

# ESET Server Security for Linux

## User guide

[Click here to display the online version of this document](#)

Copyright ©2024 by ESET, spol. s r.o.

ESET Server Security for Linux was developed by ESET, spol. s r.o.

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

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

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

REV. 4/12/2024

1 Introduction .....	1
<b>1.1 Key features of the system</b> .....	1
2 Release notes .....	1
3 System requirements .....	1
<b>3.1 Secure boot</b> .....	4
4 Installation .....	6
<b>4.1 Reinstall</b> .....	7
<b>4.2 Uninstall</b> .....	7
<b>4.3 Mass deployment</b> .....	8
5 Activate ESET Server Security for Linux .....	12
<b>5.1 Where can I find my license</b> .....	14
<b>5.2 Check the activation status</b> .....	14
6 Update, upgrade .....	14
<b>6.1 Update mirror</b> .....	16
<b>6.2 Automatic product updates</b> .....	17
7 Using ESET Server Security for Linux .....	18
<b>7.1 Dashboard</b> .....	20
<b>7.2 Status Overview</b> .....	22
<b>7.3 Scans</b> .....	23
7.3 Run On-demand scan from a Terminal window .....	24
7.3 Exclusions .....	26
7.3 Detection exclusions criteria .....	27
<b>7.4 Detections</b> .....	27
7.4 Quarantine .....	28
<b>7.5 Sent files</b> .....	31
7.5 Submit sample for analysis .....	31
<b>7.6 Events</b> .....	32
<b>7.7 Blocked files</b> .....	33
8 Configuration .....	33
<b>8.1 Detection engine</b> .....	34
8.1 Exclusions .....	35
8.1 Processes exclusions .....	36
8.1 Detection exclusions .....	38
8.1 Add or Edit detection exclusions .....	39
8.1 Real-time file system protection .....	40
8.1 ThreatSense parameters .....	42
8.1 Additional ThreatSense parameters .....	44
8.1 Cloud-based protection .....	44
8.1 Malware scans .....	47
8.1 Remote scanning (ICAP scan) .....	48
8.1 Cleaning levels .....	48
<b>8.2 Update</b> .....	48
<b>8.3 Tools</b> .....	49
8.3 Proxy Server .....	50
8.3 Web interface .....	50
8.3 Listen address and port .....	51
8.3 Log files .....	51
8.3 Scheduler .....	52
<b>8.4 User interface</b> .....	53
8.4 Statuses .....	53

9 Remote management .....	54
10 Container security .....	54
11 Use case examples .....	54
<b>11.1 Secured ICAP with stunnel TLS proxy .....</b>	<b>55</b>
<b>11.2 Integrate ICAP server with EMC Isilon .....</b>	<b>56</b>
<b>11.3 Retrieve module information .....</b>	<b>58</b>
<b>11.4 Schedule scan .....</b>	<b>58</b>
12 File and folder structure .....	59
13 Troubleshooting .....	62
<b>13.1 Collect logs .....</b>	<b>62</b>
<b>13.2 Forgotten password .....</b>	<b>64</b>
<b>13.3 Update failed .....</b>	<b>64</b>
<b>13.4 Using the noexec flag .....</b>	<b>64</b>
<b>13.5 Real-time protection cannot start .....</b>	<b>66</b>
<b>13.6 Disable Real-time protection at boot .....</b>	<b>68</b>
<b>13.7 Outdated curl library for SMB protocol .....</b>	<b>68</b>
<b>13.8 Custom TMPDIR .....</b>	<b>68</b>
14 Glossary .....	69
15 End User License Agreement .....	69
16 Privacy Policy .....	80

# Introduction

ESET's state-of-the-art scanning engine with unsurpassed scanning speed and detection rates combined with a tiny footprint makes ESET Server Security for Linux (ESSL) the ideal choice for any server on Linux.

The main functionality is covered by the On-demand scanner and On-access scanner ([Real-time file system protection](#)).

The On-demand scanner can be started through the command line interface, the web interface, or 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 whenever a user or operating system attempts to access file system objects. Thus a scan is triggered by any attempt to access file system objects.

## Key features of the system

- Automatic product updater
- Redesigned web interface for easy management and overview of security of your system
- On-access scan by ESET's lightweight in-kernel module
- Comprehensive scan logs
- Redesigned, easy-to-use setup page with a search bar
- Quarantine
- Manageable via [ESET PROTECT](#)
- [Cloud-based protection](#)
- [Container security](#)
- [ESET Inspect](#) support

## Release notes

## System requirements

Quick links: [Supported operating systems](#), [Supported browsers](#), [Network prerequisites](#), [Supported filesystems](#)

## Hardware requirements

Hardware requirements depend on the server role. The following minimum hardware requirements are required for installation:

- Processor Intel/AMD x64 with 2 cores
- 2GB of RAM
- 700MB of free hard disk space
- Glibc 2.17 or later
- Linux OS kernel versions 3.10.0 and later
- en\_US.UTF-8 encoding locale

## Supported operating systems

ESET Server Security for Linux (ESSL) has been tested and is supported on the latest minor releases of listed operating systems. Update your operating system before installing ESSL.

64-bit Operating System	Secure Boot supported	Note
RedHat Enterprise Linux (RHEL) 7	✓	
RedHat Enterprise Linux (RHEL) 8	✓	
RedHat Enterprise Linux (RHEL) 9	✓	
CentOS 7	✓	
Ubuntu Server 18.04 LTS	✓	
Ubuntu Server 20.04 LTS	✓	
Ubuntu Server 22.04 LTS	✓	
Debian 10	✓	
Debian 11	✓	
Debian 12	✓	
SUSE Linux Enterprise Server (SLES) 15	✓	
Alma Linux 9	✓	
Oracle Linux 8	✓ (stock kernel only)	If the <a href="#">Unbreakable Enterprise Kernel</a> is used, the <a href="#">kernel-uek-devel</a> package must be installed manually. In this case, Secure Boot is not supported.
Amazon Linux 2		

ESSL should work on the most recent and frequently used open-source Linux distributions if the hardware requirements listed above are met, and software dependencies are not missing in the Linux distribution used.

**i** Linux distributions with [ELREPO](#) kernel and AWS kernel are not supported.  
RHEL with the "Protection Profile for General Purpose Operating Systems (OSPP)" is not supported.

[Remote management via ESET PROTECT.](#)

## Supported browsers

ESSL Web interface works only in the desktop versions of following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

If you experience display issues in ESSL Web interface, ensure that you use the latest version of the browsers listed above.

---

## Network prerequisites

To ensure the proper functioning of the ESET Server Security for Linux allow the network prerequisites listed in the [Knowledgebase article](#).

---

## Supported filesystems

ESET Server Security for Linux (ESSL) has been tested and is supported on the filesystems below:

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			✓

# Secure boot

To use [real-time file system protection](#) on a machine with [Secure boot](#) enabled, the ESET Server Security for Linux (ESSL) kernel module must be signed with a private key. The corresponding public key must be imported to UEFI. ESSL 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 module, Interactive mode can generate new keys and sign the kernel module. It also helps enroll the generated keys in UEFI.

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

```
/opt/eset/efs/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 module 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/efs/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/efs/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 ESSL kernel module on one of those machines containing the private key and then transfer the signed kernel module to the other machines. When the signing is complete:

1. Copy/paste the signed kernel module from `/lib/modules/<kernel-version>/eset/efs/eset_rtp` to the same path on the target machines.
2. Call `depmod <kernel-version>` on the target machines.
3. Restart ESET Server Security for Linux on the target machine to update the modules table. Execute the following command as a privileged user:

```
systemctl restart efs
```

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

# Installation

ESET Server Security for Linux (ESSL) is [distributed as a binary file \(.bin\)](#).



Make sure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system.



## Update your OS

If your [OS is supported](#), ensure it has the most recent updates installed before installation of ESET Server Security for Linux.

## Installer without unnecessary modules

Since version 10, the ESET Server Security for Linux installation package contains only essential modules, reducing its size to 15% of the original size. Due to this change, ESET Server Security for Linux is only partially functional after the installation.



To have a fully functional product, you need to either:

- Use the installer with parameter `-m MIRROR`, which will copy modules from the *MIRROR* directory during installation, for example, created by [MirrorTool](#)
- [Activate ESET Server Security for Linux](#) and download the missing modules

The product is fully functional after the upgrade if the previous version was activated and had all modules.

## Installation via Terminal

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

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

 [See the available command-line arguments](#)

To display the available parameters (arguments) of ESET Server Security for Linux binary file, run the following command from a Terminal window:

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

### Available parameters

Short form	Long form	Description
-h	--help	Display command line arguments
-n	--no-install	Do not install after unpacking
-y	--accept-license	Do not show the license; the license has been accepted
-f	--force-install	Force installation via package manager without asking
-g	--no-gui	Do not setup/start GUI after installation
-u	--unpack-ertp-sources	Unpack 'ESET Real-time file system protection kernel module' sources, do not perform installation
-m		Copy module nups from MIRROR directory

### Gain .deb or .rpm installation package

To gain .deb or .rpm installation package suitable for your OS, run ESET distribution script with "-n"



command line argument:

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

or

```
sudo sh ./efs.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. After you accept the product License Agreement, the installation will complete and displays the [Web interface](#) login details.

The installer would inform you of any dependency problems.

## Installation via ESET PROTECT

To deploy ESET Server Security for Linux remotely on your computers, refer to the [ESET PROTECT Software Install](#) online help section.

If needed, [enable the Web interface remotely](#).

## Activate ESET Server Security for Linux

To enable regular updates of detection modules, [activate ESET Server Security for Linux](#).

### Third-party apps



A summary of third-party apps used by ESET Server Security for Linux can be found in the *NOTICE\_mode* file stored at `/opt/eset/efs/doc/modules_notice/`.

## Reinstall

If the installation breaks for any reason, [rerun the installer](#). Your settings will remain intact.

## 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 efs`
- `dpkg remove efs`

Red Hat based distributions:

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

SUSE based distributions:

- `zypper remove efs`
- `rpm -e efs`

## Mass deployment

This topic provides a high-level overview of mass deployment of ESET Server Security 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 Server Security for Linux, you have to decide which package to use. ESET Server Security 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/efs-8.0.1081.0.x86_64.bin":
    mode => "0700",
    owner => "root",
    group => "root",
    source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.bin"
  ]}
  exec {"Execute bin package installation":
    command => '/tmp/efs-8.0.1081.0.x86_64.bin -y -f'
  }
}
```

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

    file {"/tmp/efs-8.0.1081.0.x86_64.rpm":
      mode => "0700",
      owner => "root",
      group => "root",
      source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.rpm"
    }

    package {"efs":
      ensure => "installed",
      provider => 'rpm',
      source => "/tmp/efs-8.0.1081.0.x86_64.rpm"
    }
  }
}
```

## Chef

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

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

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

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

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

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

# Ansible

## 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: efs-8.0.1084.0.x86_64.bin  
    dest: /home/ansible/  
  
- name : "Install product bin package"  
  shell: bash ./efs-8.0.1084.0.x86_64.bin -y -f -g  
.....
```

## 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: ./efs-8.0.1085.0.x86_64.deb
    dest: /home/ansible/efs-8.0.1085.0.x86_64.deb
    owner: ansible
    mode: a+r
  when:
    - ansible_os_family == "Debian"

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

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

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

## Activate ESET Server Security for Linux

Activate your ESET Server Security for Linux (ESSL) using a [license](#) obtained from your ESET distributor.

### Activate using the Web interface

1. Log in to the [Web interface](#).
2. Click **Status Overview > License**.
3. Select the desired method of activation:
  - [Activate with License Key](#) – For users who purchased an ESET Server Security for Linux License Key.
  - [ESET Business Account](#) – For registered [ESET Business Account \(EBA\)](#) users who have an ESET Server Security for Linux license imported to EBA. Your EBA (or ESET MSP Administrator (EMA)) username and password are required.
  - [Offline license](#) – Use this option if ESET Server Security for Linux cannot connect to the internet and ESSL will be used in an offline environment.



- [ESET management console](#)

If the license expires, you can change the license to a different one at the same location.

## Using EBA or EMA login credentials to activate ESSL

1. Log in to the [Web interface](#).
2. Click **Status Overview** > **License**, and select **ESET Business Account**.
3. Type your EBA or EMA login credentials.
4. If there is only a single ESSL (or ESET File Security for Linux) license in your EBA or EMA account and no sites are created, the activation will complete instantly. Otherwise, you have to select a specific license or a site ([license pool](#)) to active ESSL.
5. Click **Activate**.

## Activate using the Terminal

Use the `/opt/eset/efs/sbin/lic` utility as a privileged user to activate ESET Server Security for Linux from a Terminal window.

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

### Examples

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

#### Activation using a License Key

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

or

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

while XXXX-XXXX-XXXX-XXXX-XXXX represents your ESET Server Security for Linux License Key.

#### Activation using an EBA or EMA account

1. Execute:

```
/opt/eset/efs/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 ESSL license in your EBA or EMA account and no sites are created, the activation will complete instantly. Otherwise, a list of available ESSL licenses and sites ([license pool](#)) will display.



4. Execute one of the following commands:

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

#### Activation via an offline license file

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

or

```
/opt/eset/efs/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](#).

When the activation is complete, access the [Web interface](#) to launch the initial [scan](#) of your system or to [configure](#) ESET Server Security for Linux.

## 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-xxxxxxxxx) and Password when applicable, Public License ID (xxx-xxx-xxx), product name (or list of products) and quantity.

## Check the activation status

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

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

The commands below must be executed by a privileged user:

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

or

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

✓ 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 Server Security for Linux, the output displays the related license details.

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

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

## Update and upgrade

### Update modules

Product modules, including detection modules, are updated automatically.

To manually update detection modules, click **Module update > Check and update**.

If an ESET Server Security for Linux update was not stable, roll back the module updates to a previous state. Click **Status Overview > Module update > Module rollback**, select the desired duration, click **Rollback now**.

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

```
/opt/eset/efs/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
-r	--rollback=VALUE	Rolls back to the oldest snapshot of the scanner module and blocks all updates for VALUE hours
-l	--list-modules	Display the list of product modules
	--check-app-update	Check the availability of new product version in the repository
	--perform-app-update	Download and install new product version if available
	--accept-license	Accept license changes



### upd limitation

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

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/efs/bin/upd --rollback=48
```



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

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

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

## Upgrade ESET Server Security for Linux to a later version

New versions of ESET Server Security for Linux are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules.

### Determine the installed product version

There are two methods to determine the ESET Server Security for Linux product version:

- In the [Web interface](#), click **Help > About**.
- Execute `/opt/eset/efs/sbin/setgui -v` in a Terminal window.

## Upgrade ESET Server Security for Linux locally

- Run an OS-related installation package as described in the [Installation](#) section.
- In the [Web interface](#), click **Status Overview > Product update > Check for update**.
- Use the `upd` utility with the `--perform-app-update` parameter.
- [Configure automatic updates/upgrades](#).

## Upgrade ESET Server Security for Linux remotely

If you use ESET PROTECT to manage ESET Server Security for Linux, you can initiate an upgrade in the following ways:

- [Software install](#) task.
- In the [Web interface](#), click **Dashboard > ESET applications > click ESET Server Security > Update installed ESET products**.
- [Configure automatic updates/upgrades](#).

# Update mirror

Several ESET security products ([ESET PROTECT](#), [ESET Endpoint Antivirus](#), etc.) allow you to create copies of update files that can be used 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 Server Security for Linux to use an update mirror

1. In the [Web interface](#) navigate to **Setup > Update > Primary Server**.
2. In the **Basic** section, click the toggle next to **Choose automatically** to turn it off.
3. In the **Update server** field, type the URL address of the mirror server in one of the following forms:  
  
a. `http://<IP>:<port>/<path_to_update_folder>`  
  
b. `http://<hostname>:<port>/<path_to_update_folder>`
4. Type the applicable username and password.
5. Click **Save**.

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

### Update from a local directory

- i** To update from a local directory, for example, `/updates/eset`, type into the **Update server** field:  
`file:///updates/eset/`

## Automatic product updates

Since version 9.1 automatic product updates for ESET Server Security for Linux (ESSL) are enabled by default. We recommend that you keep this setting enabled to ensure that ESSL has the latest product updates applied when a new update is available.

To edit automatic product updates in ESSL version 9.1 and later:

1. In the [Web interface](#), click **Setup > Update**.
2. In the **Product Update** section, click the toggle next to **Auto-updates**.
3. If you prefer to use a custom update server for product updates:
  - a. Define the server address in the **Custom server** field.
  - b. Type the **Username** and **Password** in the corresponding fields.
4. Click **Save**.

To activate automatic product updates in ESSL version 9.0 and earlier:

1. In the [Web interface](#), click **Setup > Update**.
2. In the **Product Update** section, select **Auto-update** from the **Update mode** list-box.
3. If you prefer to use a custom update server for product updates:
  - a. Define the server address in the **Custom server** field.
  - b. Type the **Username** and **Password** in the corresponding fields.
4. Click **Save**.

If managing ESET Server Security for Linux via ESET PROTECT, configure the above mentioned automatic updates through [Policies](#).

To alter the configuration of ESET Server Security for Linux:

1. In ESET PROTECT, click **Policies > New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Server/File Security 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 **Finish**.

### Restart Recommended

**i** If a remotely managed computer has the automatic updates turned on, and the new package is automatically downloaded, the protection status in ESET PROTECT will be **Restart Recommended**.

## Auto-updates (version 9.1 and later)

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

## Update mode (version 9.0 and earlier)

**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 **Status Overview**.

# Using ESET Server Security for Linux

## Access the Web interface

If the installation is complete, log in to the Web interface at the URL address the installer displayed, along with the login credentials.

The Web interface is available in the following languages:

- English
- French
- Spanish
- Spanish (Latin)
- German
- Japanese
- Ukrainian
- Polish

## SSL Certificate

### ESET Server Security for Linux Web interface certificate

ESET Server Security for Linux Web interface uses a self-signed certificate. Accessing the Web interface for the first time will result in a certificate issue message unless you add a [certificate exception](#).

- Add a certificate exception in Mozilla Firefox:

i

1. Click **Advanced > Add Exception**.
2. In the **Add Security Exception** window, verify **Permanently store this exception** is selected.
3. Click **Confirm Security Exception**.

- Add a certificate exception in Google Chrome:

1. Click **Advanced**.
2. Click **Proceed to <web address of ESSL Web interface> (unsafe)**.
3. At this point Google Chrome remembers the exception.

To use a custom SSL certificate for the Web interface, generate a certificate and import it to ESET Server Security for Linux.

1. Generate an SSL certificate:

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

2. Import the SSL certificate to ESET Server Security for Linux:

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

## Enable the Web interface remotely

If you complete the installation of ESET Server Security for Linux remotely via ESET PROTECT, the Web interface is not enabled.

If you want to access the Web interface on the specific machine, run the following command from a Terminal window:

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

The final output will show the URL address of the Web interface and the access credentials.

To make the Web interface available at a custom IP address and port, for example, 10.1.184.230:9999, run the following command from a Terminal window:

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

To enable the Web interface via ESET PROTECT, use the [Run Command task](#) to execute the following command:

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

where <password> represents the desired password defined by you.

[^ Available options for the setgui command](#)

Options - short form	Options - long form	Description
-g	--gen-password	Generate a new password to access the Web interface
-p	--password=PASSWORD	Define a new password to access the Web interface
-f	--passfile=FILE	Set a new password read from a file to access the Web interface
-r	--gen-cert	Generate a new private key and a certificate
-a	--cert-password=PASSWORD	Set certificate password
-l	--cert-passfile=FILE	Set certificate password read from file
-i	--ip-address=IP:PORT	Server address (IP and port number)
-c	--cert=FILE	Import certificate
-k	--key=FILE	Import private key
-d	--disable	Disable Web interface
-e	--enable	Enable Web interface

## Changing password via Web interface

1. Click the user profile next to logout button.
2. Click **Change password**.
3. Type in the old and new password. The new password must fulfill the criteria listed on the screen.
4. Click **Save**.

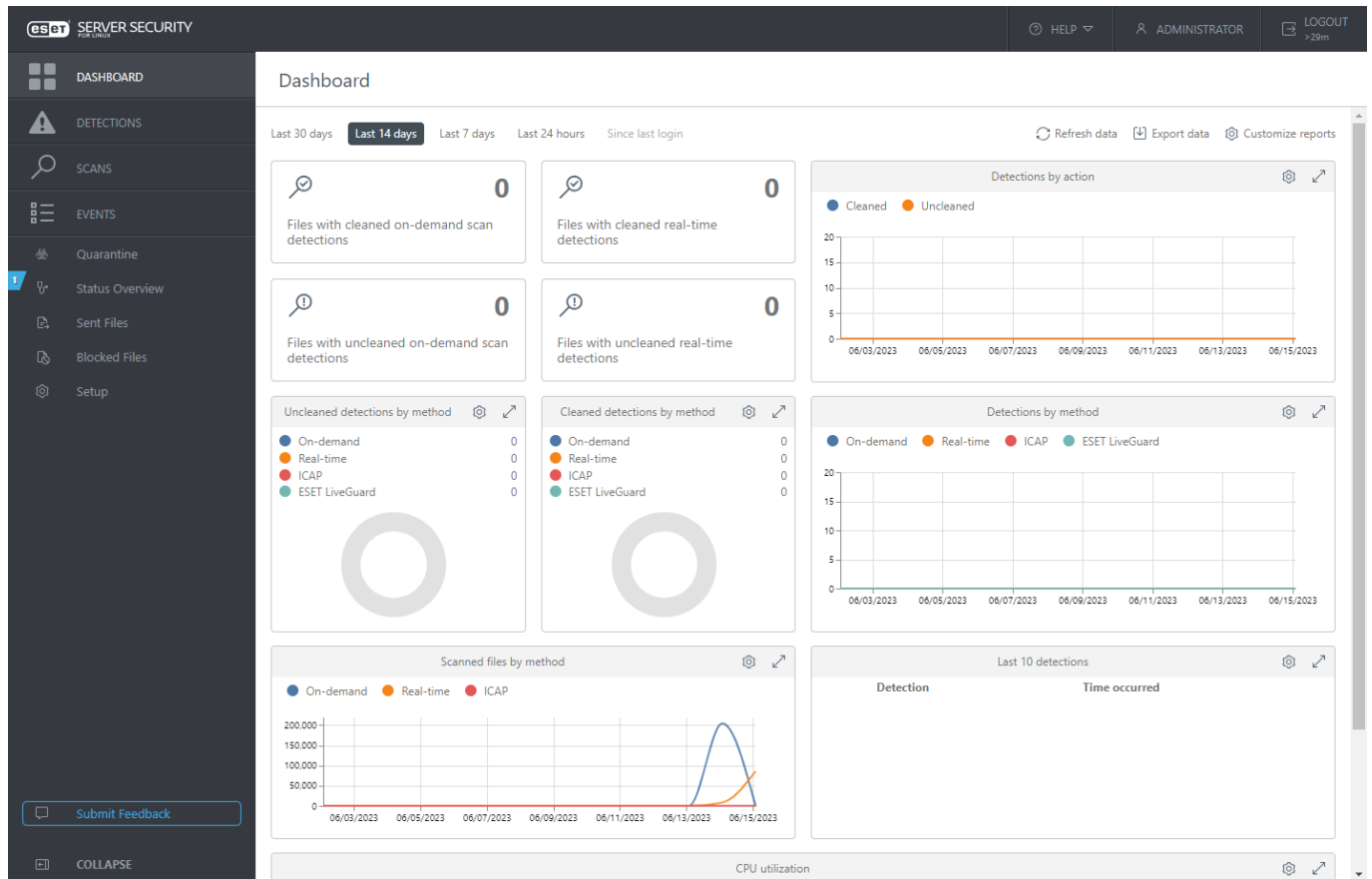
## Product activation and initial scan

If you [activated](#) your instance of ESET Server Security for Linux, update the detection modules (click **Status Overview > Module update > Check and update**) and run an initial [scan](#) of your file system.

## Dashboard

The **Dashboard** provides provides simple [scan statistics](#).





## Scan statistics

ESET Server Security for Linux provides simple scan statistics via charts or tables:

- **Detections by action**
- **Detections by method**
- **Uncleaned detections by method**
- **Cleaned detections by method**
- **Scanned files by method \***
- **Last 10 detections**
- **Top 10 users with the most on-access detections**
- **Last 10 on-demand scans with detections**
- **CPU utilization \***
- **Memory and swap utilization \***

and in the form of tiles:


- Files with cleaned on-demand scan detections
- Files with cleaned real-time detections
- Files with uncleaned on-demand scan detections
- Files with uncleaned real-time detections

**i** Statistics marked by \* above are not 100% accurate. Values are sampled in 15-minute intervals and further processed before display.

Click a statistics tile or chart to go to the [Scans](#) or [Detections](#) screen. Use period presets to filter the statistics.

If the number of uncleaned detections is higher than 0, the background color of "uncleaned" statistics turns red.


## Statistics to display

1. Click  **Customize reports**.
2. Select/deselect the desired statistics.
3. Click **Save**.

To remove single statistics, click its configuration button , select **Remove**.

The configuration of statistics remains intact, unless you delete the browser cache.

## Download scan statistics

To download all scan statistics for the selected period as a *.zip* archive file, click  **Export Data**. The *.zip* archive file contains the statistics in *.csv* files.


To download specific scan statistics, click its configuration button , select **Download**, then select **CSV** or **PDF**.

# Status Overview

The **Status Overview** provides an overview of [module and product updates](#), license information and [product activation](#) options, and status of other services.

When everything is working without any issues, the tile is green. If there are options to improve the protection status of your system, or insufficient protection status is detected, the tile color will change and additional information will display. Click the tile to see the details.

### Mute or un-mute status alerts

**i** Each non-green status alert can be muted by clicking **Mute this alert**. The status will turn grey, and the related tile will display  next to the related item. Click **Un-mute this alert** to turn the status notification back on.

If a [status is disabled](#) via ESET PROTECT, neither **Un-mute this alert**, nor **Enable** is available in the **Status Overview**.

## Module update

If all modules are up to date, the **Module update** tile is green. If module updates are suspended temporarily, the tile turns orange. If the update fails, the tile color changes to red. Click the tile to see the details.

To launch the update of detection modules manually, click **Module update > Check and update**, and wait till the update completes.

## Product update

If all product components are up to date, the **Product update** tile is green. Click the tile to see more details on the current version and last check for updates.

If a new version of the product is available, the tile is light-blue. To see the changelog or to upgrade to the new version, click **Product update**, then click **See changelog** or **Accept & Update now**.



To check the availability of new updates manually, click **Product update > Check for updates**.

See more details on configuring [automatic product updates](#).

## License

If the license is close to expiration, the **License** tile turns orange. If the license is expired, the tile turns red. Click the tile to see available options on changing the license.

## Real-time scanning

If the real-time file system protection is disabled, the tile is red. If you click the tile and mute the **Protection status** notification, the tile will turn green, but  will display next to its items, and  will display next to **Protection status: Disabled**.

**i** If real-time file system protection is disabled and you enable it, it can take up to a minute to restore the scanning service. Afterward, the tile will stop displaying **Scanning service: Disabled**. The **On-demand scanning** tile is displayed only if [Watchdog](#) is enabled.

## Other features (formerly Other services)

A group of other features and services that help improve your system's overall security. Click the tile to see the details.

## Scans

Launch a new scan of all local drives manually from **Scans > New Scan > Scan all local drives**.

Select **Custom scan** where you can choose [scan profile](#), define the location to be scanned. If you select **Scan with Cleaning**, the [cleaning level](#) of selected scan profile will be applied to each detected threat. To scan everything, including the configured [exclusions](#), select **Scan exclusions**.

## Custom scan targets

- Local drives
- Network drives
- Removable media
- Boot sectors — the boot sector of every mounted drive/media will be scanned.
- Custom target — type in the desired path to be scanned and press the TAB key on your keyboard.

Each executed scan is recorded in the **Scans** screen, including the information about the number of found and cleaned threats. If the **Cleaned** column is highlighted red, some infected files were not cleaned/deleted. To view more details of an entry, click it, then click **Show details**.

The **Scan detail** screen includes three tabs:

- **Overview** - Shows the same information as seen in the **Scans** screen, plus the number of disks scanned.
- [Detections](#) - Shows the details of detected infiltration and action taken against it.
- **Not scanned files** - Displays the details and reason of files that could not be scanned.

## Scan profiles

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

To create a new profile, click **Setup > Detection engine > Malware scans > On-demand scan > List of profiles**.

## On-demand scan via Terminal

To run on-demand scan from a Terminal window, use the [/opt/eset/efs/bin/odscan command](#).

## Run On-demand scan from a Terminal window

Syntax: `/opt/eset/efs/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

Options - short form	Options - long form	Description
-s	--scan	Start scan
	--show-scan-info	Display basic information (including 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 <a href="#">excluded paths and extensions</a>

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

Exit code	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

## Example

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

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

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

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

List all running scans

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

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

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

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

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

## Exclusions

### File extension exclusions

This type of exclusion can be set up for Real-time file system protection, On-demand scans and Remote scanning.

1. In the [Web interface](#), click **Setup > Detection Engine**.
2. Click:
  - **Real-time file system protection > Threatsense parameters** to modify exclusions related to [Real-time file system protection](#)
  - **Malware scans > On-demand scan > Threatsense parameters** to modify exclusions related to [On-demand scan \(custom scan\)](#)
  - **Remote scanning > Threatsense parameters** to modify exclusions related to [Remote scanning](#)
3. Next to **File extensions excluded from scanning**, click **Edit**.
4. Click **Add** and type the extension to exclude. To define several extensions at once, click **Enter multiple values**, and type the applicable extensions separated by a new line or another separator you selected.
5. Click **OK**, then click **Save** to close the dialog.
6. Click **Save** to save the changes.

## 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 the [Web interface](#), click **Setup > Detection Engine > Basic**.
2. Next to **Performance exclusions**, click **Edit**.
3. Click **Add**, define the **Path** to be skipped by the scanner. Optionally add a comment for your information.
4. Click **OK**, then click **Save** to close the dialog.
5. Click **Save** to save the changes.

## 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

- ✓ We highly recommend that you do not use wildcards in the middle of a path (for example */home/user/\*/data/file.dat*) unless your system infrastructure requires it. See the following [Knowledgebase article](#) for more information.

There are no restrictions to using wildcards in the middle of a path when using [detection exclusions](#).

## Detection exclusions criteria

- **Path**—Detection exclusion for a specified path (or any if left empty)
- **Detection name**—A detected object will be excluded if it matches the defined detection name. If the file is later infected with other malware, its detection name will change; thus, it will be detected as infiltration, and proper action will be taken against it. If **Path** is defined, only files located at that path and matching the **Detection name** will be excluded from detection. To add such detections to the exclusion list, use the [detection exclusion wizard](#). Alternatively, navigate to **Quarantine**, click a quarantined file, and select **Restore and exclude**. This option is displayed only for items the detection engine evaluated as eligible for exclusion.
- **Hash**—Excludes a file based on a specified hash (SHA1), regardless of the file type, location, name, or extension

## Detections

Every threat detected by the On-access scanner and action taken against it is recorded in the **Detections** screen.

Threats detected by the On-demand scanner and actions taken are recorded in **Scans > select a completed scan >**

**Show details > Detections.**

If a threat has been detected but not cleaned, the whole row will be highlighted red.

## Available actions

- To attempt cleaning of a detected malicious file, click the specific row, select **Rescan with cleaning**.
- To locate the file that has been detected as malicious but not deleted yet, click the corresponding row, select **Copy path** and use a file browser to look up the file.
- To create a [detection exclusion](#) based on the SHA-1 hash manually, select **Copy hash**.
- To start the [exclusion wizard](#), select **Create exclusion**.

To apply **Rescan with cleaning** or **Create exclusion** action to multiple detections at once:

1. Select the checkbox of relevant detections.
2. Click Actions, select the desired action.

## Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are falsely detected by ESET Server Security for Linux. You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Virus Lab.

## Manage quarantined items through the Web interface

The **Quarantine** screen displays a list of files stored in the quarantine folder. The list displays:

- date and time of quarantine
- path to the original location of the quarantined file
- detection name (empty for manually quarantined items)
- reason of moving the file to quarantine (empty for manually quarantined items)
- number of threats (for example, if it is an archive containing multiple infiltrations)
- size and hash of quarantined item

Click the quarantined item to display the available actions:

- **Restore**—Restore the quarantined item to its original location
- **Restore and Exclude**—Restore the quarantined item to its original location and create a [detection exclusion](#) matching the path and detection name



- **Copy path**—Copy the original path of the file to the clipboard
- **Copy hash**—Copy the SHA-1 hash of the file to the clipboard
- **Download**—Download the quarantined item to your hard drive
- **Delete from quarantine**—Delete the quarantined item permanently
- **Submit for analysis**—Submit a copy of the quarantined item for analysis to ESET

The **Restore and Exclude** option is displayed only for items the detection engine evaluated as eligible for exclusion.

Path to quarantine directory: */var/opt/eset/efs/cache/quarantine/root/*

To submit a quarantined file for analysis:

1. Select an item and select **Submit for analysis**.
2. Select an appropriate **Reason for submitting the sample**.
  - **Suspicious file**: A file that cannot be cleaned during a scan or has unusual characteristics
  - **False positive file**: A file falsely identified as malware
  - **Other**
3. Type your email address or select **Send anonymously**.
4. Click **Next**.
5. Provide any additional information.
6. Click **Send**.

## Manage quarantined items via Terminal

Syntax: `/opt/eset/efs/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	New path to restore a quarantined item to
-h	--help	Show help
-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 "0123456789":

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

or

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

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

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

or

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

or

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

## Restore file from quarantine via Terminal

1. List quarantined items.

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

## Sent files

ESET Server Security for Linux version 8.1 and later provides an overview of files submitted for analysis to ESET LiveGrid® or [ESET LiveGuard Advanced](#).

Suspicious files are automatically submitted for analysis to ESET LiveGrid®. If you enable ESET LiveGuard Advanced, manually submitted files for analysis are sent to ESET LiveGuard Advanced only. However, some automatically submitted files may still be sent to ESET LiveGrid®.

You can also [submit suspicious files or sites for analysis manually](#). It takes a few minutes for manually submitted files to be displayed in the list.

To view the list of files submitted for analysis, log in to the [Web interface](#) and click **Sent Files**. Alternatively, execute either of the following commands from a Terminal window as a privileged user:

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


or

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

If you wanted to create a temporary [detection exclusion](#) for a file sent for analysis, click the file to copy its path or hash.

## Submit sample for analysis

If you find a suspicious file on your computer or a suspicious site on the internet, you can submit it to the ESET Research Lab for analysis.

-  **ESET LiveGrid® feedback system must be enabled**
  1. In the [Web interface](#), click **Setup > Detection Engine > Cloud-based protection**.
  2. Enable **Enable ESET LiveGrid® feedback system**, click **Save**.

To submit a sample for analysis:

1. Click **Help** or **Sent Files**, then click **Submit sample for analysis**.
2. Select a **Reason for submitting the sample**.
  - **Suspicious file**: A file that cannot be cleaned during a scan or has unusual characteristics
  - **Suspicious site**: A website infected by malware
  - **False positive site**: A website falsely identified as infected by malware

- **False positive file:** A file falsely identified as malware
  - **Other**
3. Add the site address or file path.
  4. Type your email address or select **Submit anonymously**.
  5. Click **Next**.
  6. Provide additional information.
  7. Click **Send**.

You can also submit [quarantined files](#) for analysis.

## Events

Important actions taken in ESET Server Security for Linux Web interface, failed login attempts to Web interface, ESET Server Security for Linux related commands executed via Terminal and some more information is logged in the **Events** screen.

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

## Display events via Terminal

To display the content of **Events** screen via a Terminal window, use the `lslog` command line tool.

Syntax: `/opt/eset/efs/bin/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
-n	--sent-files	Display a list of <a href="#">files submitted for analysis</a>
-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 <a href="#">detections</a> 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.

## Examples

Display all event logs:

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

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

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

## Blocked files

If ESET Server Security for Linux (ESSL) is integrated with [ESET Inspect](#), files blocked by ESET Inspect will appear at **Blocked files**.

To integrate ESSL with ESET Inspect, deploy [ESET Inspect Connector](#) on the machine protected by ESSL.

ESET Inspect Connector will start communicating with ESSL automatically.

## Configuration

To alter the default configuration of ESET Server Security for Linux navigate to the **Setup** screen. You can adjust the [detection behavior](#), alter product update and connection settings, or change the password and certificate of [Web interface](#). To apply the changes, click **Save** in the **Setup** screen.

If you have configured ESET Server Security 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 Server Security for Linux), you can export it to an *.xml* file.

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

### Export configuration

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

### Import configuration

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

## Available options

Short form	Long form	Description
	--import-xml	import settings
	--export-xml	export settings
-h	--help	show help

Short form	Long form	Description
-v	--version	show version information

## Detection engine

The default setup of detection behavior provides the essential level of security which includes:

- [Real-time file system protection](#)
- Machine learning protection
- Smart optimization (most efficient combination of system protection and scanning speed)
- [ESET LiveGrid](#) reputation system

To turn on additional protection features, click **Setup** > **Detection engine**:

- Detection of [potentially unwanted applications](#)
- Detection of [potentially unsafe applications](#) (for example key loggers, password-cracking tools)
- Enable submission of suspicious or infected samples
- Configure [exclusions](#) (files, directories left out of scan) to speed up scan
- Adjust [cleaning level](#)

Every threat detected and action taken against it is logged in the **Detections** screen.

## Real-time & Machine learning protection

Advanced Machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection based on Machine learning. Read more about this type of protection in the [Glossary](#).

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

- **Malware**—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.

<b>Aggressive</b>	Reporting configured to maximum sensitivity. More detections are reported. The <b>Aggressive</b> setting can falsely identify objects as malicious, and action will be taken with such objects (depending on Protection settings).
<b>Balanced</b>	This setting is an optimal balance between performance and accuracy of detection rates and the number of falsely reported objects.
<b>Cautious</b>	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.
<b>Off</b>	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.

<b>Aggressive</b>	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.
<b>Balanced</b>	Reported balanced (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started.
<b>Cautious</b>	Reported cautious level detections are blocked, and automatic remediation (i.e., cleaning) is started.
<b>Off</b>	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.

# Exclusions

## File extension exclusions

This type of exclusion can be set up for Real-time file system protection, On-demand scans and Remote scanning.

1. In the [Web interface](#), click **Setup > Detection Engine**.
2. Click:

- **Real-time file system protection > Threatsense parameters** to modify exclusions related to [Real-time file system protection](#)
- **Malware scans > On-demand scan > Threatsense parameters** to modify exclusions related to [On-demand scan \(custom scan\)](#)
- **Remote scanning > Threatsense parameters** to modify exclusions related to [Remote scanning](#)

3. Next to **File extensions excluded from scanning**, click **Edit**.

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

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

6. Click **Save** to save the changes.

## 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 the [Web interface](#), click **Setup > Detection Engine > Basic**.
2. Next to **Performance exclusions**, click **Edit**.
3. Click **Add**, define the **Path** to be skipped by the scanner. Optionally add a comment for your information.
4. Click **OK**, then click **Save** to close the dialog.
5. Click **Save** to save the changes.

## 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

✓ We highly recommend that you do not use wildcards in the middle of a path (for example */home/user/\*/data/file.dat*) unless your system infrastructure requires it. See the following [Knowledgebase article](#) for more information.

There are no restrictions to using wildcards in the middle of a path when using [detection exclusions](#).

## Processes exclusions

The Processes exclusions feature enables you to exclude application processes from [Real-time file system protection](#).



Backup solutions strive to improve speed, process integrity, and service availability. They usually use techniques known to conflict with file-level malware protection to achieve it. Similar problems can occur when attempting to complete a live migration of virtual machines. Usually, the only effective way to avoid such situations is to deactivate Anti-Malware software.

By excluding specific processes (for example, those of the backup solution), all file operations attributed to such excluded processes are ignored and considered safe, thus minimizing interference with the backup process. We recommend using caution when creating exclusions – an excluded backup tool can access infected files without triggering an alert, which is why extended permissions are only allowed in the real-time protection module.

This feature was designed to exclude backup tools. Excluding the backup tool's scanning process ensures system stability and does not affect backup performance as the backup is not slowed down while it is running. Ultimately, it minimizes the risk of potential conflicts.

## Add binaries to the list of excluded processes


1. Click **Setup > Detection Engine > Real-time file system protection**.
2. In the **Basic > Processes exclusions** section, click **Edit** next to **Processes to be excluded from scanning**.
3. Click **Add**.
4. Type the absolute path of the binary.
5. Click **Save** twice.
6. In the **Setup** screen, click **Save**.

As soon as a binary is added to the exclusions, ESET Server Security for Linux stops monitoring its activity. Scans do not run on any file operations performed by that binary.

You can also **Edit** existing processes or **Delete** them from exclusions.


## Export/import detection exclusions

To share the configured processes exclusions with another instance of ESET Server Security for Linux that is not managed remotely, export the configuration:

1. Click **Setup > Detection Engine > Real-time file system protection**.
2. In the **Basic > Processes exclusions** section, click **Edit** next to **Processes to be excluded from scanning**.
3. Click **Export**.
4. Click the download icon  next to **Download exported data**.
5. If the browser prompts to open or save the file, select **Save**.

To import the exported processes exclusions file:

1. Click **Setup > Detection Engine > Real-time file system protection**.

2. In the **Basic > Processes exclusions** section, click **Edit** next to **Processes to be excluded from scanning**.
3. Click **Import**, then the browse icon  to browse for the exported file, click **Open**.
4. Click **Import > OK > Save**.
5. In the **Setup** screen, click **Save**.

## Detection exclusions

Detection exclusions allow you to exclude objects from cleaning (deletion or moving to quarantine) by filtering the detection name, object path or its hash.

### How detection exclusions work

Detection exclusions do not exclude files and folders from scanning as **Performance exclusions** do.

✓ Detection exclusions exclude objects from being quarantined/deleted only when they are detected by the detection engine and an appropriate rule is present in the exclusion list.

See the sample rules in the image below. The rule in the first row will exclude an object that is detected as *Eicar test file* and is located at */home/demo/Download/some.file*. The rule in the second row will exclude every detected object that has the corresponding SHA-1 hash, regardless the detection name.

Detection exclusions
? □ ×

Object criteria	Exclude detection	Comment
/home/demo/Downloads/*	Eicar test file	
D27265074C9EAC2E2122ED69294DB C4D7CCE9141	Any detection	eicar_com.zip

Add
Edit
Remove

Import
Export

Save
Cancel

## Detection exclusions object criteria

- **Path**—Detection exclusion for a specified path (or any if left empty)
- **Detection name**—A detected object will be excluded if it matches the defined detection name. If the file is later infected with other malware, its detection name will change; thus, it will be detected as infiltration, and proper action will be taken against it. If **Path** is defined, only files located at that path and matching the **Detection name** will be excluded from detection. To add such detections to the exclusion list, use the [detection exclusion wizard](#). Alternatively, navigate to **Quarantine**, click a quarantined file, and select **Restore and exclude**. This option is displayed only for items the detection engine evaluated as eligible for exclusion.
- **Hash**—Excludes a file based on a specified hash (SHA1), regardless of the file type, location, name, or extension

## Add or Edit detection exclusions

### Manually define detection exclusions

1. Click **Setup** > **Detection engine**.
2. Click **Edit** next to **Detection exclusions**, click **Add**.
3. Define the exclusion criteria:

- **Path**—Detection exclusion for a specified path (or any if left empty)
- **Detection name**—A detected object will be excluded if it matches the defined detection name. If the file is later infected with other malware, its detection name will change; thus, it will be detected as infiltration, and proper action will be taken against it. If **Path** is defined, only files located at that path and matching the **Detection name** will be excluded from detection. To add such detections to the exclusion list, use the [detection exclusion wizard](#). Alternatively, navigate to **Quarantine**, click a quarantined file, and select **Restore and exclude**. This option is displayed only for items the detection engine evaluated as eligible for exclusion.
- **Hash**—Excludes a file based on a specified hash (SHA1), regardless of the file type, location, name, or extension

4. Click **OK** and then click **Save**.
5. In the **Setup** screen, click **Save**.

### Use the detection exclusion wizard

1. Select a [detection](#) and select **Create exclusion**.
2. Select the appropriate exclusion criteria:
  - **Exact file**—Exclude a file by SHA-1 hash
  - **Detection**—Exclude a file by detection name

- **Path + Detection**—Exclude a file matching the path and detection name

3. Type a comment if applicable. It displays in the list of detection exclusions at **Setup > Detection engine >** click **Edit** next to **Detection exclusions**.


4. Click **Create exclusion**.

## Edit or remove a detection exclusion


1. Click **Setup > Detection engine**.
2. Click **Edit** next to **Detection exclusions**.
3. Select an exclusion, click **Edit** or **Remove**.
4. Save your changes.

## Export/import detection exclusions

To share the configured detection exclusions with another instance of ESET Server Security for Linux that is not managed remotely, export the configuration:

1. Click **Setup > Detection engine**.
2. Click **Edit** next to **Detection exclusions**, click **Export**.
3. Click the download icon  next to **Download exported data**.
4. If the browser prompts to open or save the file, select **Save**.

To import the exported detection exclusions file:

1. Click **Setup > Detection engine**.
2. Click **Edit** next to **Detection exclusions**, click **Import**.
3. Click the browse icon  to browse for the exported file, click **Open**.
4. Click **Import > OK > Save**.
5. In the **Setup** screen, click **Save**.

## 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 after 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.

**i** 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.

### Remote on-access scan of a locally mounted NFS shared folder is not supported

**i** Suppose you have the NFS kernel server installed on a machine protected by ESET Server Security for Linux (ESSL); if its shared folder is locally mounted on a remote machine not protected by ESSL, on-access scanner of ESSL will not work there.

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

1. Click **Setup > Detection engine > Real-time file system protection > Basic**.
2. Disable **Enable Real-time file system protection**.

## 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 it is connected 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:

1. In the [Web interface](#), click **Setup > Detection engine > Real-time file system protection > ThreatSense parameters**.
2. Enable or disable **Enable Smart optimization**.
3. Click **Save**.

## 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 to be scanned
- The combination of various detection methods
- Cleaning levels, etc.

To enter the setup window, click **Setup > Detection engine**, 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**

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 is able to recognize several additional types of packers through the use of code emulation

**i** 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. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not covered by the previous virus signatures database. The disadvantage is a (very small) 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 types of files to be excluded from scan.

## Other

When configuring ThreatSense engine parameters setup for a On-demand computer scan, the following options in **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, making use of 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 levels of nested archives 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 of 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**.

## 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.

By default, ESET Server Security for Linux (ESSL) 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.

Alter the configuraiton at **Setup > Detection engine > Cloud-based protection**.



## 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.

### Enable ESET LiveGuard Advanced

Available from ESET Server Security for Linux version 8.1. Data will be sent to [ESET LiveGuard Advanced](#).

### 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 detected 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 all PE format files (for example, *.exe*, *.dll*, *.sys*) and ELF files (for example, *.axf*, *.bin*, *.elf*). Also text files with "x" flag (executable)

- 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, .sh, .py, .pl*
- 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 Server Security 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.

### Change of the service name

On March 23, 2022, ESET Dynamic Threat Defense was re-branded to ESET LiveGuard Advanced. In ESET business products, you can find it also as ESET LiveGuard. Both names refer to the same service.

#### Availability

The service is available only if ESET Server Security for Linux version 8.1 or later is [managed remotely](#).



#### [Activate ESET LiveGuard Advanced before use](#)

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

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

or

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

To enable the service in ESSL:

1. [Activate ESET LiveGuard Advanced](#).
2. In the [Web interface](#), click **Setup** > **Detection Engine** > **Cloud-based protection**.

3. Enable **Enable ESET LiveGrid® reputation system (recommended)**, **Enable ESET LiveGrid® feedback system**, then enable **Enable ESET LiveGuard**.
4. 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](#).
5. Click **Save**.

#### [Instructions to enable ESET LiveGuard Advanced remotely via ESET PROTECT](#)

1. In ESET PROTECT, click **Policies > New policy** and type a name for the policy.
2. Click **Settings** and select **ESET Server/File Security 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**, then enable **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 the policy applies to.
7. Click **OK**, then click **Finish**.

## ESET Status Portal

[ESET Status Portal](#) provides an up-to-date view of ESET services availability. It provides a view of ESET services and reports on service statuses, including past incidents. If you are an ESET user experiencing any issues with your ESET service and ESET Status Portal does not indicate them, contact [ESET Technical Support](#).

## 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 a profile name and click **Add**. The new profile will display 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 [Real-time & Machine Learning protection](#) section.

# Remote scanning (ICAP scan)

To protect external ICAP compatible devices/software remotely, enable and configure **Remote scanning**.

1. In the Web interface navigate to **Setup > Detection Engine > Remote Scanning**.
2. Turn on the toggle key next to **Enable remote scanning using ICAP service**.
3. Click **Edit** next to **Listen addresses and ports**, click **Add**, define the address and port of ICAP server. Click **OK**, then click **Save**.
4. Optionally, review and adjust [ThreatSense parameters](#).
5. Click **Save**.

[See how to integrate ICAP server with EMC Isilon.](#)

## Supported ICAP clients

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

## Cleaning levels

- **No cleaning**—Infected files are not cleaned automatically. The number of found threats is highlighted red in the **Detections occurred** column. The **Cleaned** column is highlighted red but displays 0.
- **Normal cleaning**—The program attempts to automatically clean or delete infected files, except those that would cause loss of useful data, for example, an archive file containing a mix of infected and clean files. The number of detected files in the archive file count towards **Detections occurred**, and the **Cleaned** column is highlighted red.
- **Strict cleaning**—The program cleans or deletes all infected files. The only exceptions are the system files.
- **Rigorous cleaning**—The program cleans or deletes all infected files without exception.
- **Delete**—The program deletes all infected files without exception.

## 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 Server Security for Linux update was not stable, roll back the module updates to a previous state. Click **Status Overview > Module update > Module rollback**, select the desired duration, click **Rollback now**.

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

Since version 9.1 automatic product updates for ESET Server Security for Linux (ESSL) are enabled by default. We recommend that you keep this setting enabled to ensure that ESSL has the latest product updates applied when a new update is available.

For version 9.0 and earlier activate automatic updates by selecting **Auto-update** from the **Update mode** list-box.

### Auto-updates (version 9.1 and later)

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

### Update mode (version 9.0 and earlier)

**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 **Status Overview**.

### Custom server, Username, Password

If you manage several ESSL 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.

## Tools

In **Setup > Tools** section of ESET Server Security for Linux Web interface you can modify the general configuration of ESET Server Security for Linux.

- Define the details of a [Proxy server](#) to connect to the internet
- Change the password and/or certificate of [Web interface](#)
- Configure how [log files](#) are handled

- Enable/disable Watchdog

You can also [schedule](#) on-demand scan.

## Watchdog

The watchdog service keeps checking the status of scan daemon. If the service is enabled, the status of scanning service is displayed in **Status overview** on the **On-demand scanning** and **Real-time scanning** tiles.

If the watchdog service is disabled, the **On-demand scanning** tile is hidden in **Status overview**.

## Proxy Server

Configure ESET Server Security 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**.

## Web interface

To change the IP address and port of ESET Server Security for Linux Web interface, or add additional addresses on which the Web interface is supposed to be available, click **Edit** next to **Listen addresses and ports**. Click **Add**, type in the proper address and port, click **OK** and then click **Save**. Click **Save** in the **Setup** screen.

To import a new [certificate](#) and corresponding private key, use the **Certificate** and **Private key** buttons. If the certificate is password protected, type the password to the **Certificate password** field. Click **Save** in the **Setup** screen.

## Disable and enable the Web interface

If you click the toggle next to **Enable web interface** and click **Save** in the Setup screen, you will be logged out immediately and the Web interface will not be available anymore.

 [You can enable the Web interface again via a Terminal window.](#)

If you complete the installation of ESET Server Security for Linux remotely via ESET PROTECT, the Web interface is not enabled.

If you want to access the Web interface on the specific machine, run the following command from a Terminal window:

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

The final output will show the URL address of the Web interface and the access credentials.

To make the Web interface available at a custom IP address and port, for example, 10.1.184.230:9999, run the following command from a Terminal window:

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

To enable the Web interface via ESET PROTECT, use the [Run Command task](#) to execute the following command:

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

where <password> represents the desired password defined by you.

 [Available options for the setgui command](#)

Options - short form	Options - long form	Description
-g	--gen-password	Generate a new password to access the Web interface
-p	--password=PASSWORD	Define a new password to access the Web interface
-f	--passfile=FILE	Set a new password read from a file to access the Web interface
-r	--gen-cert	Generate a new private key and a certificate
-a	--cert-password=PASSWORD	Set certificate password
-l	--cert-passfile=FILE	Set certificate password read from file
-i	--ip-address=IP:PORT	Server address (IP and port number)
-c	--cert=FILE	Import certificate
-k	--key=FILE	Import private key
-d	--disable	Disable Web interface
-e	--enable	Enable Web interface

## Listen address and port

ESET Server Security for Linux allows you to configure a custom IP address and port for both, the [Web interface](#) and [ICAP server](#).

## Log files

Modify the [configuration](#) of ESET Server Security for Linux logging.

### Minimum logging verbosity

Logging verbosity defines the level of details the log files include regarding ESET Server Security 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 **Events**, **Detections**, or **Sent Files** screen or log list (`lslog`):

1. Turn on **Automatically delete records older than (days)**.
2. Adjust the day to specify the age of files to be hidden.
3. Click **Save**.

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 automatically be defragmented if the fragmentation percentage is higher than value specified in the **If the number of unused records exceeds (%)** field. Unused records stand for hidden logs. 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 which is 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 so. With recent switch to systemd and its journal, syslog facility is less important but still can be used for filtering logs.

## Scheduler

ESET Server Security for Linux version 8 and later allows periodic weekly [custom scans](#) on defined days and times.

### Schedule a scan

1. In the [Web interface](#), click **Setup > Tools > Scheduler**.
2. Next to **Tasks**, click **Edit**.
3. Click **Add**.
4. Name the schedule, set a time, and select the days when the custom scan will be automatically triggered. Click **Next**.
5. Select a [scan profile](#).



6. Select **Scan targets**, and/or define custom targets separated by a new line.
7. Select/deselect available **Options** ([Scan with cleaning](#), Scan [exclusions](#)).
8. Click **Finish**, then click **Save** to close the dialog.
9. Click **Save** to save all changes.

To modify any scheduled task, in step 3 above, select the specific task and click **Edit**. Continue with the remainder of steps.

To remove a scheduled task, in step 3 above, select the specific task and click **Remove**. Continue with steps 8 and 9.

### Execution of scheduled tasks

- ✓ The scheduler takes use of [cron](#), and is executed if the applicable computer is running. If the computer is off, the task will run at the next scheduled time the computer is on.

## User interface

To configure notifications displayed in [Status Overview](#):

1. In the [Web interface](#), click **Setup > User interface > User interface elements**.
2. Click **Edit** next to **Display in Protection status**.
3. Select the applicable [app status](#).
4. Click **OK** and then click **Save**.

**i** Not selected status is muted in [Status Overview](#). All changes apply only locally.

If you manage ESET Server Security for Linux remotely, see [display statuses in ESET PROTECT](#).

## Statuses

Each selected status in **Setup > User interface > User interface elements > Display in Protection status > Edit** displays a notification in **Status Overview** if the related module is disabled, non-functional, or missing.

**i** Not selected status is muted in [Status Overview](#). All changes apply only locally.

## Display statuses in ESET PROTECT

To display statuses in ESET PROTECT when managing ESET Server Security for Linux remotely:

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

3. Click **User interface** > **User interface elements**.
4. Click **Edit** next to **Send to ESET management console**.
5. Select the appropriate statuses and click **OK**.
6. Click **Continue** > **Assign**, and select the desired group of computers the policy applies to.
7. Click **OK**, then click **Finish**.

## Remote management

To manage ESET Server Security 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 Server Security for Linux.

ESSL from version 8.1 supports the [merge of local and remote lists of policies](#).

## Container security

Linux servers are often a base for running Docker containers and Docker orchestration tools. The container security feature is part of the [real-time file system protection](#) in ESET Server Security for Linux (ESSL).

ESSL can detect threats or suspicious activity in a container and block them but cannot eliminate them; meaning, a suspicious script will be blocked from execution but will not be deleted. You can delete it manually.

ESET's [real-time file system protection](#) can scan the container in the following phases:

- process of building the container image
- deploying the container image on a machine protected by ESSL

The activity inside the container is also scanned in real-time for suspicious behavior

At ESET, we tested [Docker CE](#) (Community Edition) version 20.10.7.

## Use case examples

In this chapter we will cover most common use cases of ESET Server Security for Linux:

- [Secured ICAP with stunnel TLS proxy](#)
- [Integrate ICAP server with EMC Isilon](#)
- [Retrieve module information](#)

- [Schedule scan](#)

## Secured ICAP with stunnel TLS proxy

You can use the stunnel service to manage encrypted connection for ICAP scanning to increase security.

1. [Install](#) and [activate](#) ESET Server Security for Linux.
2. To enable ICAP scanning click **Setup > Detection engine > Remote scanning** > click the toggle next to **Enable remote scanning using ICAP service**.
3. Install stunnel by package manager. On Ubuntu 20.04, execute the following command from a Terminal window as a privileged user:

```
sudo apt install stunnel
```

4. Store private and public keys to encrypt communication by stunnel in a file with restricted access. This certificate needs to be trusted by an ICAP client, which will connect to ESSL via this secured connection. Example of how to store keys and set permissions:

```
sudo cat private_key.pem ca_key.pem >> /etc/pki/tls/private/stunnel.pem
```

```
sudo chmod 400 /etc/pki/tls/private/stunnel.pem
```

5. Create a configuration file */etc/stunnel/stunnel.conf* readable only by root (chmod 0600) containing the following lines:

```
[efs_icap]
accept = 0.0.0.0:11344
connect = 0.0.0.0:1344
cert = /etc/pki/tls/private/stunnel.pem
```

- **efs\_icap**—Service name, which we configure in the following lines. Stunnel supports forwarding of multiple connections.
- **accept**—IP address and port that will accept ICAPS connections. In this example is localhost and port 11344
- **connect**—IP address and port where ESSL listen for ICAP requests. In this example is the same machine and the default port 1344

**i** Stunnel can even run on a dedicated server and connect to multiple machines with ESSL or be sandboxed in chroot. For all stunnel options see the [manual](#).

6. Start stunnel by systemd and enable it to run automatically after system boot:

```
sudo systemctl start stunnel
```

```
sudo systemctl enable stunnel
```

7. Open port for ICAPS port in a firewall. On Ubuntu 20.04, execute the following commands from a Terminal window as a privileged user:

```
sudo ufw allow 11344/tcp  
sudo ufw reload
```

8. Configure ICAP client (for example, storage) according to its guide and connect it to port 11344, where ESSL runs with stunnel and trusts the used certificate. Then test if the antivirus connection works, for example, on the eicar sample.

## Integrate ICAP server with EMC Isilon

### Overview

You can scan the files you store on an Isilon cluster for computer viruses, malware, and other security threats by integrating with ESET Server Security for Linux (ESSL) through the Internet Content Adaptation Protocol (ICAP).

### Prerequisite

1. ESSL is installed and its Web interface is enabled.
2. Isilon OneFS is installed.

### Enable ICAP server in ESSL

In this example ICAP server will listen on IP address 10.1.169.28 and on port 1344.

1. Click **Setup > Detection Engine > Remote scanning**, turn on both **Enable remote scanning using ICAP service** and **Dell EMC Isilon compatibility**.
2. Click **Edit** next to **Listen addresses and ports**.
3. Click **Add**.
4. Type the applicable IP address and port. In our example, the IP address is 10.1.168.28, and port is 1344.
5. Click **Save**.

### Enabling ICAP server in OneFS

1. Log in to OneFS administration panel, click **Data Protection > Antivirus > ICAP Servers > Add an ICAP Server**.
2. Select **Enable ICAP Server**, and type the URL address of ICAP server to the **ICAP Server URL** field using the

following pattern: `icap://<IP_ADDRESS>:<PORT>/scan`

In our example: `icap://10.1.168.28:1344/scan`

3. Click **Add Server**.
4. Click **Settings**, select **Enable Antivirus Service**.
5. Type into **Path prefixes** the path to scan. To scan all paths, type `/ifs` (without quotation marks).
6. Click **Save changes**.

## Scan-related settings on EMC Isilon

- [File size, file name or file extension restrictions](#)
- [On-access scanning](#) or [on-demand scanning via policy](#)
- [Threat response settings](#)

## How does it work?

When a file is written to (or accessed on) the EMC Isilon cluster, OneFS queues the file to be scanned, and sends the file to the ICAP server configured in both OneFs and ESSL. ESSL scans the file and provides feedback on the scanned file to EMC Isilon. OneFS decides how to deal with the scanned files based on [threat response settings](#).

## Test your setup

To test your setup, you need to have access from your computer to OneFS cluster through one of the supported protocols. In our example, we will use the NFS protocol.

1. Configure NFS:
  - a. Log in to OneFS administration panel, click **Protocols > UNIX Sharing (NFS) > Create Export**.
  - b. Leave the default settings, verify the path is `/ifs`, click **Save**.
2. Mount NFS share on your Linux machine:

```
mkdir isilon
```

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

3. Complete a test scan:
  - a. Get eicar antivirus test file from [www.eicar.org](http://www.eicar.org), copy it to Isilon's NFS share and try to read its content.

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

```
cp eicar.com isilon
```

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

b. Based on your OneFS antivirus settings, the result will be either permission denied on that file (default), or the file will be truncated or deleted. For example:

```
cat: isilon/eicar.com: Permission denied
```

c. To check the detected threat, log in to OneFS administration panel, click **Data Protection > Antivirus**.

## Retrieve module information

Use the `upd` utility with `-l` parameter in a Terminal window to list all modules and their versions.

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

## Schedule scan

ESET Server Security for Linux v8 has a built-in [scheduler](#) to execute periodic custom scans on defined days and times. To set up a periodic custom scan without the built-in [scheduler](#), follow the instructions below.

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 in-depth full disk scan every Sunday at 2am

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/efs/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/efs/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

This topic details the file and folder structure of ESET Server Security for Linux, if ESET Technical Support asked you to access files for troubleshooting purposes. The [list of daemons and command line utilities](#) is available further below.

### Base directory

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

```
/var/opt/eset/efs/lib
```

### Cache directory

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

```
/var/opt/eset/efs/cache
```

### Binary files directory

The directory where the relevant ESET Server Security for Linux binary files are stored.

```
/opt/eset/efs/bin
```

There you find the following utilities:

- [lslog](#)—Use it to display logs gathered by ESET Server Security for Linux.

- [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 Server Security for Linux system binary files are stored.

```
/opt/eset/efs/sbin
```

There you find the following utilities:

- [cfg](#)—Use it to import/export ESET Server Security for Linux settings.
- [cloud](#)—Use it to check ESET LiveGuard Advanced status.
- [collect\\_logs.sh](#)—Use it to generate all essential logs as an archive file to the home folder of being logged in user.
- [lic](#)—Use it to activate ESET Server Security for Linux with the purchased license key or to check the activation status and license validity.
- [setgui](#)—Use it to enable/disable ESET Server Security for Linux Web interface and manage related operations.
- `startd`—Use it to start ESET Server Security for Linux daemon manually if it was stopped.

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

```
systemctl status efs.service
```

or

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

Sample output from `systemctl`:



```
user@example: ~
● efs.service - ESET Server Security
   Loaded: loaded (/lib/systemd/system/efs.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-06-21 09:26:57 CEST; 1h 32min ago
     Process: 2596 ExecStartPre=/opt/eset/efs/lib/install_scripts/check_start.sh
     Process: 3341 ExecStartPost=/bin/sleep 2 (code=exited, status=0/SUCCESS)
    Main PID: 3340 (startd)
       Tasks: 38 (limit: 4626)
      Memory: 640.0M
      CGroup: /system.slice/efs.service
              └─3340 /opt/eset/efs/sbin/startd
                  └─3343 /opt/eset/efs/lib/logd
                      └─3344 /opt/eset/efs/lib/scand
                          └─3345 /opt/eset/efs/lib/sysinfod
                              └─3346 /opt/eset/efs/lib/updated
                                  └─3347 /opt/eset/efs/lib/licensed
                                      └─3348 /opt/eset/efs/lib/utild
                                          └─3349 /opt/eset/efs/lib/confd
                                              └─3354 /opt/eset/efs/lib/watchd
                                                  └─3355 /opt/eset/efs/lib/oaeventd
                                                      └─3625 /opt/eset/efs/lib/webd/backend/webd
                                                          └─3821 /opt/eset/efs/lib/authd
```

## 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+odfeeder – On-demand scanning helpers
- lib/utild – Utility service
- lib/sysinfod – OS and media detection service
- lib/icapd – ICAP service for NAS scanning
- lib/webd – https server and Web interface

## Command-line utilities

- bin/[lslog](#) – Logs listing utility
- bin/[odscan](#) – On-demand scanner
- sbin/[cfg](#) – Configuration utility

- `sbin/`[lic](#) – Licensing utility
- `bin/`[upd](#) – Module update utility
- `bin/`[guar](#) – Quarantine management utility
- `sbin/`[setgui](#) – Basic Web interface setup
- `sbin/`[collect\\_logs.sh](#) – Script to generate essential logs as an archive file if requested by ESET customer care

## Troubleshooting

This section describes how to troubleshoot the various issues below.

- [Activation issues \(English only\)](#)
- [Collect logs](#)
- [Forgotten password](#)
- [Update failed](#)
- [Using the noexec flag](#)
- [Real-time protection cannot start](#)
- [Disable Real-time protection at boot](#)
- [Outdated curl library for SMB protocol](#)
- [Custom TMPDIR](#)

## Collect logs

If ESET Technical Support requests logs from ESET Server Security for Linux, use the `collect_logs.sh` script available at `/opt/eset/efs/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/efs/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. 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/efs/sbin/ecp_logging.sh -e
```

alternatively

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

alternatively

```
sudo /opt/eset/efs/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](#).

## Forgotten password

To reset the Web interface password, open a Terminal window on the machine where ESET Server Security for Linux is installed.

- To generate a new password, run the following command with root privileges:

```
/opt/eset/efs/sbin/setgui -g
```

- To define a new password, run the following command with root privileges:

```
/opt/eset/efs/sbin/setgui --password=PASSWORD
```

while PASSWORD is supposed to be replaced with the desired password.

The final output will show the URL address of the Web interface and access credentials.

## Update failed

If for any reason product modules fail to update, information will be provided in the dashboard.

**Recent update attempts failed** - ESET Server Security for Linux has not been able to connect to the update server recently to check for the latest virus signature updates. Check your network connectivity and then try to update the modules again by clicking **Check and update**.

**Detection Engine out of date** - The Detection Engine has not been updated for some time. Check your network connectivity and then try to update the modules again by clicking **Check and update**.

## Using the noexec flag

If you have the `/var` and `/tmp` paths mounted with `noexec` flag and restricted write for `/opt`, the installation of ESET Server Security 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/efs drwxrwxr-x. root eset-efs-daemons
```

2. Execute the following commands:

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

3. Replace */opt/eset/lib/modules* with symlink:

```
# rmdir /opt/eset/lib/modules
# ln -s /opt/eset/lib/modules /usr/lib/efs
```

4. Compile the essential modules:

```
# /opt/eset/efs/bin/upd --compile-nups
```

5. Restart the efs service:

```
# systemctl restart efs
```

If a normal, unprivileged user runs efs utilities, you can get the same error when the user's home directory is mounted noexec.

## Workaround

1. Either allow others to use */opt/eset/lib/modules*

```
# chmod o+rwX /opt/eset/lib/modules
```

- 2a. Or create a folder where exec for specific user is enabled:

```
# mkdir /usr/lib/efs-user
# chown <user>:<user_group> /usr/lib/efs-user
```

```
# chmod 770 /usr/lib/efs-user
```

2b.Run utility with specified MODMAPDIR variable, for example:

```
# MODMAPDIR=/usr/lib/efs-user /opt/eset/efs/bin/lslog -s
```

## Real-time protection cannot start

### Issue

Real-time protection cannot start due to missing kernel files or enabled Secure Boot.

The **Events** screen in the Web interface of ESET Server Security for Linux (ESSL) displays an error message.

TIME	COMPONENT	EVENT
November 30, 2020 3:47 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
November 30, 2020 3:47 PM	Real-time protection service	If you are running UEK kernel, make sure you have kernel-uek-devel installed
November 30, 2020 3:47 PM	Real-time protection service	Cannot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/eset/efs/eset_rtp.ko: No such file or directory

### Missing kernel files

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

### Secure Boot is enabled

In system logs, a corresponding error message is displayed:

```
Nov 30 15:47:02 localhost.localdomain efs[373639]: ESET File Security error: cannot find kernel sources directory for kernel version 5.4.17-2036.100.6.1.el8uek.x86_64
```

```
Nov 30 15:47:02 localhost.localdomain efs[373641]: ESET File Security error: please check if kernel-devel (or linux-headers) package version matches the current kernel version
```

```
Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: Cannot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/eset/efs/eset_rtp.ko: No such file or directory
```

```
Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Warning: If you are running UEK kernel, make sure you have kernel-uek-devel installed
```

```
Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
```

## Missing kernel files

```
Feb 05 14:58:47 ubuntu2004 efs[52262]: ESET File Security Error: Secure Boot requires signed kernel modules. Please run "/opt/eset/efs/lib/install_scripts/sign_modules.sh" to sign our modules.
```

```
Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Secure Boot is enabled. Please sign the kernel module /lib/modules/5.8.0-41-generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.
```

```
Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
```

Secure Boot is enabled

## Solution

If the machine with ESSL installation has Secure Boot enabled, refer to the [Secure Boot section](#).

### Method 1 - Requires operating system restart

1. Upgrade your operating system packages to the latest version. On CentOS 7, execute the following command from a Terminal window as a privileged user:

```
yum upgrade
```

2. Restart the operating system.

### Method 2

1. Install the latest kernel-devel modules (on RPM-based Linux distributions) or the latest linux-headers (on DEB based Linux distributions). On Ubuntu Linux, execute the following command from a Terminal window as a privileged user:

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

2. Restart the ESSL service. Execute the following command from a Terminal window as a privileged user:

```
systemctl restart efs
```

### Method 3 - OS with Unbreakable Enterprise Kernel

If the [Unbreakable Enterprise Kernel](#) is used, the [kernel-uek-devel](#) package must be installed manually.

1. On Oracle Linux, execute the following command from a Terminal window as a privileged user:

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

2. Restart the ESSL service. Execute the following command from a Terminal window as a privileged user:

```
systemctl restart efs
```

## Disable Real-time protection at boot

If a machine protected by ESET Server Security for Linux is slow to respond and the CPU is constantly overloaded, you can disable Real-time protection at boot for troubleshooting purposes.

1. Start the computer and wait for the GRUB menu to appear.
2. Highlight the kernel you want to use and press E.
3. Go down to the line starting with `linux` and add the `eset_rtp=0` parameter to the end of the line.
4. To boot, press CTRL+X.

### NOTE

Modifying the GRUB might slightly differ on some Linux distributions.

## Outdated curl library for SMB protocol

If you try to upload quarantine file using ESET PROTECT, you may get the following error message:

TIME	COMPONENT	EVENT
11/30/2022, 06:21 AM	Scanning service	File 'MyFile' upload to SMB server 'MyServer' failed: CURL: This version of libcurl does not support SMB protocol
11/30/2022, 06:17 AM	Scanning service	File 'MyFile' upload to SMB server 'MyServer' failed: CURL: This version of libcurl does not support SMB protocol

- To use this feature, ensure you have curl version 7.40.0 or later installed on your machine.

## Custom TMPDIR

To change the default temporary directory `/tmp` for ESET Server Security for Linux:

1. Create a custom directory `/efs-tmp` with read and write permission for `eset-efs-daemons`. Execute the following commands from a Terminal window as a privileged user:

```
sudo mkdir /efs-tmp
```

```
sudo chmod g+rw /efs-tmp
```

```
sudo chgrp eset-efs-daemons /efs-tmp/
```



The result should look like this:

```
ls -l /  
  
drwxrwxr-x. 1 root eset-efs-daemons 0 Jan 15 15:56 efs-tmp
```

2. Set environment variable to the configuration file:

```
sudo echo TMPDIR=/efs-tmp >> /opt/eset/efs/etc/systemd/environment
```

3. Restart the product:

```
sudo systemctl restart efs
```

## 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 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\\_home](https://go.eset.com/eol_home). 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.

## **ADDENDUM TO THE AGREEMENT**

**Network Connected Devices Security Assessment.** Additional provisions apply to the Network Connected Devices Security Assessment as follows:

The Software contains a function for checking the security of End User's local network and security of devices in local network which requires local network name and information about devices in local network such as presence, type, name, IP address and MAC address of device in local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. This function may also provide information concerning availability of security software solution to secure devices in local network.

**Protection Against Misuse of Data.** Additional provisions apply to the Protection Against Misuse of Data as follows:

The Software contains a function that prevents loss or misuse of critical data in direct connection with theft of a Computer. This function is switched off under the default settings of the Software. The ESET HOME Account needs to be created for it to be activated, through which the function activates data collection in the event of computer theft. If you chose to activate this function of the Software, data about the stolen Computer will be collected and sent to the Provider, which can include data about the Computer's network location, data about the content displayed on the Computer screen, data about the configuration of the Computer and/or data recorded by a camera connected to the Computer (hereinafter referred to as "Data"). The End User shall be entitled to use Data obtained by this function and provided via ESET HOME Account exclusively for rectifying an adverse situation caused by theft of a Computer. For the sole purpose of this function, Provider process Data as specified in Privacy Policy and in compliance with relevant legal regulations. The Provider shall allow End User to access the Data for the period required to achieve the purpose for which the data was obtained which shall not exceed retention period specified in Privacy Policy. Protection against misuse of data shall be used exclusively with Computers and accounts End User have legitimate access to. Any illegal use will be reported to competent authority. Provider will comply with relevant laws and assist law enforcement authorities in case of the misuse. You agree and acknowledge that You are responsible for safeguarding the password to access ESET HOME Account and you agree that You shall not disclose your password to any third party. End User is responsible for any activity using Protection Against Misuse of Data function and ESET HOME Account, authorized or not. If ESET HOME Account is compromised, notify Provider immediately. Additional provisions for the Protection Against Misuse of Data shall be applicable exclusively to ESET Internet Security and ESET Smart Security Premium End Users.

**ESET Secure Data.** Additional provisions apply to the ESET Secure Data as follows:

1. Definitions. In these additional provisions to the ESET Secure Data the following words have the corresponding meanings:

- a) "Information" any information or data encrypted or decrypted using the software;
- b) "Products" the ESET Secure Data software and the documentation;
- c) "ESET Secure Data" the software(s) used for the encryption and decryption of electronic data;



All references to the plural shall include the singular and all references to the masculine shall include the feminine and neuter and vice versa. Words without specific definition shall be used in compliance with definitions stipulated by the Agreement.

2. Additional End User declaration. You acknowledge and accept that:

- a) It is Your responsibility to protect, maintain and backup Information;
- b) You should fully back-up all information and data (including without limit any critical information and data) on Your Computer before installation of the ESET Secure Data;
- c) You must keep a safe record of any passwords or other information used for setting up and using ESET Secure Data, you must also make backup copies of all encryption keys, license codes, key-files and other data generated to separate storage media;
- d) You are responsible for the use of Products. The Provider shall not be liable for any loss, claim or damage suffered as a consequence of any unauthorized or mistaken encryption or decryption of Information or other data wherever and however that Information or other data is stored;
- e) Whilst Provider has taken all reasonable steps to ensure the integrity and security of the ESET Secure Data, the Products (or any of them) must not be used in any area which is dependent on a fail-safe level of security or is potentially hazardous or dangerous, including but not limited to nuclear facilities, aircraft navigation, control or communication systems, weapon and defense systems and life support or life monitoring systems;
- f) It is End User's responsibility to ensure that the level of security and encryption provided by the products is adequate for Your requirements;
- g) You are responsible for Your use of the Products or any of them, including but not limited to ensure that such use complies with all applicable laws and regulations of the Slovak Republic or such other country, region or state where the Products are used. You must ensure that prior to any use of the Products you have ensured that it is not in contravention of any government (in the Slovak Republic or otherwise) embargo;
- h) ESET Secure Data may contact the Provider servers from time to time in order to check for the license information, available patches, service packs and other updates that may improve, maintain, modify or enhance the operation of ESET Secure Data and may send general system information related to the its functioning in compliance with Privacy Policy.
- i) Provider shall not be responsible for any loss, damage, expense or claim arising from the loss, theft, misuse, corruption, damage or destruction of passwords, set up information, encryption keys, license activation codes and other data generated or stored during use of the software.

Additional provisions for the ESET Secure Data shall be applicable exclusively to ESET Smart Security Premium End Users.

**Password Manager Software.** Additional provisions apply to the Password Manager Software as follows:

1. Additional End User declaration. You acknowledge and accept that You may not:

- a) use Password Manager Software to operate any mission-critical application where human life or property may be at stake. You understand that the Password Manager Software is not designed for such purposes and that its failure in such cases could lead to death, personal injury, or severe property or environmental damage for which Provider is not responsible.

PASSWORD MANAGER SOFTWARE IS NOT DESIGNED, INTENDED OR LICENSED FOR USE IN HAZARDOUS

ENVIRONMENTS REQUIRING FAIL-SAFE CONTROLS INCLUDING, WITHOUT LIMITATION, THE DESIGN, CONSTRUCTION, MAINTENANCE OR OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, AND LIFE SUPPORT OR WEAPONS SYSTEMS. PROVIDER SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH PURPOSES.

b) use Password Manager Software in a manner that breaches this agreement or the laws of the Slovak Republic or your jurisdiction. Specifically you may not use Password Manager Software to conduct or promote any illegal activities including uploading data of harmful content or content that might be used for any illegal activities or that in any way violates the law or the rights of any third party (including any intellectual property rights), including but not limited to any attempts to gain access to accounts in Storage (For the purposes of these additional terms to the Password Manager Software "Storage" refers to the data storage space managed by Provider or a third party other than Provider and the user for the purpose of enabling synchronization and backup of user data) or any accounts and data of other Password Manager Software or Storage users. If you violate any of these provisions, Provider is entitled to immediately terminate this agreement and pass on to you the cost of any necessary remedy, as well as take any necessary steps to prevent you from further use of Password Manager Software without the possibility of refund.

2. LIMITATION OF LIABILITY. PASSWORD MANAGER SOFTWARE IS PROVIDED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE THE SOFTWARE AT YOUR OWN RISK. THE PRODUCER IS NOT LIABLE FOR DATA LOSS, DAMAGES, LIMITATION OF SERVICE AVAILABILITY INCLUDING ANY DATA SENT BY PASSWORD MANAGER SOFTWARE TO EXTERNAL STORAGE FOR THE PURPOSE OF DATA SYNCHRONIZATION AND BACKUP. ENCRYPTING THE DATA USING PASSWORD MANAGER SOFTWARE DOES NOT IMPLY ANY LIABILITY OF THE PROVIDER REGARD-ING THE SECURITY OF THAT DATA. YOU EXPRESSLY AGREE THAT THE DATA ACQUIRED, USED, ENCRYPTED, STORED, SYNCHRONIZED OR SENT USING PASSWORD MANAGER SOFTWARE CAN ALSO BE STORED ON THIRD-PARTY SERVERS (APPLIES ONLY TO THE USE OF PASSWORD MANAGER SOFTWARE WHERE SYNCHRONIZATION AND BACKUP SERVICES HAVE BEEN ENABLED). IF PROVIDER IN ITS SOLE DISCRETION SELECTS TO USE SUCH A THIRD-PARTY STORAGE, WEBSITE, WEB PORTAL, SERVER OR SERVICE, PROVIDER IS NOT LIABLE FOR THE QUALITY, SECURITY, OR AVAILABILITY OF SUCH A THIRD-PARTY SERVICE AND TO NO EXTENT IS PROVIDER LIABLE TO YOU FOR ANY BREACH OF CONTRACTUAL OR LEGAL OBLIGATIONS BY THE THIRD PARTY NOR FOR DAMAGES, LOSS OF PROFITS, FINANCIAL OR NON-FINANCIAL DAMAGES, OR ANY OTHER KIND OF LOSS WHILE USING THIS SOFTWARE. PROVIDER IS NOT LIABLE FOR THE CONTENT OF ANY DATA ACQUIRED, USED, ENCRYPTED, STORED, SYNCHRONIZED, OR SENT USING PASSWORD MANAGER SOFTWARE OR IN STORAGE. YOU ACKNOWLEDGE THAT PROVIDER DOES NOT HAVE ACCESS TO THE CONTENT OF THE STORED DATA AND IS NOT ABLE TO MONITOR IT OR REMOVE LEGALLY HARMFUL CONTENT.

Provider owns all rights to improvements, upgrades and fixes related to Password Manager Software ("Improvements") even in the event that any such Improvements have been created based on feedback, ideas or suggestions submitted by you in any form. You will not be entitled to any compensation, including any royalties related to such Improvements.

PROVIDER ENTITIES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR CLAIMS AND LIABILITIES OF ANY KIND ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF PASSWORD MANAGER SOFTWARE BY YOU OR BY THIRD PARTIES, TO THE USE OR NON-USE OF ANY BROKERAGE FIRM OR DEALER, OR TO THE SALE OR PURCHASE OF ANY SECURITY, WHETHER SUCH CLAIMS AND LIABILITIES ARE BASED ON ANY LEGAL OR EQUITABLE THEORY.

PROVIDER ENTITIES AND LICENSORS ARE NOT LIABLE TO YOU FOR ANY AND ALL DIRECT, INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO ANY THIRD-PARTY SOFTWARE, ANY DATA ACCESSED THROUGH PASSWORD MANAGER SOFTWARE, YOUR USE OR INABILITY TO USE OR ACCESS PASSWORD MANAGER SOFTWARE, OR ANY DATA PROVIDED THROUGH PASSWORD MANAGER SOFTWARE, WHETHER SUCH DAMAGE CLAIMS ARE BROUGHT UNDER ANY THEORY OF LAW OR EQUITY. DAMAGES EXCLUDED BY THIS CLAUSE INCLUDE, WITHOUT LIMITATION, THOSE FOR LOSS OF BUSINESS PROFITS, INJURY TO PERSON OR PROPERTY, BUSINESS INTERRUPTION, LOSS OF BUSINESS OR PERSONAL INFORMATION. SOME JURISDICTIONS DO

NOT ALLOW LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS RESTRICTION MAY NOT APPLY TO YOU. IN SUCH CASE THE EXTENT OF PROVIDER LIABILITY WILL BE THE MINIMUM PERMITTED UNDER APPLICABLE LAW.

INFORMATION PROVIDED THROUGH PASSWORD MANAGER SOFTWARE, INCLUDING STOCK QUOTES, ANALYSIS, MARKET INFORMATION, NEWS, AND FINANCIAL DATA, MAY BE DELAYED, INACCURATE, OR CONTAIN ERRORS OR OMISSIONS, AND PROVIDER ENTITIES AND LICENSORS WILL HAVE NO LIABILITY WITH RESPECT THERETO. PROVIDER MAY CHANGE OR DISCONTINUE ANY ASPECT OR FEATURE OF PASSWORD MANAGER SOFTWARE OR THE USE OF ALL OR ANY FEATURES OR TECHNOLOGY IN PASSWORD MANAGER SOFTWARE AT ANY TIME WITHOUT PRIOR NOTICE TO YOU.

IF THE PROVISIONS IN THIS ARTICLE ARE VOID FOR ANY REASON OR PROVIDER IS DEEMED LIABLE FOR LOSSES, DAMAGES ETC UNDER APPLICABLE LAWS, THE PARTIES AGREE THAT PROVIDER'S LIABILITY TO YOU WILL BE LIMITED TO THE TOTAL AMOUNT OF LICENSE FEES PAID BY YOU.

YOU AGREE TO INDEMNIFY, DEFEND AND HOLD HARMLESS PROVIDER AND ITS EMPLOYEES, SUBSIDIARIES, AFFILIATES, REBRANDING AND OTHER PARTNERS FROM AND AGAINST ANY AND ALL THIRD PARTY (INCLUDING OWNERS OF THE DEVICE OR PARTIES WHOSE RIGHTS WERE AFFECTED BY THE DATA USED IN PASSWORD MANAGER SOFTWARE OR IN STORAGE) CLAIMS, LIABILITIES, DAMAGES, LOSSES, COSTS, EXPENSES, FEES THAT SUCH PARTIES MAY INCUR AS A RESULT OF YOUR USE OF THE PASSWORD MANAGER SOFTWARE.

3. Data in Password Manager Software. Unless otherwise, and explicitly, selected by you, all data entered by you that is saved into a Password Manager Software database is stored in encrypted format on your computer, or other storage device as defined by you. You understand that in the case of deletion of, or damage to, any Password Manager Software database or other files, all the data contained therein will be irreversibly lost and you understand and accept the risk of such loss. The fact that your personal data is stored in encrypted format on the computer does not mean that the information cannot be stolen or misused by someone who discovers the Master Password or gains access to the customer-defined activation device for opening the database. You are responsible for maintaining the security of all access methods.

4. Transmission of Personal Data to Provider or Storage. If You select so and solely for the purpose of ensuring timely data synchronization and backup, Password Manager Software transmits or sends personal data from the Password Manager Software database - namely passwords, login information, Accounts and Identities to Storage over the Internet. Data is transmitted exclusively in encrypted form. The use of Password Manager Software for filling in online forms with passwords, logins or other data may require that information being sent over the Internet to the website identified by You. This transmission of data is not initiated by Password Manager Software and therefore Provider cannot be held responsible for the security of such interactions with any website operated by various providers. Any transactions over the Internet whether or not in conjunction with Password Manager Software is done at Your own discretion and risk, and You will be solely responsible for any damage to Your Computer or loss of data resulting from the download and/or use of any such material or service. To minimize the risk of losing valuable data, Provider recommends that End User perform periodic backup of the database and other sensitive files to external drives. Provider is not able to provide You with any assistance in recovering lost or damaged data. If Provider provides backup services for End User database files in case of damage or deletion of the files on End User's Computer, such backup service is without any warranty and does not imply any liability of Provider to you whatsoever.

By using Password Manager Software, you agree that the software may contact the Provider servers from time to time in order to check for the license information, available patches, service packs and other updates that may improve, maintain, modify or enhance the operation of Password Manager Software. The software may send general system information related to the functioning of Password Manager Software in compliance with Privacy Policy.

5. Uninstall information and instructions. Any information that you would like to retain from the database must

be exported prior to uninstalling Password Manager Software.

Additional provisions for the Password Manager Software shall be applicable exclusively to ESET Smart Security Premium End Users.

**ESET LiveGuard.** Additional provisions apply to the ESET LiveGuard as follows:

The Software contains a function of additional analysis of files submitted by End User. The Provider shall only use the files submitted by End User and results of analysis in compliance with Privacy Policy and in compliance with relevant legal regulations.

Additional provisions for the ESET LiveGuard shall be applicable exclusively to ESET Smart Security Premium End Users.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

## Privacy Policy

The protection of personal data is of particular importance to 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"). We want to comply with the transparency requirement as legally standardized under the EU General Data Protection Regulation ("GDPR"). To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") as a data subject about following personal data protection topics:

- Legal Basis of Personal Data Processing,
- Data Sharing and Confidentiality,
- Data Security,
- Your Rights as a Data Subject,
- Processing of Your Personal Data
- Contact Information.

## Legal Basis of Personal Data Processing

There are a few legal bases for data processing which We use according to the applicable legislative framework related to protection of personal data. The processing of personal data at ESET is mainly necessary for the performance of the [End User License Agreement](#) ("EULA") with End User (Art. 6 (1) (b) GDPR), which is applicable for the provision of ESET products or services, unless explicitly stated otherwise, e.g.:

- Legitimate interest legal basis (Art. 6 (1) (f) GDPR), that enables us to process data on how our customers use our Services and their satisfaction to provide our users with the best protection, support and experience We can offer. Even marketing is recognized by applicable legislation as a legitimate interest, therefore We usually rely on it for marketing communication with our customers.
- Consent (Art. 6 (1) (a) GDPR), which We may request from You in specific situations when we deem this legal basis as the most suitable one or if it is required by law.

- Compliance with a legal obligation (Art. 6 (1) (c) GDPR), e.g. stipulating requirements for electronic communication, retention for invoicing or billing documents.

## Data Sharing and Confidentiality

We do not share your data with third parties. However, ESET is a company that operates globally through affiliated companies or partners as part of our sales, service and support network. Licensing, billing and technical support information processed by ESET may be transferred to and from affiliates or partners for the purpose of fulfilling the EULA, such as providing services or support.

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these countries does not require any special authorization or agreement.

## Data Security

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 the relevant supervisory authority as well as affected End Users as data subjects.

## Data Subject's Rights

The rights of every End User matter and We would like to inform you that all End Users (from any EU or any non-EU country) have the following rights guaranteed at ESET. To exercise your data subject's rights, you can contact us via support form or by e-mail at [dpo@eset.sk](mailto:dpo@eset.sk). For identification purposes, we ask you for the following information: Name, e-mail address and - if available - license key or customer number and company affiliation. Please refrain from sending us any other personal data, such as the date of birth. We would like to point out that to be able to process your request, as well as for identification purposes, we will process your personal data.

**Right to Withdraw the Consent.** Right to withdraw the consent is applicable in case of processing based on consent only. If We process your personal data on the basis of your consent, you have the right to withdraw the consent at any time without giving reasons. The withdrawal of your consent is only effective for the future and does not affect the legality of the data processed before the withdrawal.

**Right to Object.** Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

Please note that in some cases, despite your consent withdrawal, we are entitled to further process your personal data on the basis of another legal basis, for example, for the performance of a contract.

**Right of Access.** As a data subject, you have the right to obtain information about your data stored by ESET free of charge at any time.

**Right to Rectification.** If we inadvertently process incorrect personal data about you, you have the right to have this corrected.

**Right to Erasure and Right to Restriction of Processing.** As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

If we use your personal data for the sole purpose of direct marketing and you have revoked your consent or objected to the underlying legitimate interest of ESET, We will restrict the processing of your personal data to the extent that we include your contact data in our internal black list in order to avoid unsolicited contact. Otherwise, your personal data will be deleted.

Please note that We may be required to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities. Retention obligations and periods may also result from the Slovak legislation. Thereafter, the corresponding data will be routinely deleted.

**Right to Data Portability.** We are happy to provide You, as a data subject, with the personal data processed by ESET in the xls format.

**Right to Lodge a Complaint.** As a data subject, You have a right to lodge a complaint with a supervisory authority at any time. ESET is subject to the regulation of Slovak laws and We are bound by data protection legislation as part of the European Union. The relevant data supervisory authority is The Office for Personal Data Protection of the Slovak Republic, located at Hraničná 12, 82007 Bratislava 27, Slovak Republic.

## Processing of Your Personal Data

Services provided by ESET implemented in our product are provided under the terms of [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 the product [documentation](#). To make it all work, We need to collect the following information:

**Licensing and Billing Data.** The name, e-mail address, license key and (if applicable) address, company affiliation and payment data are collected and processed by ESET in order to facilitate the activation of license, license key delivery, reminders on expiration, support requests, license genuineness verification, provision of our service and other notifications including marketing messages in line with applicable legislation or Your consent. ESET is legally obliged to keep the billing information for the period of 10 years, however the licensing information will be anonymized no later than 12 months after the expiration of license.

**Update and Other Statistics.** The processed information includes 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 are processed for the purpose of provision update and upgrade services and for the purpose of maintenance, security and improvement of our backend infrastructure.

This information is kept apart from the identification information required for the licensing and billing purposes since it does not require the identification of End User. The retention period is up to 4 years.

**ESET LiveGrid® Reputation System.** One-way hashes related to infiltration are processed for the purpose 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. The End User is not identified during this process.

**ESET LiveGrid® Feedback System.** Suspicious samples and metadata from the wild are collected 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 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 our 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.

All information obtained and processed through the ESET LiveGrid® Feedback System are meant to be used without the identification of End User.

**Network Connected Devices Security Assessment.** To provide the security assessment function, We process the local network name and information about devices in your local network, such as presence, type, name, IP address and MAC address of the device in your local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. The license information identifying the End User will be anonymized no later than 12 months after the expiration of the license.

**Technical Support.** The contact and licensing 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. The data processed for technical support is stored for 4 years.

**Protection Against Misuse of Data.** If the ESET HOME Account on <https://home.eset.com> is created and the function is activated by End User in connection with theft of computer, following information will be collected and processed: the location data, screenshots, data about the configuration of computer and data recorded by computer's camera. The collected data are stored on our servers or on the servers of our service providers with retention period of 3 months.

**Password Manager.** If You choose to activate the function of Password Manager, the data related to your login details are stored in an encrypted form only on your computer or other designated device. If You activate the synchronization service, the encrypted data are stored on our servers or on the servers of our service providers to ensure such service. Neither ESET nor the service provider have access to the encrypted data. Only You have the key to decrypt the data. The data will be removed upon the deactivation of the function.

**ESET LiveGuard.** If You choose to activate the ESET LiveGuard function, it requires the submission of samples such as files predefined and selected by the End User. The samples You choose for the remote analysis will be uploaded to the ESET service, and the result of the analysis will be sent back to Your computer. Any suspicious samples are processed in the manner of information collected by ESET LiveGrid® Feedback System.

**Customer Experience Improvement Program.** If You chose to activate [Customer Experience Improvement Program](#) , the anonymous telemetry information relating to the use of Our products will be collected and used, based on Your consent.

Please note that if the person using our products and services is not the End User who has purchased the product or service and concluded the EULA with Us, (e.g. an employee of the End User, a family member or a person otherwise authorized to use the product or service by the End User in compliance with EULA, the processing of the data is carried out in the legitimate interest of ESET within the meaning of Art. 6 (1) f) GDPR to enable the user authorized by End User to use the products and services provided by Us in accordance with EULA.

## Contact Information

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](mailto:dpo@eset.sk)