ESET File Security for Linux

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

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

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

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

REV. 7/25/2022

Introduction

ESET's state-of-the-art scanning engine has unsurpassed scanning speed and detection rates combined with a very small footprint that makes ESET File Security for Linux (EFSL) the ideal choice for any server on Linux.

Main functionality is covered by the On-demand scanner and On-access scanner.

The On-demand scanner can be started by a privileged user (usually a system administrator) through the command line interface, the web interface or by the operating system's automatic scheduling tool (e.g., 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 and/or operating system attempts to access file system objects. This also clarifies the use of the term On-access; because 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
- SELinux support
- Quarantine
- Manageable via ESET Security Management Center

Release notes

ESET File Security for Linux version 7.2 hotfix (7.2.578)

- Fixed: A potential vulnerability in the on-access scanner - reported internally
- Fixed: Memory leak could occur under special circumstances
- Fixed: On-demand scan issues resulted in a system freeze

ESET File Security for Linux version 7.2 hotfix

- New: Ability to check for an update of application via the upd command-line utility or from the WebGUI.
- New: Ability to enable automatic update of application during server restart

- New: Support for Ubuntu 20.04 LTS
- New: Support for RedHat Enterprise Linux (RHEL) 8
- New: Support for CentOS 8
- New: Support for Debian 10
- New: Support of ICAP scanning for Nutanix
- New: Support for EncFS file system
- Improved: Performance and system footprint of real-time protection scanner
- Improved: Changes in WebGUI settings needs to be confirmed or discarded before leaving settings section
- SELinux compatibility on CentOS
- Fixed: On-demand scan enabled from WebGUI might not remove all detections if they exist in separate partitions
- Fixed: Real-time protection scanner could slow down a machine during the boot process in certain scenarios
- Fixed: Error "Cannot accept the connection" when too many connections were opened to icapd
- Fixed: Enabling "Shut down computer after scan" task from ESMC did not work
- Fixed: A rare kernel crash could occur when unloading modules
- Removed: Support for rspamd spam filtering system
- Other minor bug fixes and optimizations

ESET File Security for Linux version 7.1 hotfix

- New: Added ICAP scanning support for Citrix ShareFile
- New: Updated Software End User License Agreement
- Improved: Performance of Real-time protection scanner
- Improved: Odscan utility in command line is able to return status of On-demand scan as exit code
- Fixed: An issue causing excessive error logging into syslog
- Fixed: An issue causing excessive error logging into event log during update
- Fixed: An issue where activation with offline licenses did not work
- Fixed: Some words in the scan detail page in WebGUI were not translated
- Fixed: Other minor bug fixes and improvements

ESET File Security for Linux version 7.1

- New: Scheduler - the ability to schedule an on-demand scan through Web interface or an ESET Security Management Center policy
- New: List of files which were not scanned during an on-demand scan (for example, password-protected files) is available in scan details
- New: Support for changed exclusions workflow in upcoming ESET Security Management Center 7.1 release
- New: Support for subscription licenses
- New: Ability to "Restore and Exclude" quarantined samples through Web interface
- New: Automatic log maintenance
- Improved: Output of modules date and versions in terminal
- Improved: Update of third-party components
- Improved: List of on-demand scans triggered by ESET Security Management Center console
- Improved: More clear error messages
- Fixed: Compatibility issues with SSSD on SELinux
- Fixed: Activation on SELinux via Http proxy
- Fixed: SELinux denies port change of ICAP and Web interface
- Fixed: "Log all objects" setting has been removed temporarily
- Fixed: Cannot change ESET File Security for Linux Web interface password through ESET Security Management Center
- Fixed: Web interface improvements
- Fixed: Bug fixes & many under-the-hood optimizations regarding performance and stability

System requirements

Hardware requirements depend on the server role. The following minimum hardware requirements must be met before the installation process in order to run ESET File Security for Linux properly:

- processor Intel/AMD x64
- 700MB of free hard disk space
- 256MB of free RAM
- glibc 2.12 or later

- 2.6.32 and later Linux OS kernel versions
- Any locale with UTF-8 encoding

ESET File Security for Linux has been tested and is supported on the listed operating systems' latest minor releases. Update your operating system before installing efs.

- RedHat Enterprise Linux (RHEL) 6 64-bit
- RedHat Enterprise Linux (RHEL) 7 64-bit
- RedHat Enterprise Linux (RHEL) 8 64-bit
- CentOS 6 64-bit
- CentOS 7 64-bit
- Centos 8 64-bit
- Ubuntu Server 16.04 LTS 64-bit
- Ubuntu Server 18.04 LTS 64-bit
- Ubuntu Server 20.04 LTS 64-bit
- Debian 9 64-bit
- Debian 10 64-bit
- SUSE Linux Enterprise Server (SLES) 12 64-bit
- SUSE Linux Enterprise Server (SLES) 15 64-bit

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

AWS and ELREPO kernels

Linux distributions with AWS or ELREPO kernel are not supported.

ESET File Security for Linux should also work on the most recent and frequently used open-source Linux distributions if:

- the hardware requirements criteria above are met,
- and software dependencies are not missing in the Linux distribution used.

NOTE
Secure Boot is not supported.

Remote management via ESET Security Management Center.

Supported browsers

The ESET File Security for Linux Web interface works in the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

SELinux support

SELinux is supported in the following distributions:

- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- Centos 6
- Centos 7
- Centos 8

Installation of EFS SELinux module policy requires selinux-policy-devel package to be installed. To start the OS without ESET File Security for Linux SELinux module, use the `eset_selinux=0` kernel parameter during OS boot.

Installation

ESET File Security for Linux is distributed as a binary file (*.bin*).

NOTE
Make sure your OS has the most recent updates installed before installation of ESET File Security for Linux.

Remove version 4.x first
If you have ESET File Security for Linux version 4.x installed, remove it first. Version 7.x is not compatible with version 4.x.
If you have been using ESET Remote Adminstrator to manage ESET File Security for Linux version 4, upgrade to ESET Security Management Center in order to manage version 7 remotely.

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-<VERSION>.x86_64.bin`
- `sh ./efs-<VERSION>.x86_64.bin`

See available command-line arguments.

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

```
bash ./efs-<VERSION>.x86_64.bin -h
```

Available parameters

Short form	Long form	Description
`-h`	`--help`	Display command-line arguments
`-n`	`--no-install`	Do not perform installation after unpacking
`-y`	`--accept-license`	Do not show the license, license has been accepted
`-f`	`--force-install`	Force installation via package manager without asking
`-g`	`--no-gui`	Do not setup/start GUI after installation

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-<VERSION>.x86_64.bin -n
```

or

```
sudo sh ./efs-<VERSION>.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. Once you accept the product License Agreement, installation will complete and displays the Web interface login details.

The installer would inform you of any dependency problems.

Installation via ESET Security Management Center (ESMC)

To deploy ESET File Security for Linux remotely on your computers, refer to the ESMC Software Install online help section.

To enable regular updates of detection modules, activate ESET File Security for Linux.

If needed, enable the Web interface remotely.

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

Uninstall

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

Ubuntu/Debian based distributions:

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

Red Hat based distributions:

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

Mass deployment

This topic provides a high-level overview of mass deployment of ESET File 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 File Security for Linux, you have to decide which package to use. ESET File 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-7.0.1081.0.x86_64.bin":
           mode => "0700",
           owner => "root",
           group => "root",
           source => "puppet:///modules/efs/efs-7.0.1081.0.x86_64.bin"
         }
    exec {"Execute bin package installation":
           command => '/tmp/efs-7.0.1081.0.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-7.0.1081.0.x86_64.deb":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/efs/efs-7.0.1081.0.x86_64.deb"
             }
        package {"efs":
               ensure => "installed",
               provider => 'dpkg',
               source => "/tmp/efs-7.0.1081.0.x86_64.deb"
             }
 }
if $osfamily == 'RedHat' {

        file {"/tmp/efs-7.0.1081.0.x86_64.rpm":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/efs/efs-7.0.1081.0.x86_64.rpm"
             }

        package {"efs":
               ensure => "installed",
               provider => 'rpm',
               source => "/tmp/efs-7.0.1081.0.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-7.0.1084.0.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-7.0.1084.0.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-7.0.1084.0.x86_64.deb' do
        source 'efs-7.0.1084.0.x86_64.deb'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
        only_if { node['platform_family'] == 'debian'}
end

cookbook_file '/tmp/efs-7.0.1084.0.x86_64.rpm' do
                source 'efs-7.0.1084.0.x86_64.rpm'
                owner 'root'
                group 'root'
                mode '0700'
                action :create
                only_if { node['platform_family'] == 'rhel'}

dpkg_package 'efsu' do
        source '/tmp/efs-7.0.1084.0.x86_64.deb'
        action :install
        only_if { node['platform_family'] == 'debian'}
end

rpm_package 'efsu' do
        source '/tmp/efs-7.0.1084.0.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-7.0.1084.0.x86_64.bin
    dest: /home/ansible/

- name : "Install product bin package"
  shell: bash ./efs-7.0.1084.0.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-7.0.1085.0.x86_64.deb
          dest: /home/ansible/efs-7.0.1085.0.x86_64.deb
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "Debian"

      - name: "Copy rpm package to VM"
        copy:
          src: ./efs-7.0.1085.0.x86_64.rpm
          dest: /home/ansible/efs-7.0.1085.0.x86_64.rpm
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "RedHat"

      - name: "Install deb package"
        apt:
          deb: /home/ansible/efs-7.0.1085.0.x86_64.deb
          state: present
        when:
          - ansible_os_family == "Debian"

      - name: "Install rpm package"
        yum:
          name: /home/ansible/efs-7.0.1085.0.x86_64.rpm
          state: present
        when:
          - ansible_os_family == "RedHat"
....
```

Update and upgrade

Update of modules

Product modules, including detection modules, are updated automatically.

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

If an ESET File Security for Linux update was not stable, roll back the module updates to a previous state. Click **Dashboard** > **Modules 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 *
	`--server=ADDRESS`	Update server address
	`--username=USERNAME`	Username to authenticate update eligibility
	`--password=PASSWORD`	Password to authenticate update eligibility
	`--proxy-addr=ADDRESS`	Proxy server address
	`--proxy-port=PORT`	Proxy server port
	`--proxy-username=USERNAME`	Username to access the proxy server protected by username/password
	`--proxy-password=PASSWORD`	Password to access the proxy server protected by username/password
	`--update-server-type=UPDATE_TYPE`	Type of update server
	`--list-update-server-type`	List of available types of update servers
	`--check-app-update`	Check the availability of new product version in the repository**
	`--download-app-update`	Download new product version if available**
	`--perform-app-update`	Download and install new product version if available**
	`--accept-license`	Accept license changes**

* - available from ESET File Security for Linux version 7.1

** - available from ESET File Security for Linux version 7.2

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

Example

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

```
sudo /opt/eset/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 File Security for Linux to a later version

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

Note
An upgrade from ESET File Security for Linux version 4 to version 7 is not possible. A clean new installation is needed. The settings from version 4 cannot be imported to version 7.

Which product version is currently installed?

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

1. In the Web interface, navigate to **Help** > **About**.
2. Execute `/opt/eset/efs/sbin/setgui -v` in a Terminal window.

How to upgrade ESET File Security for Linux?

Local options

- Run an OS-related installation package as described in the Installation section

- In the Web interface, navigate to **Dashboard** > **Product update**, click **Check for update**
- Use the `upd` utility with the `--perform-app-update` parameter
- Configure automatic updates/upgrades

Remote management via ESET Security Management Center (ESMC)

If managing ESET File Security for Linux through ESMC, you can initiate upgrade the following ways:

- Software install task
- In the Web interface, navigate **Dashboard** > **ESET Applications** > right-click ESET File Security for Linux > **Update installed ESET products...**
- Configure automatic updates/upgrades

Update mirror

Several ESET security products (ESET Security Management Center, 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 File Security for Linux to use an update mirror

1. In the Web interface navigate to **Setup** > **Update** > **Primary Server**.
2. In the **Basic** section, switch 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>`
   b. `http://<hostname>:<port>`
4. Enter 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.

Automatic product component updates

In ESET File Security for Linux version 7.2 you can activate automatic product component updates, including upgrade to later product versions:

1. In the Web interface, navigate to **Setup** > **Update**.
2. In the **Program Component Update** section, select **Auto-update** from the **Update mode** list-box.
3. If you prefer to use a custom update server for product component updates:
    a.Define the server address in the **Custom server** field.
    b.Enter the **Username** and **Password** in the corresponding fields.
4. Click **Save**.

If managing ESET File Security for Linux via ESET Security Management Center, configure the above mentioned automatic updates through Policies.

To alter the configuration of ESET File Security for Linux:

1. In ESET Security Management Center click **Policies** > **New policy** and type a name for the policy.
2. Click **Settings**, and select **ESET Endpoint for Linux (V7+)** from the drop-down menu.
3. Adjust the desired settings and click **Save** in each dialog where you made a change.
4. Click **Finish**.

Update mode

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

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

Activate ESET File Security for Linux

Activate your ESET File Security for Linux using a license obtained from your ESET distributor.

Activate using Web interface

1. Log in to the Web interface
2. Click **Dashboard** > **License** tile and select the desired method of activation:
    a.**Activate with License Key**
    b.**Offline license**

c. **ESET Security Management Center**

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

Activate using Terminal

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

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

Example

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

```
/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 File Security for Linux License Key.

Activate using ESET Security Management Center (ESMC)

Log in to ESMC Web interface, navigate to **Client Tasks** > **Product Activation**, and follow the instructions on Product Activation.

Once the activation is complete, access the Web interface to launch the initial scan of your system or to configure ESET File 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-xxxxxxxxxx) and Password when applicable, Public License ID (xxx-xxx-xxx), product name (or list of products) and quantity.

I have a Username and a Password

If you have a Username and a Password, convert them to a License Key at the ESET Business Account License converter page:

https://eba.eset.com/LicenseConverter

Check the activation status

The functionality described below is available in ESET File Security for Linux version 7.2 and later.

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]`

Example

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
```

Using ESET File Security for Linux

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
- Polish

If you complete the installation of ESET File Security for Linux remotely via ESET Security Management Center, the Web interface is not enabled.
If you want to access the Web interface on the particular 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 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 Security Management Center, 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

ESET File Security for Linux Web Interface certificate

ESET File Security for Linux Web console 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:

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 EFSL Web interface> (unsafe)**.
3. At this point Google Chrome remembers the exception.

To use your own SSL certificate for the Web interface, generate a certificate and import it to ESET File 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 File Security for Linux:

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

If you activated your instance of ESET File Security for Linux, update the detection modules (click **Dashboard > Module update > Check and update**) and run an initial scan of your file system.

Dashboard

The **Dashboard** provides an overview of protection status, module updates, license information and product activation options, and displays a summary of notifications.

Protection status

When everything is working without any issues, the protection status is green. If there are options to improve the protection status of your system, or insufficient protection status is detected, you will see "Attention required" on the **Protection status** tile. Click the tile to see the details.

> **Mute or un-mute protection status alerts**
> Each non-green protection status alert can be muted by clicking **Mute this alert**. The protection module status will turn grey, and the protection module tile will be moved to the bottom of the list. Click **Un-mute this alert** to turn the status notification back on.
> If the protection status is disabled via ESET Security Management Center, neither **Un-mute this alert**, nor **Enable** is available in the **Dashboard**.

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.

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.

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. Select **Scan exclusions** to scan everything, including the configured 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** - This tab is available from ESET File Security for Linux version 7.1. Displays the details and reason of files that could not be scanned.

Run On-demand scan from a Terminal window

To run on-demand scan from a Terminal window, use the /opt/eset/efs/bin/odscan command

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

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`
`-s`	`--scan`	Start scan
	`--profile=PROFILE`	Scan with selected PROFILE
	`--profile-priority=PRIORITY`	Task will be run with the specified priority. Priority can be: normal, lower, lowest, idle
	`--readonly`	Scan without cleaning
	`--local`	Scan local drives
	`--network`	Scan network drives
	`--removable`	Scan removable media
	`--boot-local`	Scan the boot sectors of local drive
	`--boot-removable`	Scan the boot sectors of removable media
	`--boot-main`	Scan the main boot sector
	`--exclude=FILE`	Skip selected file or directory
	`--ignore-exclusions`	Scan also excluded paths and extensions

Exit codes available from version 7.1.561

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

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

Some exclusions and exclusion paths work differently in ESET File Security for Linux version 7.0 and 7.1+.

File extension exclusions

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

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)

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 other separator you selected.

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

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

Exclusions in ESET File Security for Linux version 7.1+

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.

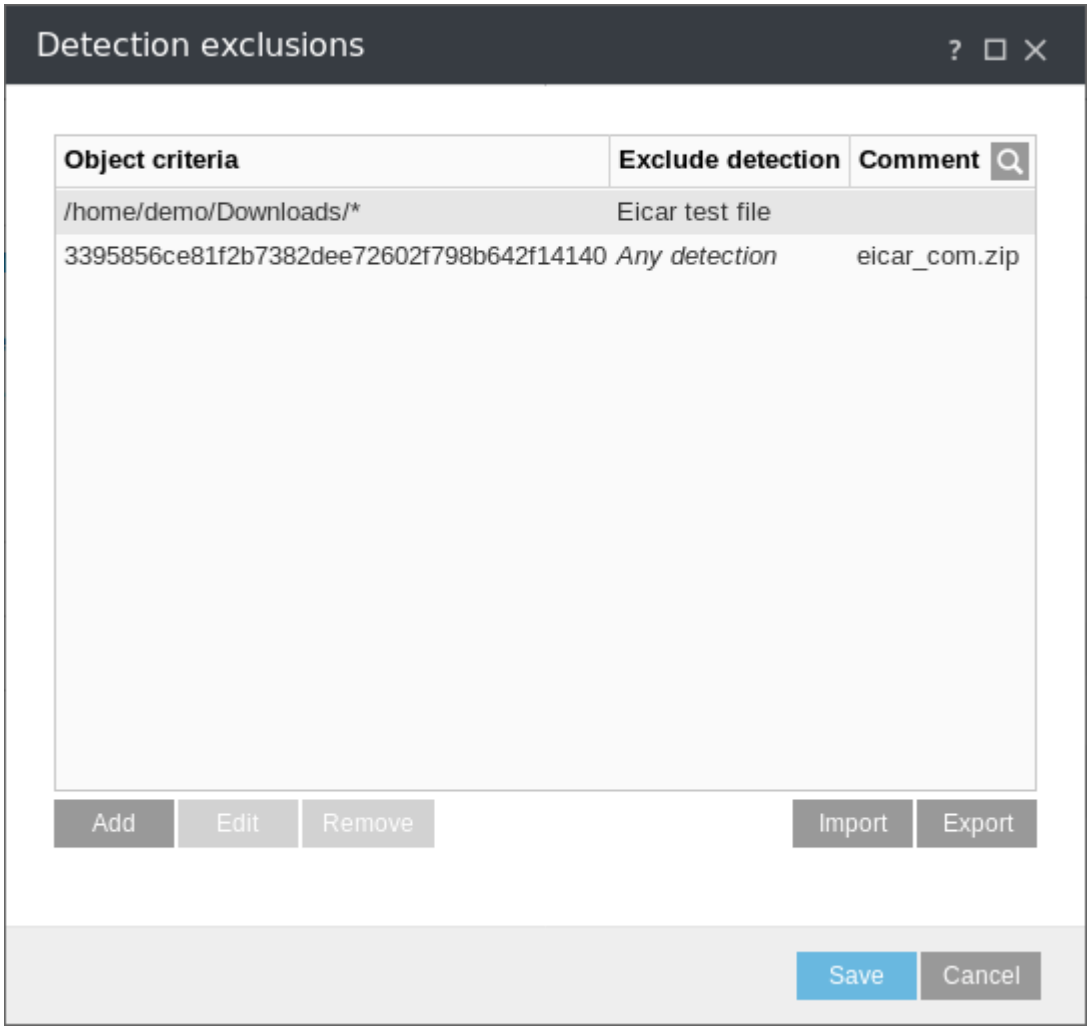
5. Click **Save** to save the changes.

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

- **Path** – Detection exclusion for a specified path (or any if left empty).

- **Detection name** – A detected object will be excluded only if matches the defined detection name. If the file becomes infected later with other malware, so its detection name will not match the one in an exclusion rule anymore, it will be detected as an infiltration and proper action will be taken against it. This type of exclusion can only be used for certain types of detections. To add such detections to the exclusion list, navigate to **Quarantine**, right-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 its extension.

Exclusion paths

For ESET File Security for Linux v7.2

*/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.

For ESET File Security for Linux v7.1

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

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

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

For ESET File Security for Linux v7.0

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

/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.

Exclusions in ESET File Security for Linux version 7.0

File and folder exclusion

This type of exclusions can help you to exclude desired files from being scanned for presence of malicious software.

1. In the Web interface, click **Setup > Detection Engine > Basic**.
2. Next to **Exclusions**, click **Edit**.
3. Click **Add** and select the exclusion type:
   - **Exclude path** - Define the path to be excluded from the scan.
   - **Exclude hash** - Define the hash of the file to be excluded.
   - **Exclude detection** - Define the exact name of the threat (detection) to be ignored during scan, and optionally define a path mask.

- If left empty, every threat with the selected threat name is excluded.
- If a path to a directory is defined, every threat with the selected threat name in the defined directory and its sub-directories is excluded.

- If a path to a file is defined, only the specific file with the selected threat name is excluded.

4. Define a single entity (for example, path, hash, or threat).
5. Click **OK**, then click **Save** to close the dialog.
6. Click **Save** to save the changes.

Detections

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

If a threat has been detected, but not cleaned, the whole row will by highlighted red. To attempt cleaning of a detected malicious file, click the particular row, select **Rescan with cleaning**.

To locate the file that has been detected as malicious, but not deleted yet, click the related row, select **Copy path** and use a file browser to look up the file.

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 File 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: the date and time of quarantine, the path to the original location of the quarantined file, reason of moving the file to quarantine, number of threats (for example, if it is an archive containing multiple infiltrations), and size of quarantined item.

Click the quarantined item to display the available actions: **Restore**, **Restore and Exclude**, **Copy path**, **Download**, **Delete from quarantine**.

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/*

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

Options - short form	Options - long form	Description
`-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
`-f`	`--follow`	Wait for new items and append them to the output
	`--restore-path=path`	New path to restore a quarantined item to
`-h`	`--help`	Show help and quit.
`-v`	`--version`	Show version information and quit

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 "123456789" which is marked "**x**" in the **excludable** column to the *Download* folder:

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

or

```
/opt/eset/efs/bin/quar --restore-exclude=9876543210 --restore-
```

```
path=/home/$USER/Download/
```

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
```

Events

Important actions taken in ESET File Security for Linux Web interface, failed login attempts to Web interface, ESET File 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 occured, 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
`-s`	`--scans`	List On-Demand scan logs
`-d`	`--detections`	List Detection Log records

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
```

Configuration

To alter the default configuration of ESET File 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 File 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 File 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
`-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
- 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
- Turn on Shared local cache

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

Exclusions

Some exclusions and exclusion paths work differently in ESET File Security for Linux version 7.0 and 7.1+.

File extension exclusions

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

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)

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 other separator you selected.
5. Click **OK**, then click **Save** to close the dialog.
6. Click **Save** to save the changes.

Exclusions in ESET File Security for Linux version 7.1+

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.

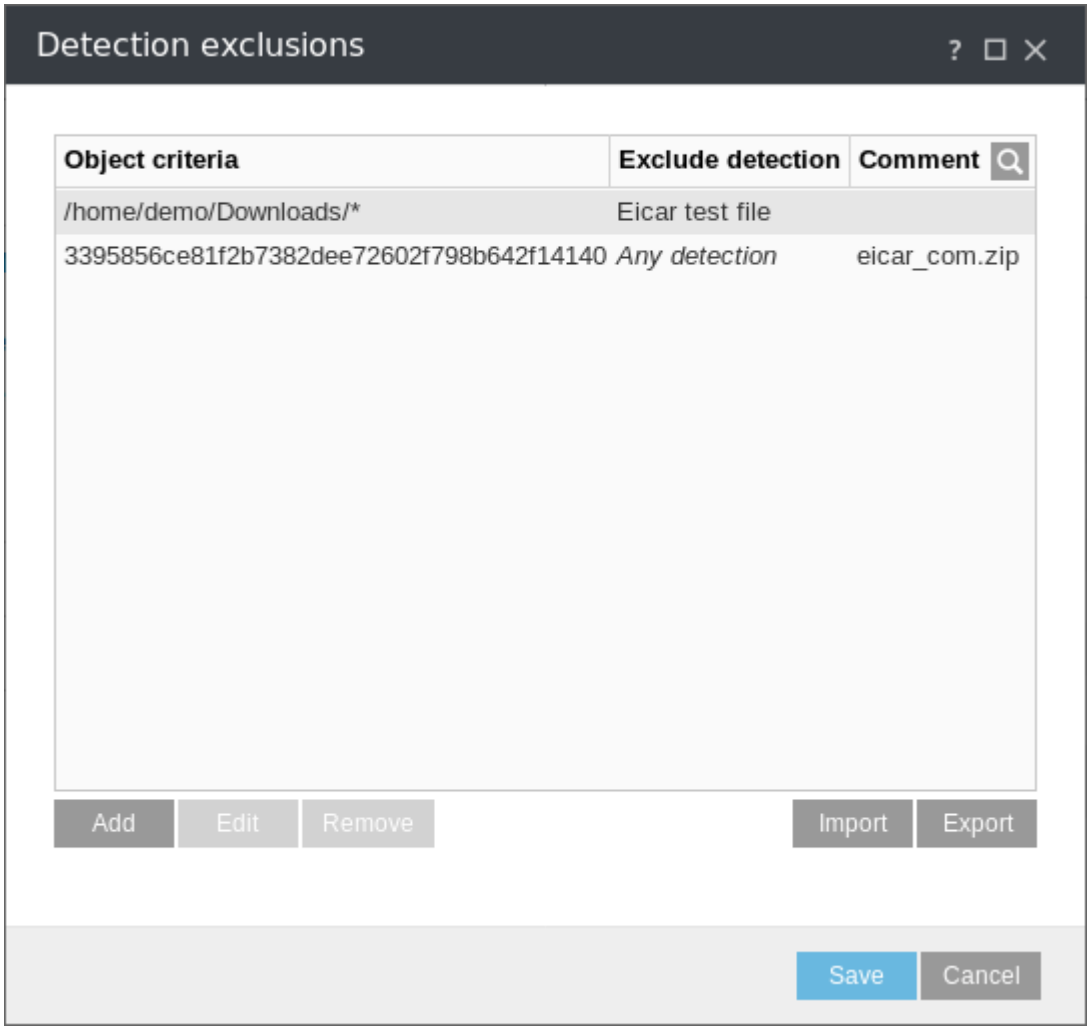
5. Click **Save** to save the changes.

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

- **Path** – Detection exclusion for a specified path (or any if left empty).
- **Detection name** – A detected object will be excluded only if matches the defined detection name. If the file

becomes infected later with other malware, so its detection name will not match the one in an exclusion rule anymore, it will be detected as an infiltration and proper action will be taken against it. This type of exclusion can only be used for certain types of detections. To add such detections to the exclusion list, navigate to **Quarantine**, right-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 its extension.

Exclusion paths

For ESET File Security for Linux v7.2

*/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.

For ESET File Security for Linux v7.1

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

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

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

For ESET File Security for Linux v7.0

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

/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.

Exclusions in ESET File Security for Linux version 7.0

File and folder exclusion

This type of exclusions can help you to exclude desired files from being scanned for presence of malicious software.

1. In the Web interface, click **Setup > Detection Engine > Basic**.
2. Next to **Exclusions**, click **Edit**.
3. Click **Add** and select the exclusion type:
   - **Exclude path** - Define the path to be excluded from the scan.
   - **Exclude hash** - Define the hash of the file to be excluded.
   - **Exclude detection** - Define the exact name of the threat (detection) to be ignored during scan, and optionally define a path mask.

- If left empty, every threat with the selected threat name is excluded.
- If a path to a directory is defined, every threat with the selected threat name in the defined directory and its sub-directories is excluded.
- If a path to a file is defined, only the specific file with the selected threat name is excluded.

4. Define a single entity (for example, path, hash, or threat).
5. Click **OK**, then click **Save** to close the dialog.
6. Click **Save** to save the changes.

Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another real-time scanner), real-time protection can be disabled by disengaging **Enable Real-time file system protection** automatically in **Setup** > **Detection engine** > **Real-time file system protection** > **Basic**.

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.

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 upon 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.

*The feature is available from ESET File Security for Linux version 7.1.

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 ThreatSense parameters section), 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 they have been 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, navigate to **Setup** > **Detection engine** > **Real-time file system protection**, click **ThreatSense parameters** > **Other** and select or deselect **Enable Smart optimization**.

Cloud-based protection

ESET LiveGrid® is an advanced early warning system comprised of several cloud-based technologies. It helps detect emerging threats based on reputation and improves scanning performance by means of whitelisting. New threat information is streamed in real-time to the cloud, which enables the ESET Malware Research Lab to provide timely response and consistent protection at all times. Users can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid®.

When installing ESET File Security for Linux, select one of the following options:

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

ESET LiveGrid® will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date

and time, the process by which the threat appeared on your computer and information about your computer's operating system.

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

Enable ESET LiveGrid® reputation system (recommended)

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

Enable ESET LiveGrid® feedback system

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

Submit crash reports and diagnostic data

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

Submit 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, file name, 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

Submit infected samples

This will submit all infected samples to ESET for analysis and to improve future detection.

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

Submit suspicious samples

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

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

with active content.

Exclusions

Click Edit option next to Exclusions in ESET LiveGrid® allows you 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.

Malware scans

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

Selected profile

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

List of profiles

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

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. Cilck **OK**, then click **Save**.

4. Optionally, review and adjust ThreatSense parameters.

5. Click **Save**.

See how to integrate ICAP server with EMC Isilon.

Cleaning levels

No cleaning – Infected files will not be cleaned automatically. The number of found threats will be highlighted red in the **Detections occurred** column, and the **Cleaned** column will also be highlighted red, but displaying 0.

Normal cleaning – The program will attempt 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 such an archive file will count towards **Detections occurred**, and the **Cleaned** column will be highlighted red.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files.

Rigorous cleaning – The program will clean or delete all infected files without any exception.

Delete – The program will delete all infected files without any exception.

Shared local cache

ESET Shared local cache will boost performance in virtualized environments by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache. Turn on the Caching option switch to save information about scans of files and folders on your network to the local cache. If you perform a new scan, ESET File Security will search for scanned files in the cache. If files match, they will be excluded from scanning.

Cache server setup contains the following:

- Hostname - Name or IP address of the computer where the cache is located.
- Port - Number of the port used for communication (same as was set in Shared local cache).
- Password - Specify the Shared local cache password if required.

ThreatSense parameters

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection 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 concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

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

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

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, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, 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.

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).

Potentially unwanted applications – see Potentially unwanted applications in our glossary.

Potentially unsafe applications – see Potentially unsafe applications in our glossary.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets 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:

Scan alternate data streams (ADS) – Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

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.

Log all objects – If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will list also clean files contained within the archive.

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 particular 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

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 entered 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

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.

Note
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. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before module update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (*.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**.

Update

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

Pre-release updates include most recent bug fixes and/or detection methods that will be 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 File Security for Linux update was not stable, roll back the module updates to a previous state. Click **Dashboard** > **Modules update** > **Module rollback**, select the desired duration, click **Rollback now**.

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

Tools

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

You can also schedule on-demand scan.

Proxy Server

Configure ESET File 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 File 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 update the Web interface password, click **Change password**. Type in a new password, click **Save**.

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 switch 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 File Security for Linux remotely via ESET Security Management Center, the Web interface is not enabled.

If you want to access the Web interface on the particular 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 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 Security Management Center, 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

Options - short form	Options - long form	Description
`-d`	`--disable`	Disable Web interface
`-e`	`--enable`	Enable Web interface

Log files

Modify the configuration of ESET File Security for Linux logging.

Minimum logging verbosity

Logging verbosity defines the level of details the log files include regarding ESET File 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** screen or log list (`lslog`), turn on the **Automatically delete records older than (days)** toggle. Adjust the day to specify age of files to be hidden. 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. Click **Optimize** to begin defragmenting the log files. All empty log entries are removed to improve performance and log processing speed. This improvement can be observed especially if the logs contain a large number of entries.

Syslog Facility

Syslog facility is a syslog logging parameter 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 File Security for Linux v7.1+ 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 on which the custom scan will be automatically triggered. Click **Next**.
5. Select scan profile.
6. Select **Scan targets**, and/or defined 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 particular task and click **Edit**. Continue with the remainder of steps.

To remove a scheduled task, in step 3 above, select the particular 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.

Schedule on-demand scan with ESET File Security for Linux v7.0.

Listen address and port

ESET File Security for Linux allows you to configure a custom IP address and port for both, the Web interface and ICAP server.

Remote Management

To manage ESET File Security for Linux remotely, connect the computer hosting your ESET security product to ESET Security Management Center (ESMC).

1. Deploy the ESET Management Agent.

2. Add the computer to ESMC.

From this time on you can execute applicable client tasks regarding ESET File Security for Linux.

Use case examples

In this chapter we will cover most common use cases of ESET File Security for Linux.

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 File Security for Linux through the Internet Content Adaptation Protocol (ICAP).

Prerequisite

1. ESET File Security for Linux is installed and its Web interface is enabled.

2. Isilon OneFS is installed.

Enable ICAP server in EFS

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 enter 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 ESET File Security for Linux. ESET File Security for Linux 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. Test scan:

   a.Get eicar antivirus test file from 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

If for any reason you need to retrieve information about a particular module of ESET File Security for Linux v7.0, execute the following command from a Terminal window:

```
grep -asi -A3 "version" /var/opt/eset/efs/lib/module_name
```

Example

```
grep -asi -A3 "version" /var/opt/eset/efs/lib/em000_64.dat
```

Output:

```
version: 1073 (20190506)
build: 1122
date (dd.mm.yyyy): 06.05.2019
type: loader module
```

For ESET File Security for Linux v7.1+ 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 File Security for Linux v7.1+ has a built-in scheduler to execute periodic custom scans on defined days and times. For ESET File Security for Linux v7.0 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 particular folder every night 11pm

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 * * 0 /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 File Security for Linux, in case ESET Technical Support asked you to access files for troubleshooting purposes. The list of deamons and command-line utilities is available further below.

Base directory

The directory where ESET File 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 File 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 File 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 File Security for Linux
- odscan — use it to run on-demand scan via a Terminal window

System binary files directory

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

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

There you find the following utilities:

- setgui — use it to enable/disable ESET File Security for Linux Web interface and manage related operations.
- startd — use it to start ESET File Security for Linux daemon manually in case it was stopped.

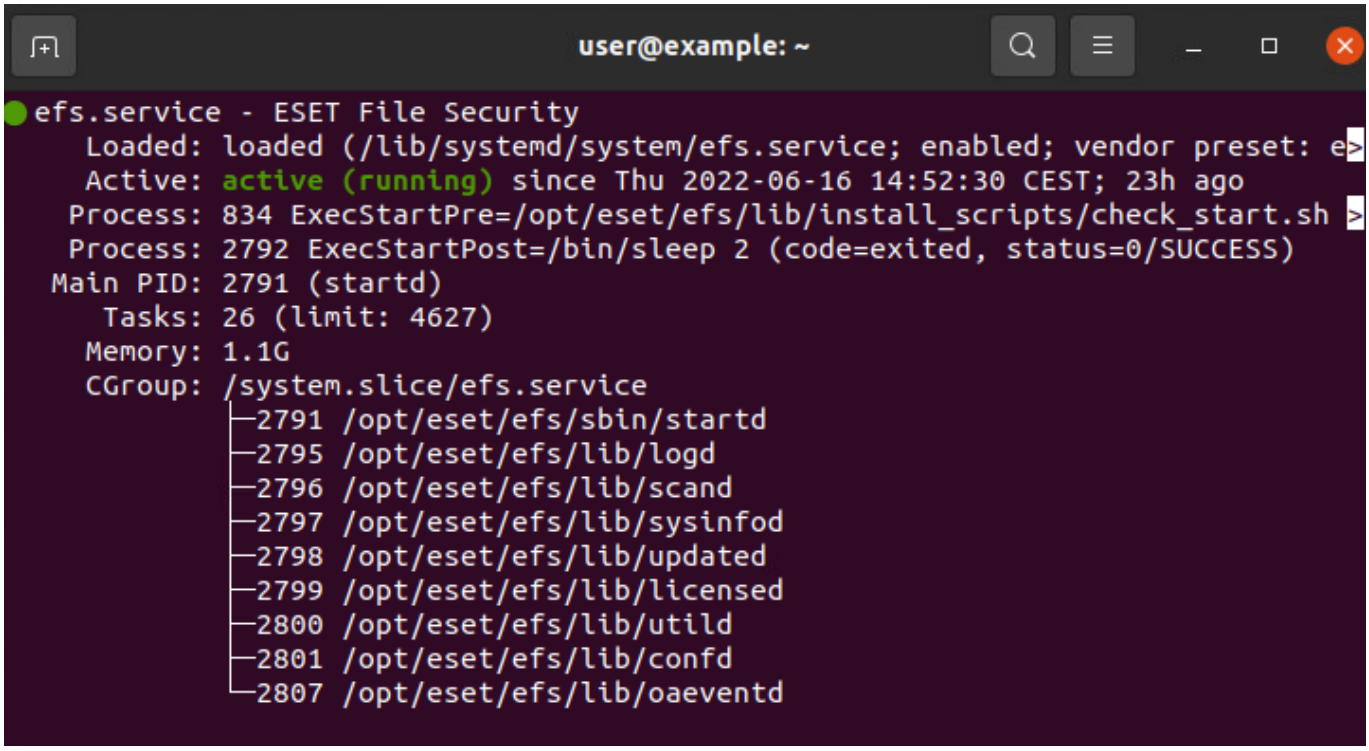
To see if ESET File Security for Linux service is active, run the following command from a Terminal window with root privileges:

```
systemctl status efs.service
```

or

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

Sample output from `systemctl`:



Daemons

- sbin/startd – Main daemon, starts and manages other deamons
- 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 – Quarantine restore helper
- 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/quar – 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)
- Forgotten password
- Update failed
- Using the noexec flag
- Real-time protection deamon unable to start
- Collect logs

Collect logs

If ESET Technical Support requests logs from ESET File 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 e-mail.

Activation logs

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

1. To enable activation logs, open `/var/opt/eset/efs/licensed/license_cfg.json` for editing. The example below uses `nano` editor. Execute the following command from a Terminal window as a privileged user:

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

2. Change `"Logging":false` to `"Logging":true`.

3. Save your changes by pressing CTRL+X, type Y, and press **Enter**.

4. Restart the `efs` service. Execute the following command from a Terminal window as a privileged user:

```
sudo systemctl restart efs
```

5. 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
```

6. Change `"Logging":true` to `"Logging":false`.

7. Save your changes by pressing CTRL+X, type Y, and press **Enter**.

8. Restart the `efs` service. Execute the following command from a Terminal window as a privileged user:

```
sudo systemctl restart efs
```

Forgot my password

To reset the Web interface password, open a Terminal window on the machine where ESET File 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 File 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, the installation of ESET File 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/
```

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

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

3. Compile the essential modules:

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

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

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

5. Reload systemd service configuration:

```
# systemctl daemon-reload
```

6. Restart the efs service:

```
# systemctl restart efs
```

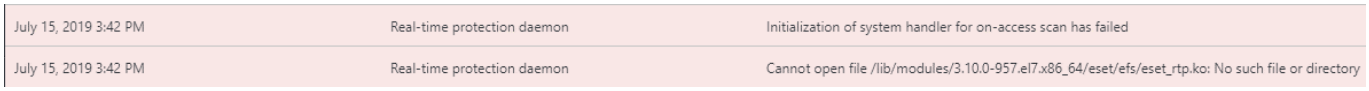
Realtime protection cannot start

Issue

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

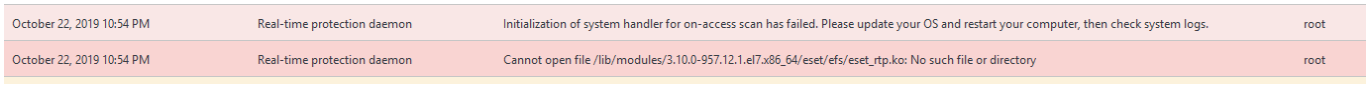
The **Events** screen in the Web interface of ESET File Security for Linux displays an error message similar to the one in one of the screenshots below:

In ESET File Security for Linux version 7.0:



July 15, 2019 3:42 PM	Real-time protection daemon	Initialization of system handler for on-access scan has failed
July 15, 2019 3:42 PM	Real-time protection daemon	Cannot open file /lib/modules/3.10.0-957.el7.x86_64/eset/efs/eset_rtp.ko: No such file or directory

In ESET File Security for Linux version 7.1:



October 22, 2019 10:54 PM	Real-time protection daemon	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.	root
October 22, 2019 10:54 PM	Real-time protection daemon	Cannot open file /lib/modules/3.10.0-957.12.1.el7.x86_64/eset/efs/eset_rtp.ko: No such file or directory	root

In system logs a corresponding error message is displayed:

Jul 15 15:42:30 localhost efs: ESET File Security error: cannot find kernel sources directory for kernel version 3.10.0-957.el7.x86_64

Jul 15 15:42:30 localhost efs: ESET File Security error: please check if kernel-devel (or linux-headers) package version matches the current kernel version

Jul 15 15:42:30 localhost oaeventd[31471]: ESET File Security Error: Cannot open file /lib/modules/3.10.0-957.el7.x86_64/eset/efs/eset_rtp.ko: No such file or directory

Solution

Method 1 - requires restart of the operating system

1. Upgrade the packages of your operating system to the latest version. On 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-dev modules (on RPM-based Linux distributions) or the latest kernel-headers (on DEB based Linux distributions). On Oracle Linux, execute the following command from a Terminal window as a privileged user:

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

2. Restart the EFS service.

```
systemctl restart efs
```

Disable Realtime protection at boot

If a machine protected by ESET File 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.

Known issues

ESET File Security for Linux v7.1

- Quarantine screen is only available in English
- Unable to “Enable more frequent updates of detection signatures”
- “Log all objects” setting does not work

ESET File Security for Linux v7.0

- SELinux denies port change of ICAP and Web interface
- ESET File Security for Linux is not available within **Install package on Repository** in the ESET Security Management Center (ESMC) software install task. However, it is possible to install ESET File Security for Linux using the **Install by direct package URL** option and using the following package URL: https://download.eset.com/com/eset/apps/business/efs/linux/v7/latest/efs.x86_64.bin

This issue will be solved by the release of ESMC 7.1

- Quarantine screen is only available in English

- Activation with Subscription license will activate ESET File Security for Linux, however ESET File Security for Linux is reporting a "License expired" message in both the Web interface and ESMC, and the expiration date is "-". Modules are updated properly.

- Unable to “Enable more frequent updates of detection signatures”

- “Log all objects” setting does not work

- Cannot change ESET File Security for Linux Web interface password through ESET Security Management Center

Glossary

- **Daemon**: A type of program on Unix-like operating systems that runs unobtrusively in the background, rather than under the direct control of a user, waiting to be activated by the occurrence of a specific event or condition.

End User License Agreement

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 (hereinafter referred to as "the Agreement") executed by and between 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 (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the 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. If You do not agree to all of the terms and conditions of this Agreement, 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 (hereinafter referred to as " 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, smart phones, 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 (hereinafter referred to as "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 system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as "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 in which has the right to use the Software in accordance 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) **Business Edition.** A Business Edition version of the Software must be obtained 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.** OEM Software 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 be also entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

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

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates 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 automatic installation of Updates. For the purpose of 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.

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 (hereinafter referred to as "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, information about the operations and functionality of the Software and information about devices in local network such as type, vendor, model and/or name of device (hereinafter referred to as "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. You hereby agree to receive notification and messages including but not limited to marketing information.

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 back-up 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 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 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 back-up copies and all related materials provided by the Provider or its business partners. 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 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. 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 act, 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 (hereinafter referred to as "Affiliates") being in violation of, or being subject to negative consequences under, Trade Control Laws which includes

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 (hereinafter referred to as "Export Control Laws") 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 (hereinafter referred to as "Sanction 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 return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

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. In case of a discrepancy between language versions of this Agreement, the English version shall prevail. This Agreement may only be modified in written form, signed by an authorized representative of the Provider, or a person expressly authorized to act in this capacity under the terms of a power of attorney.

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.

EULA ID: BUS-STANDARD-20-01

Privacy Policy

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

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

Processing of Personal Data

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

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

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

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

Data Confidentiality

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

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

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

Data Subject's Rights

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

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

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

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