device is recognized, ESET Endpoint Antivirus for Linux enables to scan it. Click **Removable media scan**, and ESET Endpoint Antivirus for Linux will scan all recognized removable media.

> When a scan is complete, it displays a quick overview of found detections and cleaned threats. To see more details, click **Show scan details**.

Menu

If you navigate to any screen through the menu , click the back button to get back to the home screen.

Protection status

When everything is working without any issues, the overall protection status (home screen) is green. If there are options to improve your system's protection status or insufficient protection status is detected, the color turns red.

To see more detailed information on protection status, click the menu icon > **Protection Status**.

Update

To manually start updates of modules, click the menu icon > **Admin** > **Update**. The screen displays the last successful update and last check for updates.

Installed modules

There are two ways to list the installed modules:

1. Click the menu icon > **Admin** > **Update** > **Show all modules**.
2. Click the menu icon > **Admin** > **About** > **Show all**.

Agent synchronization

If you manage ESET Endpoint Antivirus for Linux remotely, you can see some details of the management agent at menu > **Admin** > **Agent Synchronization**.

The details include:

- Current version—version of the currently installed remote management agent
- Last replication—represents the last attempt of synchronization between the remote management agent and ESET PROTECT
- Last successful replication
- Last status log generated—the last time the management agent generated a status log. The log file is available at `/var/log/eset/RemoteAdministrator/Agent/status.html`

About

The **About** screen provides details about the installed version of ESET Endpoint Antivirus for Linux, your operating system, and system resources.

Click **Show all** to see information about the list of installed program modules.

Scans

Quick link: Scan profiles

Run On-demand scan from a Terminal window

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

Options - short form	Options - long form	Description
`-l`	`--list`	Show currently running scans
	`--list-profiles`	Show all available scan profiles
	`--all`	Show also scans executed by other user (requires root privileges)
`-r`	`--resume=session_id`	Resume previously paused scan identified by `session_id`
`-p`	`--pause=session_id`	Pause scan identified by `session_id`
`-t`	`--stop=session_id`	Stop scan identified by `session_id`
`-s`	`--scan`	Start scan
	`--show-scan-info`	Display basic information (including `session_id`, log_name) about the started scan
	`--profile=PROFILE`	Scan with selected PROFILE
	`--profile-priority=PRIORITY`	Task will be run with the specified priority. Priority can be: `normal`, `lower`, `lowest`, `idle`
	`--readonly`	Scan without cleaning
	`--local`	Scan local drives
	`--network`	Scan network drives
	`--removable`	Scan removable media
	`--boot-local`	Scan the boot sectors of local drive
	`--boot-removable`	Scan the boot sectors of removable media
	`--boot-main`	Scan the main boot sector
	`--exclude=FILE`	Skip selected file or directory
	`--ignore-exclusions`	Scan also excluded paths and extensions

Example

Run On-demand scan of */root/* directory recursively with "@Smart scan" scan profile as a background process:

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

Run On-demand scan with "@Smart scan" scan profile regarding multiple destinations recursively:

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

List all running scans:

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

Pause scan with session-id "15". Each scan has its own unique session-id generated when it is started.

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

Stop scan with session-id "15". Each scan has its own unique session-id generated when it is started.

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

Run On-demand scan with an excluded directory */root/exc_dir* and an excluded file */root/eicar.com*:

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

Scan the boot sector of removable devices. Execute the command below as a privileged user:

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

Exit codes

The `odscan` utility ends with an exit code after completed scan. Execute `echo $?` in the Terminal window after completed scan to display the exit code.

Exit codes	Meaning
0	No threat found
1	Threat found and cleaned
10	Some files could not be scanned (may be threats)
50	Threat found
100	Error

Scan profiles

Your preferred scan parameters (Threatsense parameters) can be saved for future scanning. We recommend creating a different profile (with various scan targets, scan methods, and other parameters) for each regularly used scan.

Create a new profile through ESET PROTECT

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.

3. Click **Detection Engine** > **Malware scans** > **On-demand scan**, and click **Edit** next to **List of profiles**.

4. Type the desired name of the new profile, click **Add** and then click **Save**.

5. In the **Selected profile** drop-down menu, select the new profile you created and adjust scan-related settings in the **Malware scans** section.

6. Navigate to **Assign**, click **Assign**, select the desired group of computers the policy will apply to.

7. Click **OK** and then **Finish**.

Exclusions

Performance exclusions

By excluding paths (folders) from being scanned, the time needed to scan the file system for the presence of malware can be significantly decreased.

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.

2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.

3. Navigate to **Detection Engine** > **Exclusions** and click **Edit** next to **Performance exclusions**.

4. Click **Add**, define the **Path** to be skipped by the scanner. Optionally add a comment for your information.

5. Click **OK**, then click **Save** to close the dialog.

6. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

7. Click **OK**, then click **Finish**.

Exclusion paths

*/root/** - The "*root*" directory and all of its sub-directories and their content.

/root - The "*root*" file only.

/root/file.txt - The file.txt in "*root*" directory only.

> **Wildcards in the middle of a path are not supported**
> Do not use wildcards in the middle of a path (for example */home/user/*/data/file.dat*). ESET Endpoint Antivirus for Linux does not support it.

File extension exclusions

This type of exclusion can be set up for **Real-time file system protection** and **On-demand scan**.

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.

2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.

3. Navigate to:

- **Protections** > **Real-time file system protection** > **Threatsense parameters**
- **Detection engine** > **Malware scans** > **On-demand scan** > **Threatsense parameters**

4. Click **Edit** next to **File extensions excluded from scanning**.

5. Click **Add** and type the extension to exclude. To define several extensions at once, click **Enter multiple values**, and type the desired extensions separated by a new line or another separator you selected.

6. Click **OK**, then click **Save** to close the dialog.

7. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

8. Click **OK**, then click **Finish**.

Quarantine

The primary function of the quarantine is to store infected files safely. Files should be quarantined if they cannot be cleaned, or if it is not safe or advisable to delete them, or if falsely detected by ESET Endpoint Antivirus for Linux. You can choose to quarantine any file, especially if a file behaves suspiciously but is not detected by the antivirus scanner.

Path to quarantine directory: */var/opt/eset/eea/cache/quarantine/*

The quarantine directory is created the first time there is an item to be quarantined.

Manage quarantined items via Terminal

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

Options - short form	Options - long form	Description
`-i`	`--import`	Import file to quarantine
`-l`	`--list`	Display list of files in quarantine
`-r`	`--restore=id`	Restore quarantined item identified by id to path defined by `--restore-path`
`-e`	`--restore-exclude=id`	Restore quarantined item identified by id and marked by 'x' in the excludable column
`-d`	`--delete=id`	Delete quarantined item identified by `id`
	`--restore-path=path`	Path to restore a quarantined item to
`-h`	`--help`	Show help and quit.
`-v`	`--version`	Show version information and quit

> **Restore**
> Restore is not available if the command is not executed as a privileged user.

Example

Delete a quarantined item with id "09876543210":

```
/opt/eset/eea/bin/quar -d 09876543210
```

or

```
/opt/eset/eea/bin/quar --delete=09876543210
```

Restore a quarantined item with id "9876543210" to the *Download* folder of the logged in user and rename it to *restoredFile.test* :

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

or

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

Restore a quarantined item with id "9876543210" which is marked "**x**" in the **excludable** column to the *Download* folder:

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

or

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

Restore file from quarantine via Terminal

1. List quarantined items:

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

2. Look up the ID and name of the quarantined object you want to restore and run the following command:

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

Events

ESET Endpoint Antivirus for Linux (EEAU) commands executed via Terminal, and some more events are logged by EEAU.

Each recorded action includes the following information: time the event occurred, component (if available), event, user.

Display events via Terminal

To display the recorded **Events** via a Terminal window, use the `lslog` command-line tool as a privileged user.

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

Options - short form	Options - long form	Description
`-f`	`--follow`	Wait for new logs and append them to the output
`-o`	`--optimize`	Optimize logs
`-c`	`--csv`	Display logs in CSV format.
`-e`	`--events`	List Event logs
`-u`	`--urls`	List URL logs
`-l`	`--device-control`	List Device Control logs
`-n`	`--sent-files`	Display a list of files submitted for analysis
`-s`	`--scans`	List On-Demand scan logs
	`--with-log-name`	Display Log name column in addition
	`--ods-details=log-name`	Display details of an on-demand scan identified by log name
	`--ods-detections=log-name`	Display detections of an on-demand scan identified by log name
	`--ods-notscanned=log-name`	Display not scanned items of an on-demand scan identified by log name
`-d`	`--detections`	List Detection Log records
	`--ods-events=log-name`	Print detections found and files not scanned during specific On-demand scan identified by log name.
`-b`	`--blocked-files`	List blocked files logs
`-t`	`--network`	List Network Access Protection logs

Examples

Display all event logs:

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

Save all event logs in CSV format to a file in the *Documents* directory of current user:

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

Display every threat detected and action taken against:

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

Notifications

EEAU displays various notifications to inform you about an activity or a required action. Some of the notifications can be enabled or disabled.

The notifications are related to:

- On-demand scan—For example, a scan of a removable device has been started or completed.
- Device control—A device has been blocked, or writing data on the device is not allowed.
- Detections—For example, a threat has been found or removed, or a file has been cleaned.
- Web access protection—For example, a threat has been found or removed, or a file has been cleaned.
- Network access protection—For example, a threat has been found and blocked.
- Operating system—A restart is required, or a shutdown is scheduled.
- ESET LiveGuard Advanced since EEAU version 8.1—For example, a file is being analyzed and, therefore, cannot be opened temporarily.
- ESET Inspect since EEAU version 9.0—For example, file access is blocked, or the file is deleted due to security reasons.

Configuration

To alter the configuration of ESET Endpoint Antivirus for Linux:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Adjust the desired settings.
4. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.
5. Click **OK**, then click **Finish**.

> **Adjust existing policy settings**
> To adjust existing policy settings for ESET Endpoint Antivirus for Linux, click the policy you want to change in the list of policies and click **Edit**.

You can adjust the detection behavior, alter product updates and connection settings.

Suppose you have configured ESET Endpoint Antivirus for Linux according to your requirements, and you want to save the configuration for later use (or to use it with another instance of ESET Endpoint Antivirus for Linux). In that case, you can export it to an *.XML* file.

Execute the following commands with root privileges from a terminal window.

Export configuration

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

Import configuration

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

Available options

Short form	Long form	Description
`-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

Detection engine

Detection engine enables you to configure the following options:

- Exclusions
- Cloud-based protection
- Malware scans

Exclusions

Performance exclusions

By excluding paths (folders) from being scanned, the time needed to scan the file system for the presence of malware can be significantly decreased.

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Navigate to **Detection Engine** > **Exclusions** and click **Edit** next to **Performance exclusions**.
4. Click **Add**, define the **Path** to be skipped by the scanner. Optionally add a comment for your information.
5. Click **OK**, then click **Save** to close the dialog.
6. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.
7. Click **OK**, then click **Finish**.

Exclusion paths

*/root/** - The "*root*" directory and all of its sub-directories and their content.

/root - The "*root*" file only.

/root/file.txt - The file.txt in "*root*" directory only.

> **Wildcards in the middle of a path are not supported**
> Do not use wildcards in the middle of a path (for example */home/user/*/data/file.dat*). ESET Endpoint Antivirus for Linux does not support it.

File extension exclusions

This type of exclusion can be set up for **Real-time file system protection** and **On-demand scan**.

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Navigate to:

- **Protections** > **Real-time file system protection** > **Threatsense parameters**
- **Detection engine** > **Malware scans** > **On-demand scan** > **Threatsense parameters**

4. Click **Edit** next to **File extensions excluded from scanning**.
5. Click **Add** and type the extension to exclude. To define several extensions at once, click **Enter multiple values**, and type the desired extensions separated by a new line or another separator you selected.
6. Click **OK**, then click **Save** to close the dialog.

7. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

8. Click **OK**, then click **Finish**.

Cloud-based protection

Quick links: Cloud-based protection, Submission of samples, ESET LiveGuard Advanced

ESET LiveGrid® is an advanced early warning system comprised of several cloud-based technologies. It helps to detect emerging threats based on reputation and improves scanning performance utilizing whitelisting.

When deploying ESET Endpoint Antivirus for Linux remotely through ESET PROTECT, you can configure one of the following options regarding cloud-based protection:

- You can decide not to enable ESET LiveGrid®. Your software will not lose any functionality, but in some cases, ESET Endpoint Antivirus for Linux may respond slower to new threats than detection engine database update.
- You can configure ESET LiveGrid® to submit anonymous information about new threats and where the new threatening code was detected. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

By default, ESET Endpoint Antivirus for Linux is configured to submit suspicious files to the ESET Virus Lab for analysis. Files with certain extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are specific files that you or your organization want to avoid sending.

Cloud-based protection

Enable ESET LiveGrid® reputation system (recommended)

The ESET LiveGrid® reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

Enable ESET LiveGrid® feedback system

Data will be sent to the ESET Research Lab for further analysis.

Submit crash reports and diagnostic data

Submit data such as crash reports, modules or memory dumps.

Help improve the product by submitting anonymous usage statistics

Allow ESET to collect information about newly detected threats such as the threat name, date and time of detection, detection method and associated metadata, scanned files (hash, filename, origin of the file, telemetry), blocked and suspicious URL's, product version and configuration, including information about your system.

Contact email (optional)

Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is

needed.

Submission of samples

Automatic submission of detected samples

Based on the selected option, this can submit infected samples to ESET for analysis and to improve future detection.

- All infected samples
- All samples except documents
- Do not submit

Automatic submission of suspicious samples

Suspicious samples resembling threats, and/or samples with unusual characteristics or behavior are submitted to ESET for analysis.

- Executable - Includes executable files: *.exe, .dll, .sys*
- Archives - Includes archive file types: *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- Scripts - Includes script file types: *.bat, .cmd, .hta, .js, .vbs, .ps1*
- Other - Includes file types: *.jar, .reg, .msi, .swf, .lnk*
- Documents - Includes documents created in Microsoft Office, Libre Office or other office tool, or PDF's with active content

Exclusions

Click **Edit** next to **Exclusions** to configure how threats are submitted to ESET Virus Labs for analysis.

Maximum size of samples (MB)

Define the maximum size of samples to be scanned.

Allow the below network prerequisites in your firewall for ESET Endpoint Antivirus for Linux to work correctly:
- For correct operation of ESET LiveGrid® see the Knowledgebase article
- For correct operation of ESET LiveGrid® feedback system (submission of samples) see the Knowledgebase article

ESET LiveGuard Advanced

ESET LiveGuard Advanced is a paid service provided by ESET. Its purpose is to add a layer of protection specifically designed to mitigate new threats in the world.

> **Availability**
> The service is available only if ESET Endpoint Antivirus for Linux version 8.1 or later is managed remotely. Depending on the proactive protection settings of ESET LiveGuard Advanced, a file submitted for analysis might be blocked from execution until a result is received. Such blocking is accompanied by a message of "Operation not permitted" or a similar message.

To see the status of ESET LiveGuard Advanced service in your instance of EEAU, execute one of the following commands in a Terminal window as a privileged user:

```
/opt/eset/eea/lib/cloud -l
```

or

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

To enable the service in EEAU:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Click **Detection engine** > **Cloud-based protection**.
4. Enable **Enable ESET LiveGrid® reputation system (recommended)**, **Enable ESET LiveGrid® feedback system**, and **Enable ESET LiveGuard**.
5. To modify the default ESET LiveGuard Advanced settings, click ESET LiveGuard, and adjust the available options. For more information on those ESET LiveGuard settings, see the table with the heading "Section: ESET LiveGuard Advanced" in the ESET LiveGuard Advanced documentation.
6. Click **Continue** > **Assign** and select the desired group of computers to which the policy applies.
7. Click **OK**, and then click **Finish**.

ESET Status Portal

ESET Status Portal displays the current status of ESET cloud services, scheduled outages and past incidents. If you are experiencing an issue with a supported ESET service and do not see it listed in the Status Portal, contact ESET Technical Support.

Monitoring teams verify potential issues internally, and confirmed incidents are posted and updated manually to maintain high credibility and accuracy. Therefore, they appear on the Status Portal with a slight delay. Incidents with a short duration may not be posted if they are resolved before being manually confirmed.

Malware scans

This section provides options to select scan parameters for **On-demand scan**.

Selected profile

A specific set of parameters used by the On-demand scanner. You can use one of the pre-defined scan profiles or create a new profile. The scan profiles use different ThreatSense engine parameters.

List of profiles

To create a new one, click **Edit**. Type name for profile and click **Add**. New profile will be displayed in the **Selected profile** drop-down menu that lists existing scan profiles.

On-demand & Machine learning protection

Scanner settings can be configured separately for the real-time scanner and the on-demand scanner. By default, **Use real-time protection settings** is enabled. When enabled, relevant On-demand scan settings are inherited from the **Detection responses** section.

Update

By default, the **Update type** is set to **Regular update**. This ensures the detection signature database and product modules are updated automatically daily from ESET update servers.

Pre-release updates include the most recent bug fixes and detection methods available to the general public soon. However, they might not be stable at all times; therefore, it is not recommended to use them in a production environment.

Delayed updates allow updating from special update servers providing new versions of virus databases with a delay of at least X hours (that is, databases tested in a real environment and considered stable).

If an ESET Endpoint Antivirus for Linux update was not stable, roll back the module updates to a previous state. Execute the appropriate command from a Terminal window, or roll back using ESET PROTECT.

You can define up to two alternative update sources, a primary and secondary server.

By default, only one snapshot of modules is stored locally. To store more snapshots, increase the **Number of locally stored snapshots** to the desired number.

Product Update

By default, ESET Endpoint Antivirus for Linux (EEAU) does not update product components automatically.

Activate automatic updates in EEAU version 9.1 and later:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Click **Update** and click the toggle next to **Auto-updates**.
4. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

5. Click **OK**, then click **Finish**.

Activate automatic updates in EEAU version 9.0 and earlier:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Click **Update** and select **Auto-update** from the **Update mode** list-box.
4. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.
5. Click **OK**, then click **Finish**.

Update mode

Auto-update—new packages are automatically downloaded and then installed after the next restart of OS. If there have been updates to the End User License Agreement, the user must accept the updated End User License Agreement before downloading the new package.

Never-update—new packages are not downloaded, but the product displays the availability of new packages in the **Dashboard**.

Custom server, Username, Password

If you manage several EEAU instances and prefer update from a custom location, define the address and applicable access credentials of an HTTP(S) server, local drive, or removable drive.

Protections

Protections guard against malicious system attacks by controlling files, devices and internet communications. For example, remediation will start if an object classified as malware is detected. Protections can eliminate it by blocking it and then cleaning, deleting or moving it to quarantine.

Detection responses

You can configure Reporting and Protection levels of the following categories:

- **Malware detections (powered by machine learning)**—A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with the machine learning component.
  Read more about these types of applications in the Glossary.

- **Potentially unwanted applications**—Grayware or Potentially Unwanted Applications (PUAs) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. However, it could install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user.
  Read more about these types of applications in the Glossary.

• **Suspicious applications**—Include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

• **Potentially unsafe applications**—Refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications (PUAs) include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). Read more about these types of applications in the Glossary.

Reporting

Reporting is performed by the detection engine and machine learning component. You can customize the reporting threshold to fit your environment and needs. We recommend that you monitor the behavior within your environment and decide whether a different Reporting setting is more suitable. These reporting settings do not influence blocking, cleaning or deleting objects.

Aggressive	Reporting configured to maximum sensitivity. More detections are reported. The **Aggressive** setting can falsely identify objects as malicious, and action will be taken with such objects (depending on Protection settings).
Balanced	This setting is an optimal balance between performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	Reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches malicious behavior.
Off	Reporting is not active. Detections are not found, reported or cleaned. Off is not available for malware reporting and it is default value for potentially unwanted and unsafe applications.

Protection

If an object is reported, the program blocks the object and then cleans, deletes or moves it to Quarantine.

Aggressive	Reported aggressive (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started. This setting is recommended when all endpoints have been scanned with aggressive settings and falsely reported objects have been added to detection exclusions.
Balanced	Reported balanced (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Cautious	Reported cautious level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Off	Useful to identify and exclude falsely reported objects. Off is not available for malware protection and it is default value for potentially unwanted and unsafe applications.

Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning.

> Real-time file system protection does not scan the content of archive files. It scans the content of certain self-extracting archives when downloaded to the hard drive.

In exceptional cases (for example, if there is a conflict with another real-time scanner), real-time protection can

be disabled:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Click **Protections** > **Real-time file system protection**.
4. Disable **Enable Real-time file system protection**.
5. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.
6. Click **OK**, then click **Finish**.

Media to scan

By default, all types of media are scanned for potential threats:

- **Local drives**—Controls all system hard drives.
- **Removable media**—Controls CD/DVD's, USB storage, Bluetooth devices, etc.
- **Network drives**—Scans all mapped drives.

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

Scan on

By default, all files are scanned after opening, creation, or execution. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open**—Enables or disables scanning when files are opened.
- **File creation**—Enables or disables scanning when files are created.
- **Removable media access**—Enables or disables automatic scan of removable media when connecting to the computer.

Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Using ThreatSense technology detection methods (as described in the section of ThreatSense parameters), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to more closely monitor newly created files.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless modified). Files are scanned again immediately after each detection engine database update. This behavior is controlled using **Smart optimization**. If **Smart optimization** is disabled, all files are scanned each time they are accessed. To modify this setting, use ESET PROTECT:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.

3. Click **Protections** > **Real-time file system protection** > **ThreatSense parameters**.

4. Enable or disable **Enable Smart optimization**.

5. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

6. Click **OK**, then click **Finish**.

ThreatSense parameters

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also protects during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures, and virus signatures which work in unity to enhance system security significantly. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

Use ESET PROTECT to alter the configuration. Select one of the modules mentioned below, click **ThreatSense parameters**. Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- **Real-time file system protection**
- **Malware scans**
- **Remote scanning**
- **Web access protection**

ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to scan runtime packers always or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (usually, only newly-created files are scanned using these methods).

Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

- **Boot sectors/UEFI**—Scans boot sectors/UEFI for the presence of viruses in the master boot record
- **Email files**—The program supports the following extensions: DBX (Outlook Express) and EML
- **Archives**—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others

- **Self-extracting archives**—Self-extracting archives (SFX) are archives that can extract themselves

- **Runtime packers**—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner can recognize several additional types of packers through the use of code emulation

> Real-time file system protection does not scan the content of archive files. It scans the content of certain self-extracting archives when downloaded to the hard drive.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

- **Heuristics**—A heuristic is an algorithm that analyzes the (malicious) activity of programs.This technology's main advantage is identifying malicious software that did not exist or was not covered by the previous virus signatures database. The disadvantage is a (tiny) probability of false alarms

- **Advanced heuristics/DNA signatures**—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses, and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses)

Exclusions

An extension is the part of a filename delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup allows you define the file types to be excluded from scan.

Other

When configuring ThreatSense engine parameters setup for an On-demand computer scan, the following options in the **Other** section are also available:

- **Run background scans with low priority**—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications

- **Enable Smart optimization**—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, using different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific modules are applied when performing a scan.

- **Preserve last access timestamp**—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems)

Limits

The **Limits** section allows you to specify the maximum size of objects and nested archives' levels to be scanned.

Object settings

To modify object settings, disable **Default object settings**.

- **Maximum object size**—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited

- **Maximum scan time for object (sec.)**—Defines the maximum time value for scanning an object. If a user-defined value has been typed here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: unlimited

Archive scan setup

To modify archive scan settings, disable **Default archive scan settings**.

- **Archive nesting level**—Specifies the maximum depth of archive scanning. Default value: 10

- **Maximum size of file in archive**—This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: unlimited

> **Default values**
> We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

Additional ThreatSense parameters

The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Advanced heuristics, which can detect new threats before module update is released, are also used along with standard signature-based scanning methods. In addition to newly-created files, scanning is performed on self-extracting archives (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable **Default archive scan settings**.

Web access protection

Web access protection scans HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) communication between web browsers and remote servers.

Access to web pages known to contain malicious content is blocked before the content is downloaded. All other web pages are scanned by the ThreatSense scanning engine when loaded and blocked if malicious content is detected. Web access protection offers two levels of protection, blocking by the blacklist and blocking by the content.

Enable Web access protection—Monitors HTTP and HTTPS communication between web browsers and remote servers. Enabled by default, we strongly recommend that Web access protection is enabled.

Excluded applications—Click edit to exclude communications for specific network-aware applications from protocol filtering.

Excluded IPs—Click edit to exclude IP addresses from protocol content filtering.

Web access protection supports following VPNs:

- OpenVPN
- PulseSecure
- Wireguard
- ProtonVPN

> Currently Web access protection supports only HTTP proxy when it is explicitly configured in ESET Endpoint Antivirus for Linux. System and HTTPS proxies are not supported.

URL address management

The URL address management enables you to specify URL addresses to block, allow or exclude from checking. Websites in the list of **Blocked** addresses are not accessible unless they are also included in the list of **Allowed** addresses. Websites in the list of **Found malware is ignored** addresses are accessed without being scanned for malicious code.

If you want to block all HTTP addresses except addresses present in the active list of **Allowed** addresses, add * to the active list of **Blocked** addresses.

You can use the special symbols "*" (asterisk) and "?" (question mark) when building addresses lists. The asterisk substitutes any character string, and the question mark substitutes any symbol.

Pay attention when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, ensure that the symbols * and ? are used correctly in this list.

To activate a list, select **List active**. If you want to be notified when entering an address from the current list, select **Notify when applying**. See URL address management for detailed information.

HTTPS traffic scanning

HTTPS traffic scanning enables you to check for threats in communication that use the SSL and TLS protocols. You can use different scanning modes to examine SSL-protected communication with trusted certificates, unknown certificates, or certificates excluded from SSL-protected communication checking. The program will only scan traffic on ports (443, 0–65535) defined in **Ports used by the HTTPS protocol**. See HTTPS traffic scanning for detailed information.

ThreatSense parameters

ThreatSense parameters enable you to configure settings for the web access protection, such as types of objects to scan, scan options, etc. See ThreatSense parameters for detailed information.

Excluded applications

Use it to exclude communications for specific network-aware applications from protocol filtering. HTTP/POP3/IMAP communication for the selected applications will not be scanned for threats. We recommend only using this technique when applications do not function properly with protocol filtering enabled.

To exclude application from scanning:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Navigate to **Protections** > **Web access protection** and click **Edit** next to **Excluded applications**.
4. Click **Add**, define the **Path** to be skipped by the scanner.
5. Click **OK**, then click **Save** to close the dialog.
6. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.
7. Click **OK**, then click **Finish**.

Exclusion paths

*/root/** - The "*root*" directory and all of its sub-directories and their content.

/root - The "*root*" file only.

/root/file.txt - The file.txt in "*root*" directory only.

> **Wildcards in the middle of a path are not supported**
> Do not use wildcards in the middle of a path (for example */home/user/*/data/file.dat*). ESET Endpoint Antivirus for Linux does not support it.

Excluded IPs

Use it to exclude IP addresses from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected IP addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

To exclude IP address from scanning:

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Navigate to **Protections** > **Web access protection** and click **Edit** next to **Excluded IP addresses**.

3. Click **Add** and type the IP address to exclude. To define several IP addresses at once, click **Enter multiple values**, and type the desired IP addresses separated by a new line or another separator you selected.

4. Click **OK**, then click **Save** to close the dialog.

5. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.

6. Click **OK**, then click **Finish**.

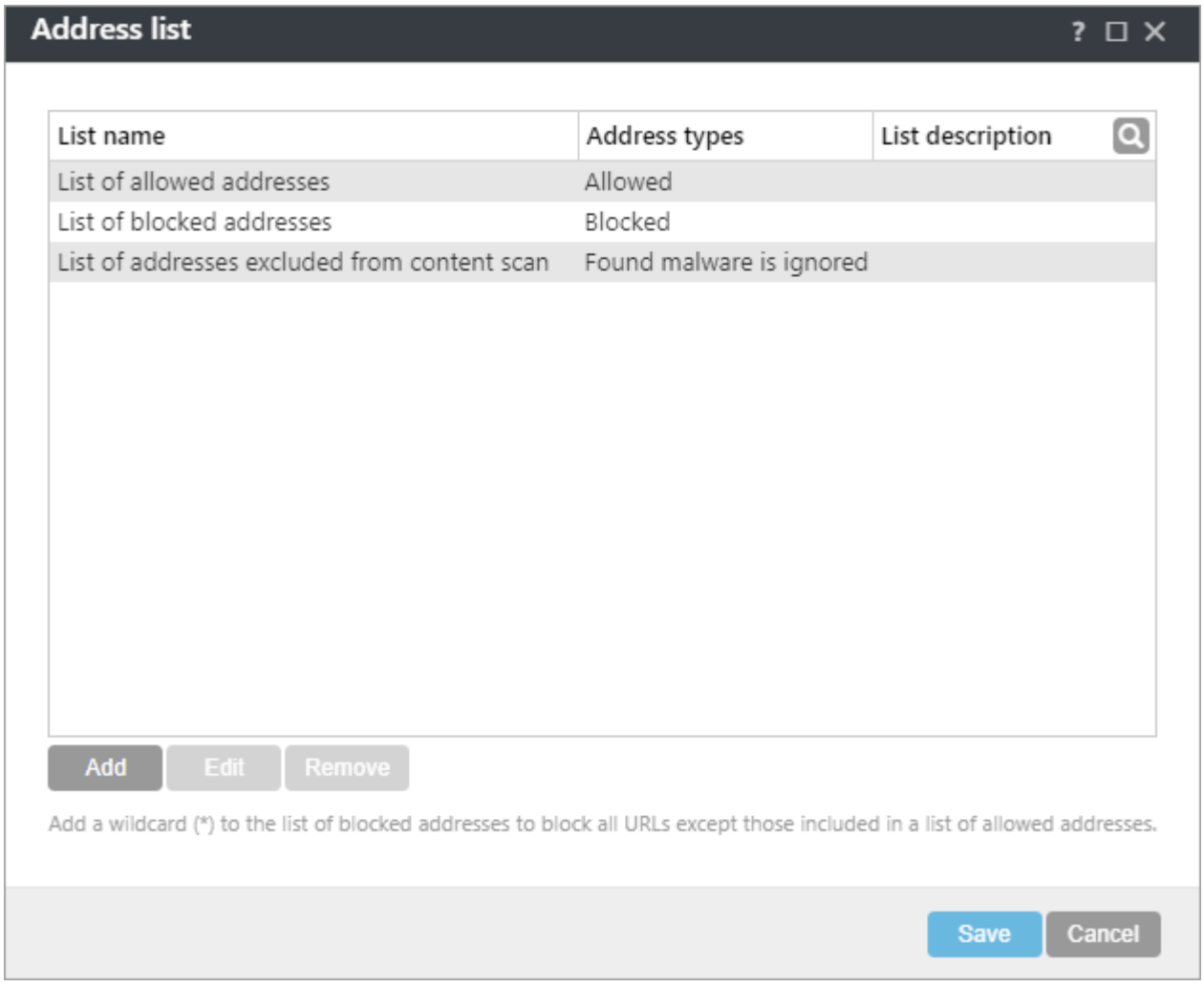
IP addresses examples

Add IPv4 address:
Single address—Adds an IP address of an individual computer, for example, 192.168.1.100.
Address range—Type the starting and ending IP addresses to specify the IP range of multiple computers, for example, 192.168.1.1-192.168.1.99.
Subnet—Subnet (a group of computers) defined by an IP address and mask. For example, 255.255.255.0 is the network mask for the 192.168.1.0 subnet, and to exclude the whole subnet type in 192.168.1.0/24.

Add IPv6 address:
Single address—Adds the IP address of an individual computer, for example, ::ffff:c0a8:164.
Subnet—Subnet (a group of computers) defined by an IP address and mask, for example, ::ffff:c0a8:100/64.

URL address management

In this section you can specify lists of HTTP addresses that will be blocked, allowed or excluded from checking.



By default, the following lists are available:

- **List of allowed addresses**—If the list of blocked addresses contains * (match everything) only addresses specified in this list can be accessed.

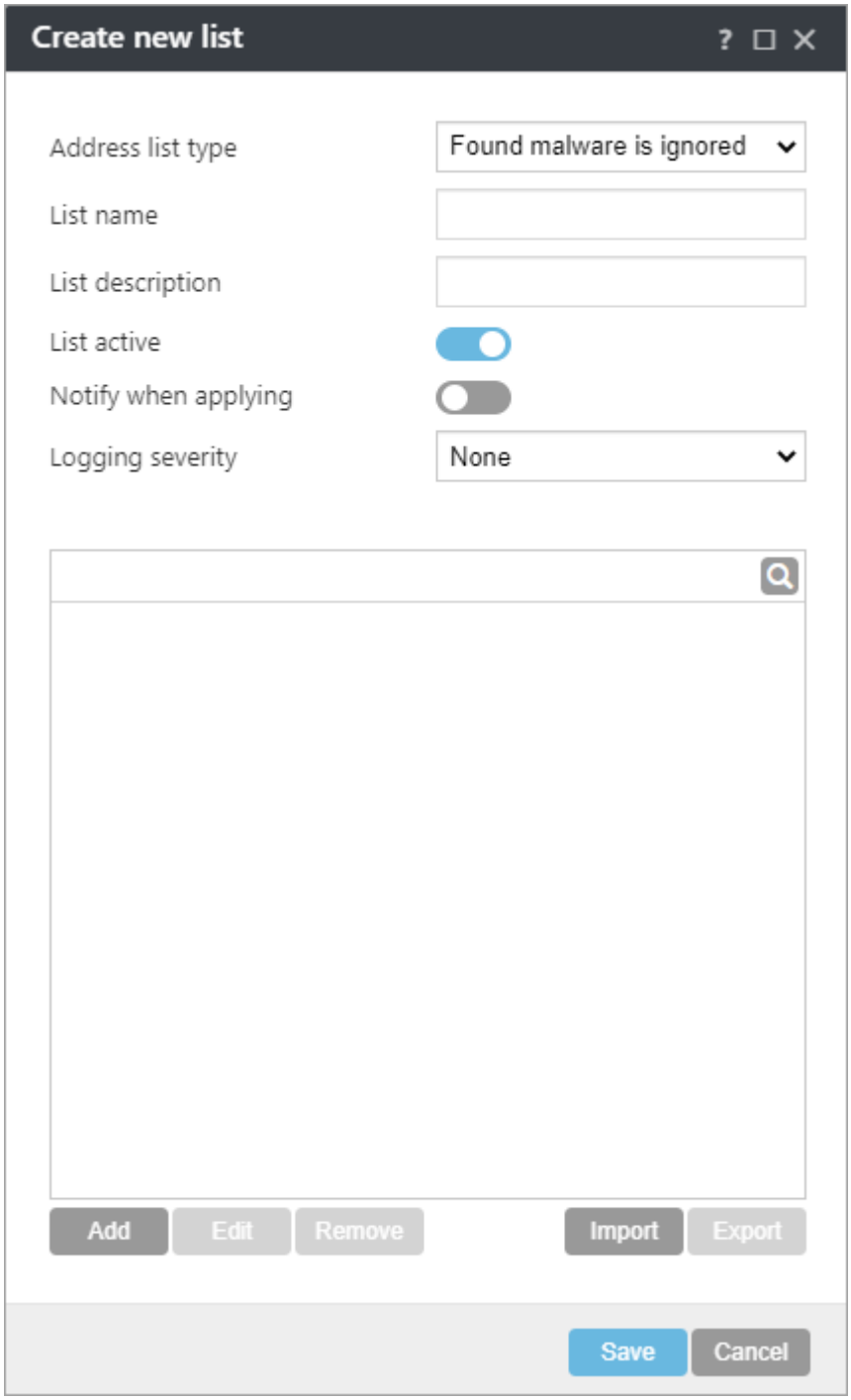
- **List of blocked addresses**—Access to the addresses specified in this list will not be allowed unless the addresses occur in the list of allowed addresses.

- **List of addresses excluded from content scan**—Addresses are accessed without being scanned for malicious code.

Click **Add** to create a new list. To delete selected list, click **Remove**.

Create new list

This dialog window enables you to configure a new list of URL addresses/masks that will be blocked, allowed or excluded from checking.



Address list type

Choose the address list type from the drop-down menu:

- **Found malware is ignored**—No checking for malicious code will be performed for any address added to this list.
- **Blocked**—Access to addresses specified in this list will be blocked.
- **Allowed**—Access to addresses specified in this list will be allowed. Addresses in this list are allowed even if they match the list of blocked addresses.

List name—Specify the name of the list. This field is not editable for pre-defined lists.

List description—Type the description of the list for better identification. This field is not editable for pre-defined lists.

Click the toggle next to **List active** to disable or enable this list. This can be useful if you do not want to delete the list permanetly.

Click the toggle next to **Notify when applying** to get notification when a specific list is used to access websites. For example, you will receive a notification when a website is blocked or allowed because it is included in list of blocked or allowed addresses. The notification will contain the name of the list.

Logging severity

Choose the logging severity from the drop-down menu:

- **None**—No messages are recorded.
- **Diagnostic**—Records diagnostic messages, including connection information with PID and path.
- **Information**—Records informative messages and sends them to ESET PROTECT.
- **Warning**—Records critical errors and warning messages and sends them to ESET PROTECT.

Information and Warning logging verbosity is available only for rules which contain at least two components without wildcards within the domain. For example:
- *.domain.com/*
- *www.domain.com/*

Control elements

- **Add**—Add a new URL address to the list. To define several URL addresses at once, click **Enter multiple values**, and type the desired URL addresses separated by a new line or another separator you selected.
- **Edit**—Modifies existing address in the list.
- **Remove**—Deletes existing address in the list.
- **Import**—Import a file with URL addresses (separate values with a line break, for example, *.*TXT* using encoding UTF-8)

URL masks

You can use masks, if the complete name of the remote server is unknown, or you want to specify a whole group of remote servers. The masks include the symbols "?" and "*":

- use ? to substitute a symbol
- use * to substitute a text string

For example *.?u applies to all addresses, where the last part ends with the letter u and contains an unknown symbol (.eu, .au, etc.).

For example *o? denotes any address with o as the last but one character.

To match the whole domain, type it in the form *.domain.com/*. Specifying protocol prefix *http://*, *https://* in the mask is optional.

To define several URL masks at once, click **Enter multiple values**, and type the desired URL masks separated by a new line or another separator you selected.

HTTPS traffic scanning

ESET Endpoint Antivirus for Linux can check for threats in communication that use the SSL and TLS protocols. You can use different scanning modes to examine SSL-protected communication with trusted certificates, unknown certificates, or certificates excluded from SSL-protected communication checking. The program will only scan traffic on ports (443, 0–65535) defined in **Ports used by the HTTPS protocol**.

Enable SSL/TLS—SSL/TLS protocol filtering is enabled by default.

SSL/TLS mode—You can choose from 2 options:

- **Policy mode**—All SSL/TLS connections are filtered, except configured exclusions.
- **Automatic mode**—Only SSL/TLS connections supported below are filtered, except configured exclusions.

Automatic mode SSL/TLS supports the following browsers and applications:

- Edge
- Firefox
- Chrome
- Chromium

- wget
- curl

> Browser or application needs to be installed by default distribution package manager. Initial start is necessary for browsers integration.

Application scan rules—Create a list of SSL/TLS filtered applications to customize ESET Endpoint Antivirus for Linux behavior for specific applications.

Certificate rules—Create a list of known certificates to customize ESET Endpoint Antivirus for Linux behavior for specific SSL certificates.

Do not scan traffic with domains trusted by ESET—When enabled, communication with trusted domains will be excluded from checking. The trustworthiness of a domain is determined by a built-in whitelist.

Block traffic encrypted by obsolete SSL—Communication using an earlier version of the SSL protocol will be blocked automatically.

Ports used by HTTPS protocol—Specifies the ports to scan traffic. Multiple port numbers must be delimited by a comma. Default value: 443, 0-65535

Root certificate

For SSL/TLS communication to work properly in the supported applications, the ESET root certificate is automatically added to the list of known root certificates (publishers).

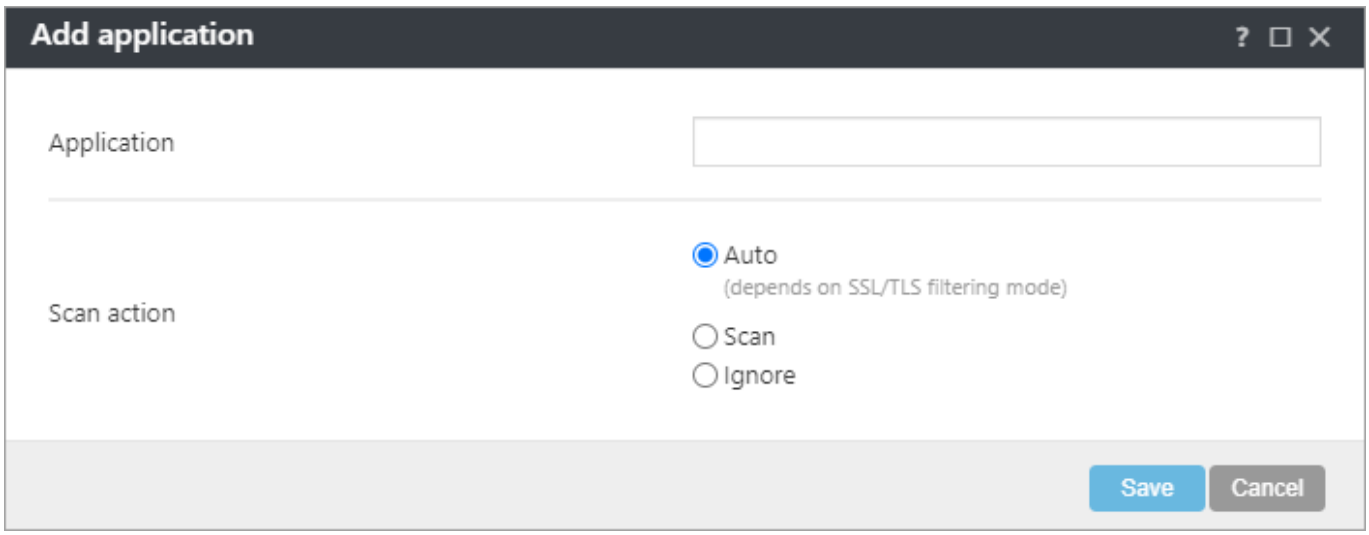
Certificate validity

If the certificate trust cannot be established—In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store. This means that the certificate is signed by someone (for example, the administrator of a web server or a small business) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by the TRCA. If **Ask about certificate validity** is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. You can select **Block communication that uses the certificate** to always terminate encrypted connections to sites with unverified certificates.

List of SSL/TLS filtered applications

The **List of SSL/TLS filtered applications** can be used to customize ESET Endpoint Antivirus for Linux behavior for specific applications.

Click **Add** to customize behavior for specific application. **Add application** window contains:



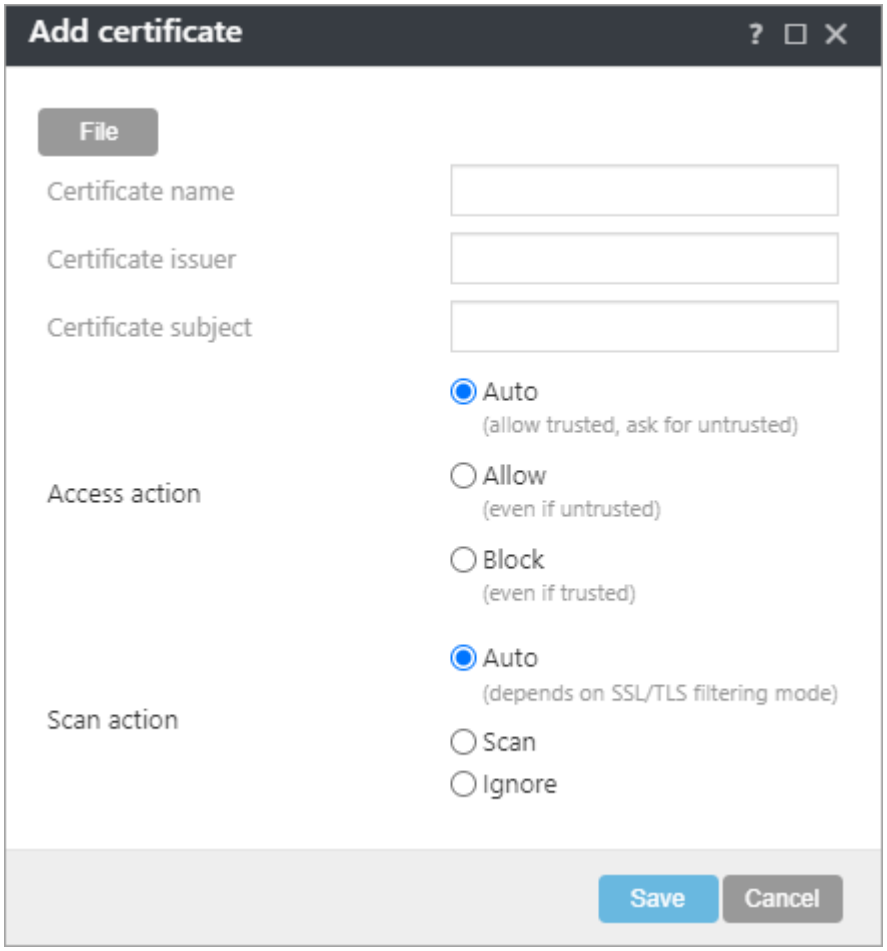
Application—Type exact path to application.

Scan action

- **Auto**—Scans in automatic mode.
- **Scan or Ignore**—Scans/Ignores communication secured by this application.

List of known certificates

The **List of known certificates** can be used to customize ESET Endpoint Antivirus for Linux behavior for specific SSL certificates.



When you are in **Add certificate** window, click **File** to browse for a certificate file. The following fields will automatically be filled using data from the certificate:

- **Certificate name**—Name of the certificate.
- **Certificate issuer**—Name of the certificate creator.
- **Certificate subject**—The subject field identifies the entity associated with the public key stored in the subject public key field.

Access action

- **Auto**—Allows trusted certificates and asks for untrusted ones.
- **Allow or Block**—Allows/Blocks communication secured by this certificate regardless of its trustworthiness.

Scan action

- **Auto**—Scans in automatic mode.

- **Scan or Ignore**—Scans/Ignores communication secured by this certificate.

Setting scan action to **Ignore** overrides access action **Block**.

Network access protection

Since version 10.2, ESET Endpoint Antivirus for Linux supports Botnet Protection.

Enable Botnet protection—Detects and blocks communication with malicious command and control servers based on typical patterns when the computer is infected and a bot is attempting to communicate. Requires web access protection to be enabled. Read more about Botnet Protection in the Glossary.

Device control

ESET Endpoint Antivirus for Linux provides automatic device (CD/DVD/USB/...) control. This module allows you to block or adjust extended filters/permissions and define a user's ability to access and work with a given device. This is useful if the computer administrator wants to prevent the use of devices containing unsolicited content.

Possible file-system damage
Applying a policy with block/read-only action on already connected devices while writing/reading data is in progress may damage their file system because they are forcibly unmounted.

Replace policy
If multiple device control rule policies are applied on an EEAU instance, the last applied policy replaces previous policies' rules.

Supported external devices:

- Storage devices connected via USB
- Internal CD/DVD drives

Device control can be turned on and configured in ESET PROTECT from the Policies section.

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Navigate to **Protections** > **Device Control**.
4. Click the toggle next to **Integrate into system**.
5. To configure Rules and Groups, click **Edit** next to the respective item.
6. Navigate to **Assign**, click **Assign**, select the desired group of computers.

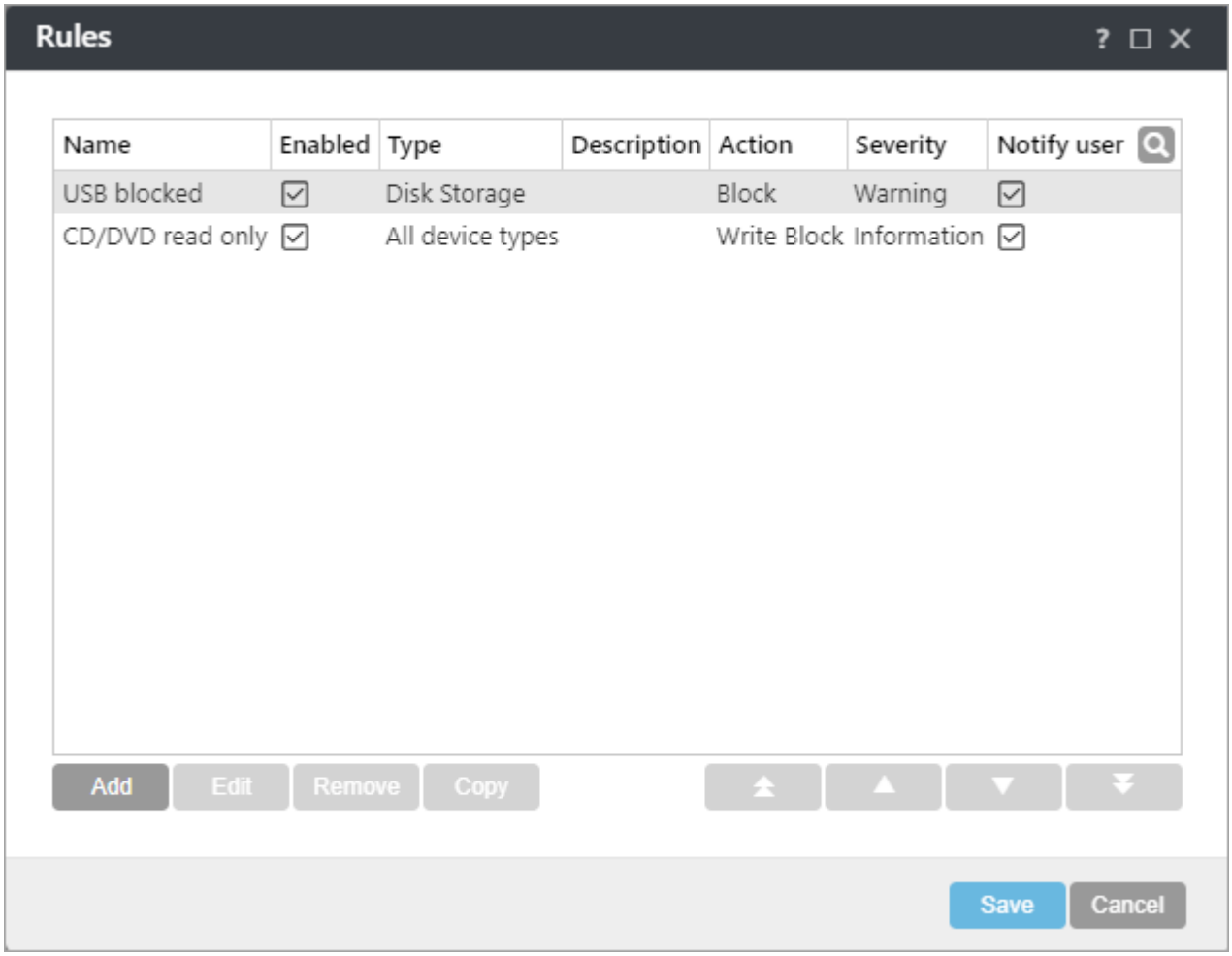
7. Click **OK**, then **Finish**.

See more information on managing endpoint security products from ESET PROTECT.

If a device blocked by an existing rule is connected/inserted, a notification window will be displayed, and access to the device will not be granted.

Device control rules editor

The **Device control rules editor** window in ESET PROTECT displays existing rules and allows for precise control of supported external devices that users connect to the computer.



Specific devices can be allowed or blocked based on defined parameters in the rule configuration. The list of rules contains several rule descriptions such as name, type of external device, and action to perform after connecting an external device to your computer.

Click **Add** or **Edit** to manage a rule. Deselect the **Enabled** check box next to a rule to disable it until you want to use it in the future. Select one or more rules and click **Remove** to delete the rule(s) permanently.

Click **Copy** to create a copy of the selected rule.

Rules are listed in order of priority, with higher-priority rules closer to the top. Move rules individually or in groups by clicking the Top/Up/Down/Bottom buttons.

The Device control log records all occurrences where Device control is triggered.

Attributes of connected devices

To list the attributes of devices connected to the computer where ESET Endpoint Antivirus for Linux is installed, use the `lsdev` utility from a Terminal window, or execute it from ESET PROTECT.

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

Options - short form	Options - long form	Description
`-l`	`--list`	Display a list of connected devices
`-c`	`--csv`	Use csv format to display a list of connected devices
`-h`	`--help`	Show help and quit
`-v`	`--version`	Show version information and quit

Device groups

The Device groups window is divided into two parts. The right part of the window contains a list of devices belonging to the respective group, and the left part of the window contains created groups. Select a group with a list of devices you want to display in the right pane.

When you open the **Device groups** window and select a group, you can add or remove devices from the list. Another way to add devices to the group is to import them from a file.

Control elements

Add—Add a group by entering its name or a device to the existing group (optionally, you can specify details such as vendor name, model, and serial number).

Edit—Modify the name of a selected group or device's parameters (vendor, model, serial number).

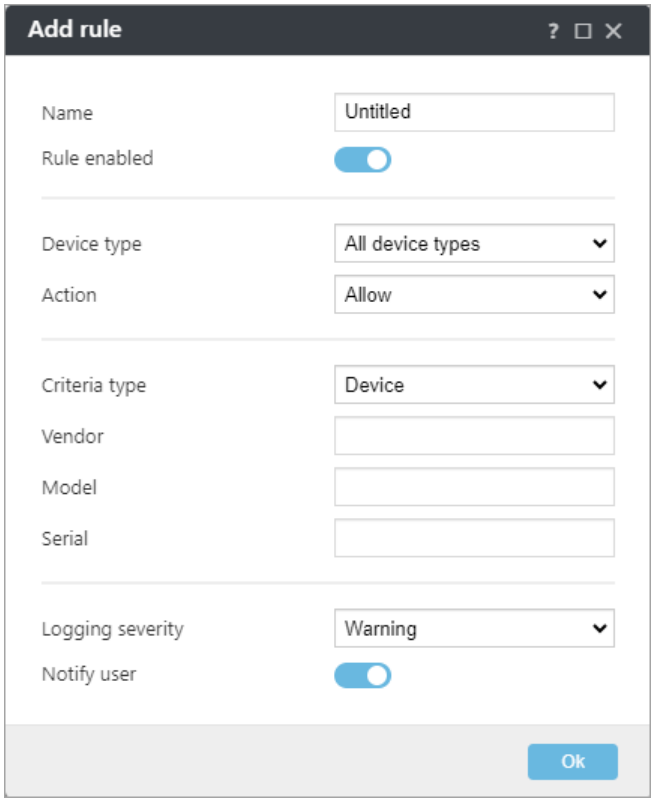
Remove—Delete a selected group or device.

Import—Import a list of devices from a file.

When you are done with customization, click **OK**. Click **Cancel** if you want to leave the **Device groups** window without saving changes.

Adding Device control rules

A Device control rule defines the action taken when a device, meeting the rule criteria, is connected to the computer.



Type a description of the rule into the **Name** field for better identification. Click the toggle next to **Rule enabled** to disable or enable this rule; this can be useful if you do not want to delete the rule permanently.

Device type

Choose the external device type from the drop-down menu:

- **Disk storage**—Applies to any disk storage connected via USB, including external CD/DVD drives and conventional memory card readers
- **CD/DVD**—Applies to internal CD/DVD drive connected via IDE or SATA
- **All device types**—Includes all types above

Device type information is collected from the operating system. Use the lsdev utility to list connected devices and their attributes.

Because these devices only provide information about their actions and do not provide information about users, they can be blocked globally only.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices allow you to select one of the following rights settings:

- **Allow**—Full access to the device
- **Block**—Access to the device is blocked
- **Write Block**—Only read access to the device

For **Criteria type**, select **Device** or **Device group**.

Additional parameters shown below can be used to fine-tune rules and tailor them to devices. All parameters are case-insensitive:

- **Vendor**—Filter by vendor name or ID.
- **Model**—The given name of the device.
- **Serial**—External devices usually have their serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

> **Undefined parameters**
> If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-insensitive, and wildcards (*, ?) are not supported.

> **Device control logs**
> To view information about a device, create a rule for that type of device, connect the device to your computer and then check the device details using the lslog command-line utility with `-l` or `--device-control` parameter.

Logging Severity

- **Information**—Records informative messages, including successful update messages, plus all records above.
- **Warning**—Records critical errors and warning messages and sends them to ESET PROTECT.

Tools

In the **Tools** section of ESET Endpoint Antivirus for Linux configuration through ESET PROTECT, you can modify the general configuration of ESET Endpoint Antivirus for Linux.

- Define the details of a Proxy server to connect to the internet
- Configure how log files are handled

Proxy Server

Configure ESET Endpoint Antivirus for Linux to use your proxy server to connect to the internet or the defined update servers (mirror). To adjust parameters, click **Setup** > **Tools** > **Proxy server**.

Log files

Modify the configuration of ESET Endpoint Antivirus for Linux logging.

Minimum logging verbosity

Logging verbosity defines the level of details the log files include regarding ESET Endpoint Antivirus for Linux.

- **Critical warnings**—Includes only critical errors (for example, failed to start antivirus protection).
- **Errors**—Errors such as "Error downloading file" will be recorded in addition to **critical warnings**.
- **Warnings**—Critical errors and warning messages will be recorded in addition to **errors**.
- **Informative records**—Record informative messages, including successful update messages, plus all records above.
- **Diagnostic records**—Include information needed to fine-tune the program and all records above.

Automatically delete records older than (days)

To hide log entries older than the specified number of days from the log list (`lslog`):

1. In ESET PROTECT, click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Click **Tools** > **Log files**.
4. Enable **Automatically delete records older than (days)**.
5. Adjust the day to specify the age of files to be hidden.
6. Click **Continue** > **Assign**, select the desired group of computers the policy will apply to.
7. Click **OK**, then click **Finish**.

Hidden logs cannot be displayed again. Log entries of On-demand scan are deleted right away. To prevent piling up of hidden logs, turn on the automatic optimization of log files.

Optimize log files automatically

When engaged, log files will be defragmented automatically if the fragmentation percentage is higher than the value specified in the **If the number of unused records exceeds (%)** field. Unused records stand for hidden logs. Click **Optimize** to begin defragmenting the log files. All empty log entries are removed to improve performance and log processing speed. This improvement can be observed, especially if the logs contain a large number of entries.

Syslog Facility

Syslog facility is a syslog logging parameter used to group similar log messages. For example, logs from daemons (which collect logs via syslog facility daemon) can go to */var/log/daemon.log* if configured. With the recent switch to systemd and its journal, syslog facility is less important but still can be used for filtering logs.

User interface

In this section of ESET Endpoint Antivirus for Linux configuration through ESET PROTECT, you can enable/disable desktop notifications, select the actions and application status to be notified about.

Desktop notifications

Turn on/off desktop notifications by switching the toggle next to **Display notifications on desktop**. They are enabled by default. These notifications contain information that does not need your intervention.

Configure the actions to be notified about:

1. Click **Edit** next to **Application notifications**.
2. Select/deselect the desired actions.
3. Click **OK**.

Protection status

Configure which application statuses are reported to ESET Endpoint Antivirus for Linux.

1. Click **Edit** next to Application statuses.
2. Under **Show in Endpoint**, select the desired application status to be notified about.
3. Click **OK**.

Application status

Each selected status at **Application statuses** > **Edit** > **Show in Endpoint** will display a notification in the initial screen of ESET Endpoint Antivirus for Linux and menu ☰ > **Protection status**.

Remote Management

To manage ESET Endpoint Antivirus for Linux remotely, connect the computer hosting your ESET security product to ESET PROTECT.

1. Deploy the ESET Management Agent.
2. Add the computer to ESET PROTECT.

From this time on, you can execute applicable client tasks regarding ESET Endpoint Antivirus for Linux.

Use case examples

This chapter covers common use cases of ESET Endpoint Antivirus for Linux:

- Retrieve module information
- Schedule scan

Retrieve module information

To see a list of all ESET Endpoint Antivirus for Linux modules and their versions, execute the following command from a Terminal window:

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

```
/opt/eset/eea/bin/upd --list-modules
Output:
EM000        1074.1 (20190925)        Update module
EM001        1558.2 (20191218)        Antivirus and antispyware scanner module
EM002         20708 (20200121)        Detection engine
EM003          1296 (20191212)        Archive support module
EM004          1197 (20200116)        Advanced heuristics module
EM005          1205 (20191209)        Cleaner module
EM017          1780 (20191217)        Translation support module
EM022          1110 (20190827)        Database module
EM023         15605 (20200121)        Rapid Response module
EM029          1026 (20191107)        Mac/Linux support module
EM037         1833B (20191125)        Configuration module
```

Schedule scan

In Unix-based systems, use cron to schedule an On-demand scan at a custom period.

To set up a scheduled task, edit the cron table (crontab) via a Terminal window.

If you are editing the cron table for the first time, you will be presented with the option to choose an editor by pressing the corresponding number. Select an editor you have experience with; for example, we refer to the Nano editor below when saving changes.

Schedule an in-depth full disk scan every Sunday at 2 am

1. To edit the cron table, execute the following command from a Terminal window as a privileged user who can access the folders to be scanned:

```
sudo crontab -e
```

2. Use the arrow keys to navigate below the text in crontab, and type the following command:

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

3. To save changes, press CTRL+X, type Y, and press **Enter**.

Schedule smart scan of a specific folder every night at 11 pm

In this example, we schedule to scan the */var/www/download/* folder every night.

1. To edit the cron table, execute the following command from a Terminal window as a privileged user who can access the folders to be scanned:

```
sudo crontab -e
```

2. Use the arrow keys to navigate below the text you see in crontab, and type the following command:

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

3. To save changes, press CTRL+X, type Y, and press **Enter**.

File and folder structure

File and folder structure

This topic details the file and folder structure of ESET Endpoint Antivirus for Linux, if ESET Technical Support asked you to access files for troubleshooting purposes. The list of daemons and command-line utilities is available to further below.

Base directory

The directory where ESET Endpoint Antivirus for Linux loadable modules containing the virus signature database are stored.

```
/var/opt/eset/eea/lib
```

Cache directory

The directory where cache of ESET Endpoint Antivirus for Linux and temporary files (such as quarantine files or reports) are stored.

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

Binary files directory

The directory where the relevant ESET Endpoint Antivirus for Linux binary files are stored.

```
/opt/eset/eea/bin
```

There you find the following utilities:

- lsdev—use it to list the attributes of devices connected to the computer
- odscan—use it to run on-demand scan via a Terminal window
- quar—use it to manage quarantined items
- upd—use it to manage module updates or to modify update settings

System binary files directory

The directory where the relevant ESET Endpoint Antivirus for Linux system binary files are stored.

```
/opt/eset/eea/sbin
```

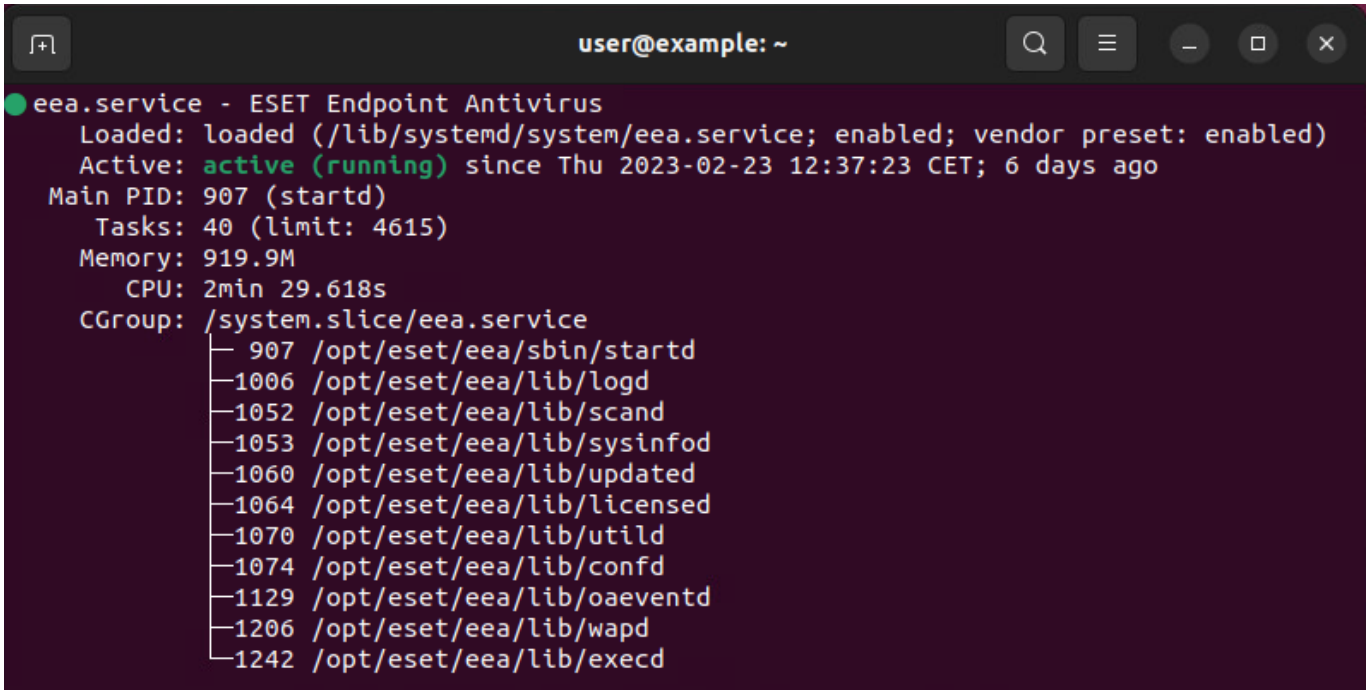
There you find the following utilities:

- collect_logs.sh—use it to generate all essential logs as an archive file to the home folder of being logged in user
- ecp_logging.sh—use it to generate logs related to product activation.
- lic—use it to activate ESET Endpoint Antivirus for Linux with the purchased license key or to check the activation status and license validity
- lslog—use it to display logs gathered by ESET Endpoint Antivirus for Linux
- startd—use it to start ESET Endpoint Antivirus for Linux daemon manually if it was stopped

To see if ESET Endpoint Antivirus for Linux service is active, run the following command from a Terminal window with root privileges:

```
systemctl status eea.service
```

Sample output from `systemctl`:



Daemons

- sbin/startd—Main daemon, starts and manages other daemons
- lib/scand—Scanning daemon
- lib/oaeventd—On-access event interception service (using eset_rtp kernel module)
- lib/confd—Configuration management service
- lib/logd—Logs management service
- lib/licensed—Activation and licensing service
- lib/updated—Module update service
- lib/execd + lib/odfeeder—On-demand scanning helpers
- lib/utild—Utility service
- lib/sysinfod—OS and media detection service
- lib/wapd—Web access protection service

Command-line utilities

- sbin/lslog—Logs listing utility
- bin/odscan—On-demand scanner
- lib/cfg—Configuration utility

- sbin/lic—Licensing utility
- bin/upd—Module update utility
- bin/quar—Quarantine management utility

Troubleshooting

This section describes how to troubleshoot the various issues below.

- Activation issues (English only)
- Collect logs
- Using the noexec flag
- Realtime protection cannot start
- NFS mount fails
- Using WireGuard with Web access protection

Collect logs

If ESET Technical Support requests logs from ESET Endpoint Antivirus for Linux, use the *collect_logs.sh* script available at */opt/eset/eea/sbin/* to generate the logs.

Launch the script from a terminal window with root privileges. For example, in Ubuntu, run the following command:

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

The script generates all essential logs as an archive file to the home folder of being logged-in user, and it will display the path to it. It also collects activation logs if available. Send that file to ESET Technical Support via email.

Activation logs

To help you troubleshoot product activation issues, related logs might be requested by ESET Technical Support.

1. Enable activation log service by executing the following command as a privileged user:

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

alternatively

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

to restart the product if essential without any prompt.

2. Try the activation process again. If it fails, run the log collecting script as a privileged user:

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

3. Send the collected logs to ESET Technical Support.

4. Disable activation logs by executing the following command as a privileged user:

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

alternatively

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

to restart the product if essential without any prompt.

Installation logs

To help you troubleshoot product installation issues, you might be requested by ESET Technical Support to send in related logs and information.

1. Copy the complete output from the terminal of the running installer.

2. To copy exact information about the version of the operating system and distribution, execute the following command from a Terminal window as a privileged user:

```
lsb_release -a
```

alternatively

```
hostnamectl
```

3. To copy exact information about the kernel, execute the following command from a Terminal window as a privileged user:

```
dmesg | grep Linux
```

alternatively

```
yum list kernel-*
```

4. To copy exact information about the hardware, execute the following command from a Terminal window as

a privileged user:

```
lshw
```

5. Collect log files using the info_get.command.

Using the noexec flag

If you have the `/var` and `/tmp` paths mounted with `noexec` flag, the installation of ESET Endpoint Antivirus for Linux fails with the following error message:

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

Workaround

The commands below are executed in a Terminal window.

1. Create a folder where `exec` is enabled with the following owner and permission set:

```
/usr/lib/eea drwxrwxr-x. root eset-eea-daemons
```

2. Execute the following commands:

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

a.If SELinux is enabled, set the context for this folder:

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

3. Compile the essential modules:

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

4. Set `MODMAPDIR` in `/usr/lib/systemd/system/eea.service` by adding a line to the `[Service]` block:

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

5. Reload systemd service configuration:

```
# systemctl daemon-reload
```

6. Restart the eea service:

```
# systemctl restart eea
```

Realtime protection cannot start

There is a sample issue, and a sample solution below demonstrated on Ubuntu.

Issue

Real-time protection is unable to start due to missing kernel files.

In */var/log/messages* an error is displayed regarding ESET Endpoint Antivirus for Linux:

Oct 15 15:42:30 localhost eea: ESET Endpoint Antivirus error: cannot find kernel sources directory for kernel version 3.10.0-957.el7.x86_64

Oct 15 15:42:30 localhost eea: ESET Endpoint Antivirus error: please check if kernel-devel (or linux-headers) package version matches the current kernel version

Oct 15 15:42:30 localhost oaeventd[31471]: ESET Endpoint Antivirus Error: Cannot open file /lib/modules/3.10.0-957.el7.x86_64/eset/eea/eset_rtp.ko: No such file or directory

Solution

Method 1 - requires restart of the operating system

1. Upgrade the packages of your operating system to the latest version. On Ubuntu, execute the following commands from a Terminal window as a privileged user:

```
apt-get update
apt-get upgrade
```

2. Restart the operating system.

Method 2

1. Install the latest kernel-headers on DEB based Linux distributions. On Ubuntu, execute the following commands from a Terminal window as a privileged user:

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

2. Restart the EEA service.

```
systemctl restart eea
```

NFS mount fails

Issue

The technology behind Web access protection breaks the connection to NFS mounts. The NFS server's default configuration expects the client to connect from a port under 1025 (accessible to the root). The connection intercepted by Web access tries to connect from a random port above 1024, resulting in the server's denial.

Workaround

You can avoid denial by changing the NFS mount server configuration to insecure. This allows the client to connect from a random port to the server.

1. On the NFS server machine, open the */etc/exports* file in your text editor as privileged user. In this example we use nano:

```
nano /etc/exports
```

2. Set your shared directory to insecure and save the changes. An example of the NFS shared directory:

```
/srv/nfs-share  10.10.10.10/24(rw,sync,no_subtree_check,no_root_squash,insecure)
```

3. Restart the NFS server. Run the following command as privileged user:

```
systemctl restart nfs-kernel-server
```

Using WireGuard with Web access protection

Issue

Suppose Web Access Protection (WAP) is combined with WireGuard using `wg-quick` from the command line or as a service. In that case, internet connectivity may be lost when both WAP and WireGuard interfaces are enabled. This is caused by a rule added to nftables by `wg-quick`, when an interface is brought up. Assume the interface is wg0, with an IP address *10.10.10.2. T*he rule is added to table *wg-quick-wg0,* chain preraw and looks like this:

```
iifname != "wg0" ip daddr 10.10.10.2 fib saddr type != local drop
```

The purpose of this rule is to provide some protection against configuration issues and malicious packets.

Workaround

On a properly configured and secured system, the nftables rule should not be necessary. Configuring `wg-quick` not to leave that rule in place should fix the connection issues. For example, you can edit the configuration file for the affected interface and, in the *[Interface]* section, add the following `PostUp` action:

```
PostUp = nft flush chain wg-quick-wg0 preraw
```

Note that the `wg-quick-wg0` name applies only to the *"wg0"* interface and has to be changed accordingly for other interfaces. If you still want to get some level of protection in place, you can replace the rule with a weaker one, for example, like this:

```
PostUp = nft flush chain wg-quick-wg0 preraw; nft 'add rule wg-quick-
wg0 preraw iifname != "wg0" iif != "lo" ip daddr 10.10.10.2 fib saddr type != local
drop'
```

Remember that all mentions of "wg0" must be updated if the interface is not "wg0". Also, it is necessary to update the IP address if it is not 10.10.10.2.

Glossary

- **Daemon**: A type of program on Unix-like operating systems that runs unobtrusively in the background. It is activated by the occurrence of a specific event or condition.

See more terms in the ESET glossary

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one

user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_business. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

b) **Forwarding of infiltrations and information to the Provider.** The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames ("Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed and, information about the operations and functionality of the Software ("Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning

copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE

YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any

person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET´s right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between

language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Update and other statistics covering information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product.
- One-way hashes related to infiltrations as part of ESET LiveGrid® Reputation System which improves the efficiency of our anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.
- Suspicious samples and metadata from the wild as part of ESET LiveGrid® Feedback System which enables ESET to react immediately to needs of our end users and keep us responsive to the latest threats providing. We are dependent on You sending us
    - infiltrations such as potential samples of viruses and other malicious programs and suspicious; problematic, potentially unwanted or potentially unsafe objects such as executable files, email messages reported by You

as spam or flagged by our product;

- information about devices in local network such as type, vendor, model and/or name of device;
- information concerning the use of internet such as IP address and geographic information, IP packets, URLs and ethernet frames;
- crash dump files and information contained.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in malware itself (collected without your knowledge or approval) or as part of filenames or URLs and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.
- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject’s Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),

- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk