ESET Endpoint Security for macOS

User guide

Click here to display the online version of this document

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

REV. 6/23/2020

1 ESET Endpoint Security for macOS 1
1.1 What's new in version 6 1
1.2 System requirements 2
2 Users connecting via ESET Security Management Center 2
3 Installation 3
3.1 Typical installation 4
3.2 Custom installation 6
3.3 Remote installation 9
4 Product activation 10
5 Uninstallation 11
6 Basic overview 12
6.1 Keyboard shortcuts 12
6.2 Checking operation of the system 13
6.3 What to do if the program does not work properly 13
7 Computer protection 14
7.1 Antivirus and antispyware protection 14
7.1 General 14
7.1 Exclusions 15
7.1 Startup protection 15
7.1 Real-time file system protection 16
7.1 Advanced options 16
7.1 When to modify Real-time protection configuration 17
7.1 Checking Real-time protection 17
7.1 What to do if Real-time protection does not work 18
7.1 On-demand computer scan 19
7.1 Type of scan 20
7.1 Smart scan 20
7.1 Custom scan 20
7.1 Scan targets 20
7.1 Scan profiles 21
7.1 ThreatSense engine parameters setup 22
7.1 Objects 23
7.1 Options 23
7.1 Cleaning 24
7.1 Exclusions 24
7.1 Limits 25
7.1 Others 25
7.1 An infiltration is detected 26
7.2 Web and email protection 27
7.2 Web access protection 27
7.2 Ports 27
7.2 URL lists 28
7.2 Email protection 28
7.2 POP3 protocol checking 29
7.2 IMAP protocol checking 30
7.3 Anti-Phishing 30

8 Firewall 31
8.1 Filtering modes 31
8.2 Firewall rules 32
8.2 Creating new rules 33
8.3 Firewall zones 33
8.4 Firewall profiles 34
8.5 Firewall logs 34
9 Device control 35
9.1 Rules editor 35
10 Web control 38
11 Tools 39
11.1 Log files 39
11.1 Log maintenance 40
11.1 Log filtering 41
11.2 Scheduler 42
11.2 Creating new tasks 43
11.2 Creating a user-defined task 45
11.3 Live Grid 46
11.3 Suspicious files 47
11.4 Quarantine 48
11.4 Quarantining files 49
11.4 Restoring a quarantined file 49
11.4 Submitting a file from Quarantine 49
11.5 Privileges 49
11.6 Presentation mode 50
11.7 Running processes 51
12 User interface 52
12.1 Alerts and notifications 52
12.1 Display alerts 53
12.1 Protection statuses 53
12.2 Context menu 54
13 Update 54
13.1 Update setup 54
13.1 Advanced options 56
13.2 How to create update tasks 57
13.3 System updates 57
13.4 Import and export settings 59
13.5 Proxy server setup 59
13.6 Shared Local Cache 60
14 End User License Agreement 60
15 Privacy Policy 68

ESET Endpoint Security for macOS

ESET Endpoint Security for macOS 6 represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine, combined with our custom firewall, utilizes speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert for attacks and malicious software that might threaten your computer.

ESET Endpoint Security for macOS 6 is a complete security solution developed from our long-term effort to combine maximum protection and a minimal system footprint. The advanced technologies, based on artificial intelligence, are capable of proactively eliminating infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other Internet-borne attacks without hindering system performance or disrupting your computer.

The product is primarily designed for use on workstations in a small business/enterprise environment. It can be used with ESET Security Management Center7, allowing you to easily manage any number of client workstations, apply policies and rules, monitor detections and remotely administer changes from any networked computer.

What's new in version 6

The graphical user interface of ESET Endpoint Security for macOS has been completely redesigned to provide better visibility and a more intuitive user experience. Some of the many improvements included in version 6 include:

- **ESET Enterprise Inspector support** - from ESET Endpoint Security for macOS version 6.9, ESET Endpoint Security for macOS can be connected with ESET Enterprise Inspector. ESET Enterprise Inspector (EEI) is a comprehensive Endpoint Detection and Response system that includes features such as: incident detection, incident management and response, data collection, indicators of compromise detection, anomaly detection, behavior detection, and policy violations. For more information about ESET Enterprise Inspector, its installation and functions, see ESET Enterprise Inspector help.
- **64-bit architecture support**
- **Firewall -** you can now create firewall rules directly from the log or the IDS (Intrusion detection system) notification window and assign profiles to network interfaces.
- **Web control** – blocks webpages that may contain inappropriate or offensive material
- **Web access protection** – monitors communication between web browsers and remote servers

• **Email protection** – provides control of email communication received via the POP3 and IMAP protocols

• **Anti-Phishing protection** – protects you from attempts to acquire passwords and other sensitive information by restricting access to malicious websites that impersonate legitimate ones

• **Device Control** – allows you to scan, block or adjust extended filters and/or permissions and define a user's ability to access and work with external devices. This feature is available in the product version 6.1 and later.

• **Presentation mode** – this option lets you run ESET Endpoint Security for macOS in the background and suppresses pop-up windows and scheduled tasks

• **Shared local cache** – allows for scanning speed improvements in virtualized environments

System requirements

For optimal performance of ESET Endpoint Security for macOS, your system should meet the following hardware and software requirements:

	System requirements:
Processor architecture	Intel 64-bit
Operating system	macOS 10.12 and later
Memory	300 MB
Free disk space	200 MB

Users connecting via ESET Security Management Center

ESET Security Management Center 7 is an application that allows you to manage ESET products in a networked environment from one central location. The ESET Security Management Center task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET Security Management Center does not provide protection against malicious code on its own, it relies on the presence of an ESET security solution on each client.

ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, macOS and operating systems that run on mobile devices (mobile phones and tablets).

ESET Security Management Center is a new generation of remote management system that differs significantly from previous versions of ESET Security Management Center. Since the architecture is completely different, ESET Security Management Center 7 is only partially compatible with ERA 6 and there is no backward compatibility with ERA 5. However, compatibility with previous versions of ESET security products remains.

Together with new ESET Security Management Center, ESET has developed a new generation of security products with a new licensing system.

To perform a complete deployment of the ESET security solutions portfolio, the following components must be installed (Windows and Linux platforms):

- ESET Security Management Center Server
- ESET Security Management Center Web Console
- ESET Management Agent

The following supporting components are optional, we recommend that you install them for best performance of the application on the network:

- Proxy
- RD Sensor
- Apache HTTP Proxy
- Mobile Device Connector

ESET Security Management Center Documentation
For more information see the ESET Security Management Center online documentation.

Installation

There are two ways to launch the ESET Endpoint Security for macOS installer:

- If you are installing from the installation CD/DVD, insert the disk into the CD/DVD-ROM drive and double-click the ESET Endpoint Security for macOS installation icon to launch the installer.
- If you are installing from a downloaded file, double-click the file you downloaded to launch the installer.

The installation wizard will guide you through basic setup. During the initial phase of installation, the installer will automatically check online for the latest product version. If a newer version is found, you will be given the option to download the latest version before continuing the installation process.

Installing from the .pkg file
During installation and the first startup of your ESET products for macOS installed from the .pkg file, it is necessary to have internet access on your mac to allow Apple to verify ESET kernel extensions notarization.

After agreeing to the End User License Agreement, you can choose from the following installation types:

- Typical installation
- Custom installation
- Remote installation

Typical installation

Typical installation mode includes configuration options that are appropriate for most users. These settings provide maximum security combined with excellent system performance. Typical installation is the default option and is recommended for those who do not have particular requirements for specific settings.

ESET Live Grid

The ESET Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The Live Grid system submits new threats to the ESET Threat Lab where they are analyzed and processed. Click **Setup** to modify the settings for the submission of suspicious files. For more information see Live Grid. If ESET Live Grid is not enabled, ESET Endpoint Security for macOS displays a security alert.

Potentially Unwanted Applications

The last step of the installation process is to configure detection of **Potentially unwanted applications**. These applications are not necessarily malicious, but can often negatively affect the behavior of your operating system. Potentially unwanted applications are often bundled with other programs you choose to download; it may be difficult to notice when they are being installed. Although these applications usually display a notification during installation, they can easily be installed without your consent.

After your first installation of ESET Endpoint Security for macOS:

1. On macOS 10.13 and later you will receive the **System Extension Blocked** notification from your system and the **Your computer is not protected** notification from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow kernel extensions on your device. To allow kernel extensions on your device, navigate to **System Preferences** > **Security & Privacy** and click **Allow** to allow system software from the developer **ESET, spol. s.r.o.** For more detailed information, visit our Knowledgebase article.
2. On macOS 10.14 you will receive **Your computer is partially protected** notification from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow **Full disc access** to ESET Endpoint Security for macOS. Click **Open System preferences** > **Security & Privacy**. Go to the **Privacy** tab and select the **Full disk access** option. Click the lock icon to enable editing. Click the plus icon and select the ESET Endpoint Security for macOS application. Your computer will display a notification to restart your computer. Click **Later**. Do not restart your computer now. Click **Start Again** in the ESET Endpoint Security for macOS notification window or restart your computer. For more detailed information, visit our Knowledgebase article.

After installing ESET Endpoint Security for macOS, you should perform a computer scan to check for malicious code. From the main program window, click **Computer scan** > **Smart scan**. For more information about On-demand computer scans, see the On-demand computer scan section.

Custom installation

Custom installation mode is designed for experienced users who want to modify advanced settings during the installation process.

Program Components

ESET Endpoint Security for macOS allows you to install the product without some of its core components (for example, Web and Email protection). Deselect the check box next to a product component to remove it from the installation.

Proxy Server

If you are using a proxy server, you can define its parameters by selecting **I use a proxy server**. In the next window, enter the IP address or URL of your proxy server in the **Address** field. In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). If the proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. If you do not use a proxy server, select **I do not use a proxy server**. If you are not sure whether you use a proxy server or not, you can use your current system settings by selecting **Use system settings (Recommended)**.

Privileges

In the next step you can define privileged users or groups that will be able to edit the program settings. From the list of users on the left, select the users and **Add** them to the **Privileged Users** list. To display all system users, select **Show all users**. If you leave the Privileged Users list empty, all users are considered privileged.

ESET Live Grid

The ESET Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed and processed. Click **Setup** to modify the settings for the submission of suspicious files. For more information see Live Grid. If ESET Live Grid is not enabled, ESET Endpoint Security for macOS displays a security alert.

Potentially Unwanted Applications

The next step of the installation process is to configure detection of **Potentially unwanted applications**. These programs are not necessarily malicious, but can often negatively affect the behavior of your operating system. These applications are often bundled with other programs you download; it may be difficult to notice when they are being installed. Although these applications usually display a notification during installation, they can easily be installed without your consent.

Firewall

Select a filtering mode for Firewall. For more information, see Filtering modes.

After your first installation of ESET Endpoint Security for macOS:

1. On macOS 10.13 and later you will receive the **System Extension Blocked** notification from your system and the **Your computer is not protected** notification from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow kernel extensions on your device. To allow kernel extensions on your device, navigate to **System Preferences** > **Security & Privacy** and click **Allow** to allow system software from the developer **ESET, spol. s.r.o.** For more detailed information, visit our Knowledgebase article.
2. On macOS 10.14 you will receive **Your computer is partially protected** notification from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow **Full disc access** to ESET Endpoint Security for macOS. Click **Open System preferences** > **Security & Privacy**. Go to the **Privacy** tab and select the **Full disk access** option. Click the lock icon to enable editing. Click the plus icon and select the ESET Endpoint Security for macOS application. Your computer will display a notification to restart your computer. Click **Later**. Do not restart your computer now. Click **Start Again** in the ESET Endpoint Security for macOS notification window or restart your computer. For more detailed information, visit our Knowledgebase article.

After installing ESET Endpoint Security for macOS, you should perform a computer scan to check for malicious code. From the main program window, click **Computer scan** > **Smart scan**. For more information about On-demand computer scans, see the On-demand computer scan section.

Remote installation

Before installation

Before installing ESET Endpoint Security for macOS on macOS 10.13 and later, we recommend that you allow ESET kernel extensions and on macOS 10.14 and later, also allow Full disc access on targeted computers. If these options are allowed after the installation, users will receive notifications **System extensions blocked,** and **Your computer is partially protected** until ESET kernel extensions and full disk access are allowed.

To allow ESET kernel extensions and full disk access remotely, your computer needs to be enrolled in the MDM (Mobile Device Management) server, such as Jamf.

Allow ESET kernel extensions

- Kernel extensions need to be allowed only with the first installation of ESET Endpoint Security for macOS. To allow kernel extensions on your device remotely:
  - If you are using Jamf as your MDM, follow our knowledgebase article.
  - If you are using different MDM, download the .plist configuration profile. Generate two UUIDs with a UUID generator of your choice and use a text editor to replace strings with the text **insert your UUID 1 here** and **insert your UUID 2 here** in the downloaded configuration profile. Deploy the .plist configuration profile file using the MDM server. Your computer needs to be enrolled in the MDM server to be able to deploy configuration profiles to those computers.

Allow full disk access

- On macOS 10.14, you will receive the notification **Your computer is partially protected** from ESET Endpoint Security for macOS after installation. To access all ESET Endpoint Security for macOS functions and prevent the notification from appearing, you need to allow **Full disk access** to ESET Endpoint Security for macOS before installation of the product. To allow **Full disk access** remotely:
  - If you are using Jamf as your MDM, follow our knowledgebase article.
  - To allow **Full disk access** remotely, download the .plist configuration file. Generate two UUIDs with a UUID generator of your choice and use a text editor to replace strings with the text **insert your UUID 1 here** and **insert your UUID 2 here** in the downloaded configuration profile. Deploy the .plist configuration profile file using the MDM server. Your computer needs to be enrolled in the MDM server to be able to deploy configuration profiles to those computers.

Installation

You can install ESET Endpoint Security for macOS remotely using ESET Security Management Center from the web console by creating a Software install task.

For detailed instructions, visit:

- Software install task ERA online help topic
- Deploy or upgrade ESET endpoint products using ERA Knowledgebase article
- Software install task ESET Security Management Center online help topic

After installation

If you did not allow ESET kernel extensions and full disc access:

Allow ESET kernel extensions

After your first installation of ESET Endpoint Security for macOS:

1. On macOS 10.13 and later, you will receive the **System Extension Blocked** notification from your system, and the **Your computer is not protected** notification from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow kernel extensions on your device.
    a. To allow kernel extensions on your device manually, navigate to **System Preferences** > **Security & Privacy** and click **Allow** to allow system software from the developer **ESET, spol. s.r.o.** For more detailed information, visit our Knowledgebase article.
    b. To allow kernel extensions on your device remotely:
        i. If you are using Jamf as your MDM, follow our knowledgebase article.
        ii. If you are using different MDM, download the .plist configuration profile. Generate two UUIDs with a UUID generator of your choice and use a text editor to replace strings with the text **insert your UUID 1 here** and **insert your UUID 2 here** in the downloaded configuration profile. Deploy the .plist configuration profile file using the MDM server. Your computer needs to be enrolled in the MDM server to be able to deploy configuration profiles to those computers.

Allow full disk access

- On macOS 10.14, you will receive the notification **Your computer is partially protected** from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow **Full disk access** to ESET Endpoint Security for macOS. To allow **Full disk access** remotely:
    - If you are using Jamf as your MDM, follow our knowledgebase article.
    - To allow **Full disk access** remotely, download the .plist configuration file. Generate two UUIDs with a UUID generator of your choice and use a text editor to replace strings with

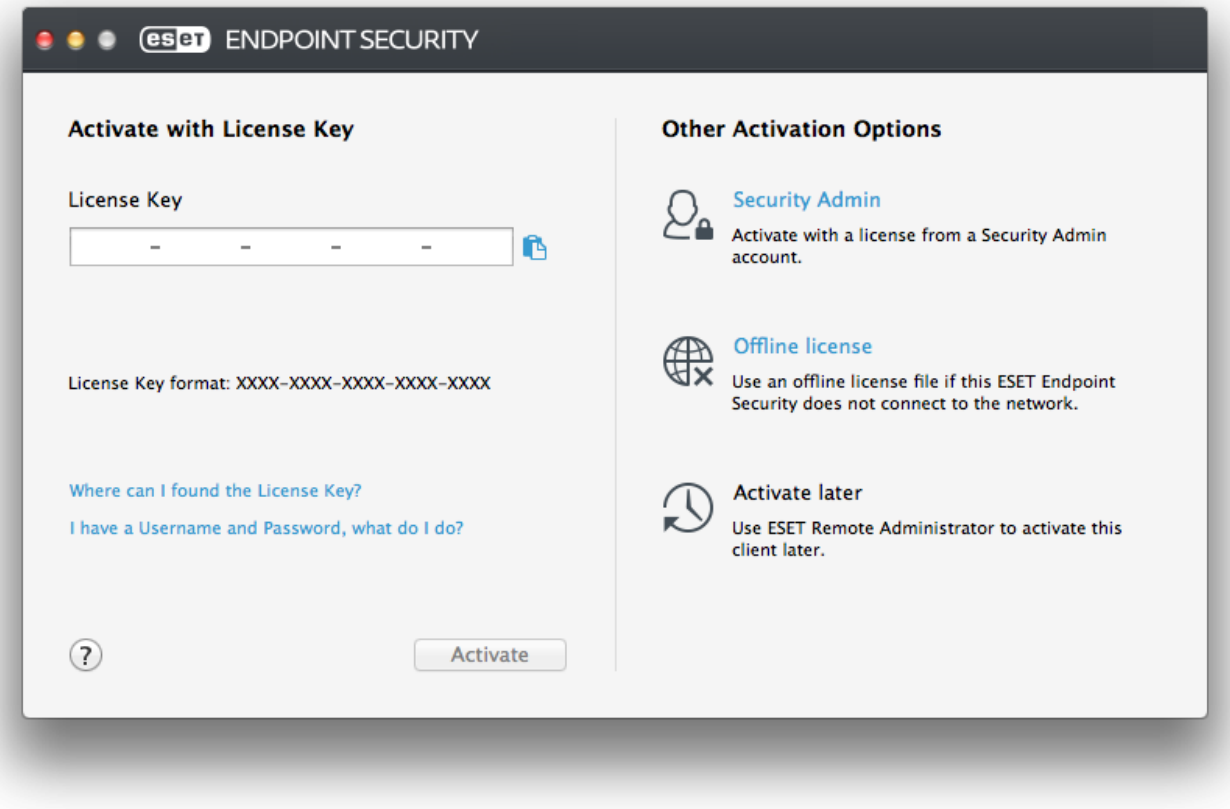
the text **insert your UUID 1 here** and **insert your UUID 2 here** in the downloaded configuration profile. Deploy the .plist configuration profile file using the MDM server. Your computer needs to be enrolled in the MDM server to be able to deploy configuration profiles to those computers.

You can also allow Full disk access manually. For detailed instructions, visit our Knowledgebase article.

Product activation

After installation is complete, you will be prompted to activate your product. There are multiple activation methods that can be used. The availability of a particular activation method may vary depending on the country, as well as the means of distribution (CD/DVD, ESET web page, etc.) for your product.

To activate your copy of ESET Endpoint Security for macOS directly from the program, click the ESET Endpoint Security for macOS icon located in the macOS Menu Bar (top of the screen) and click **Product activation**. You can also activate your product from the main menu under **Help** > **Manage license** or **Protection status** > **Activate product**.



You can use any of the following methods to activate ESET Endpoint Security for macOS:

• **Activate with License Key** – A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and activation of the license. You can find your License key in the email received after the purchase or on the license card included in the box.

• **Security Admin** – An account created on the ESET License Administrator portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.

• **Offline license** – An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the ESET License Administrator portal and is used in environments where the application cannot connect to the licensing authority.

You can also activate this client at a later time if your computer is a member of managed network and your administrator plans to use ESET Remote Administrator to activate your product.

Silent activation
ESET Remote Administrator is able to activate client computers silently using licenses made available by the administrator.

ESET Endpoint Security for macOS version 6.3.85.0 (or later) provides you with the option to activate the product using Terminal. To do so, issue the following command:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Replace `XXXX-XXXX-XXXX-XXXX-XXXX` with a License Key that has already been used for the activation of ESET Endpoint Security for macOS or registered in ESET License Administrator. The command will return either the "OK" state or an error if the activation fails.

Uninstallation

There are multiple ways to launch the ESET Endpoint Security for macOS uninstaller:

• insert the ESET Endpoint Security for macOS installation CD/DVD into your computer, open it from your desktop or **Finder** window and double-click **Uninstall**

• open the ESET Endpoint Security for macOS installation file (*.dmg*) and double-click **Uninstall**

• launch **Finder**, open the **Applications** folder on your hard drive, CTRL+click the **ESET Endpoint Security for macOS** icon and select **Show Package Contents**. Open the **Contents** > **Helpers** folder and double-click the **Uninstaller** icon.

Basic overview

The main program window of ESET Endpoint Security for macOS is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.

The following sections are accessible from the main menu:

• **Protection status** – provides information about the protection status of your Computer, Firewall, Web and Mail protection.

• **Computer scan** – this section allows you to configure and launch the On-demand computer scan.

• **Update** – displays information about modules updates.

• **Setup** – select this section to adjust your computer's security level.

• **Tools** – provides access to Log files, Scheduler, Quarantine, Running processes and other program features.

• **Help** – displays access to help files, Internet Knowledgebase, support request form and additional program information.

Keyboard shortcuts

Keyboard shortcuts that can be used when working with ESET Endpoint Security for macOS:

• *cmd+,* – displays ESET Endpoint Security for macOS preferences,
• *cmd+O* – resizes the ESET Endpoint Security for macOS main GUI window to the default size and moves it to the center of the screen,

• *cmd+Q* – hides the ESET Endpoint Security for macOS main GUI window. You can open it by clicking the ESET Endpoint Security for macOS icon in the macOS Menu Bar (top of the screen),

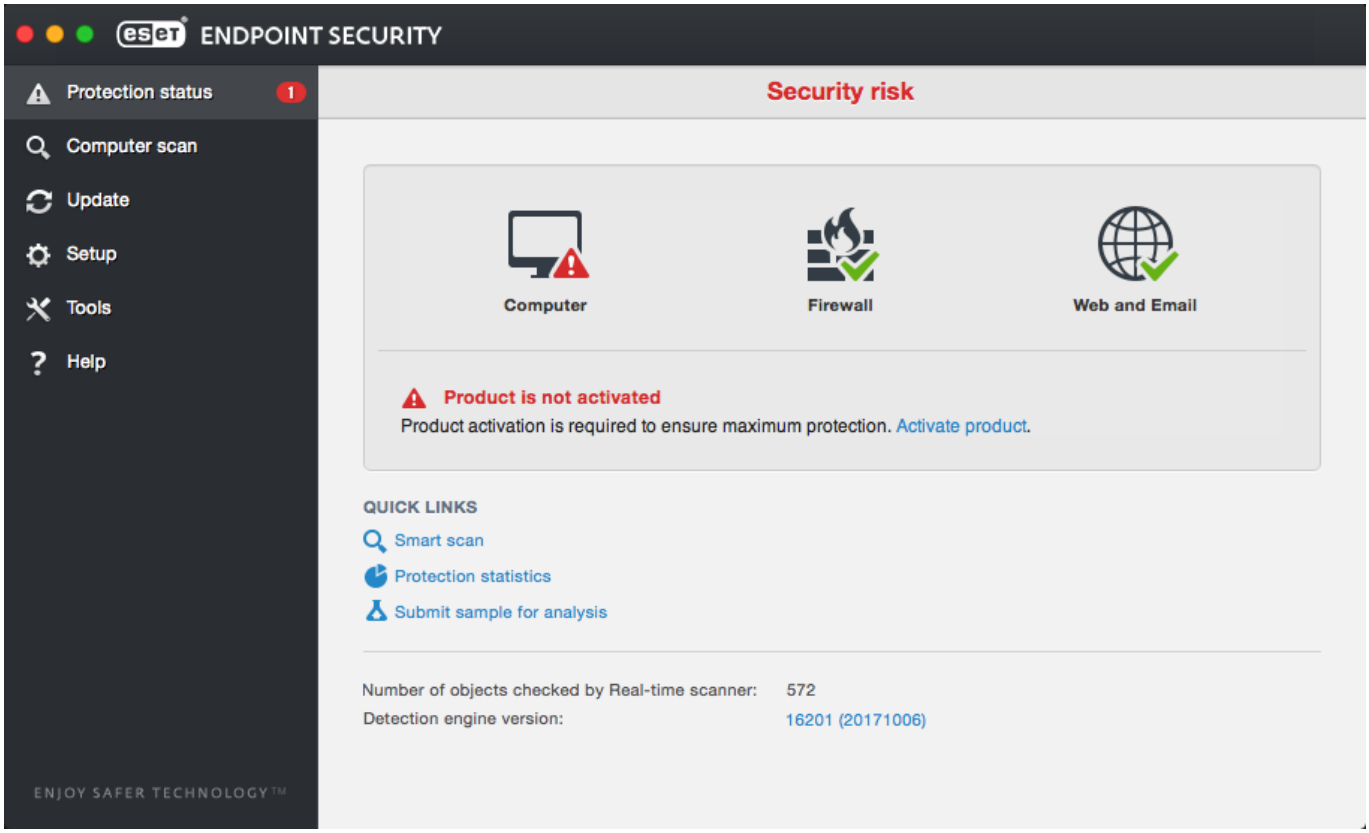
• *cmd+W* – closes the ESET Endpoint Security for macOS main GUI window.

The following keyboard shortcuts work only if **Use standard menu** is enabled under **Setup** > **Enter application preferences ...** > **Interface**:

- *cmd+alt+L* – opens the **Log files** section,
- *cmd+alt+S* – opens the **Scheduler** section,
- *cmd+alt+Q* – opens the **Quarantine** section.

Checking operation of the system

To view your protection status click **Protection status** from the main menu. A status summary about the operation of ESET Endpoint Security for macOS modules will be displayed in the primary window.



What to do if the program does not work properly

When a module is functioning properly, a green check mark icon is displayed. When a module is not functioning properly, a red exclamation point or an orange notification icon is displayed. Additional information about the module and a suggested solution for fixing the

issue is displayed in the main program window. To change the status of individual modules, click the blue link below each notification message.

If you are unable to solve a problem using the suggested solutions, you can search the ESET Knowledgebase for a solution or contact ESET Customer Care. Customer Care will respond quickly to your questions and help resolve any issues with ESET Endpoint Security for macOS.

Computer protection

Computer configuration can be found under **Setup** > **Computer**. It displays the status of **Real-time file system protection**. To turn off individual modules, switch the desired module to **DISABLED**. Note that this may decrease the level of protection of your computer. To access detailed settings for each module, click **Setup**.

Antivirus and antispyware protection

Antivirus protection guards against malicious system attacks by modifying files that pose potential threats. If a threat with malicious code is detected, the Antivirus module can eliminate it by blocking it and then cleaning it, deleting it or moving it to quarantine.

General

In the **General** section (**Setup** > **Enter application preferences...** > **General**), you can enable detection of the following types of applications:

• **Potentially unwanted applications** – These applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the way it behaved before these applications were installed). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.

• **Potentially unsafe applications** – These applications are commercial, legitimate software that can be abused by attackers if installed without user consent. This classification includes programs such as remote access tools, for this reason this option is disabled by default.

• **Suspicious applications** – These applications include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection. A Packer is a runtime self-extracting executable that includes several

kinds of malware in a single package. The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

To set up File System or Web and Mail exclusions, click **Setup**.

Exclusions

In the Exclusions section you can exclude certain files/folders, applications or IP/IPv6 addresses from scanning.

Files and folders listed in the **File System** tab will be excluded from all scanners: Startup, Real-time and On-Demand (Computer scan).

- **Path** – path to excluded files and folders
- **Threat** – if there is a name of a threat next to an excluded file, it means that the file is only excluded for that threat, but not completely. If that file becomes infected later with other malware, it will be detected by the antivirus module.
-  – creates a new exclusion. Enter the path to an object (you can also use the wild cards * and *?*) or select the folder or file from the tree structure.
-  – removes selected entries
- **Default** – Roll back exclusions to the last saved state.

In the **Web and Mail** tab, you can exclude certain **Applications** or **IP/IPv6 addresses** from protocol scanning.

Startup protection

Startup file check automatically scans files at system startup. By default, this scan runs regularly as a scheduled task after a user logon or after a successful modules update. To modify ThreatSense engine parameter settings applicable to the Startup scan, click **Setup**. You can learn more about ThreatSense engine setup by reading this section.

Real-time file system protection

Real-time file system protection checks all types of media and triggers a scan based on various events. Using ThreatSense technology (described in ThreatSense engine parameter setup), Real-time file system protection may vary for newly created files and existing files. Newly created files can be more precisely controlled.

By default, all files are scanned upon **file opening**, **file creation** or **file execution**. We recommend that you keep these default settings, as they provide the maximum level of Real-time protection for your computer. Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another Real-time scanner), Real-time protection can be terminated by clicking the ESET Endpoint Security for macOS icon located in your Menu Bar (top of the screen) and selecting **Disable Real-time File System Protection**. Real-time file system protection can also be disabled from the main program window (click **Setup** > **Computer** and switch **Real-time file system protection** to **DISABLED**).

The following types of media can be excluded from the Real-time scanner:

- **Local drives** – system hard drives
- **Removable media** – CDs, DVDs, USB media, Bluetooth devices, etc.
- **Network media** – all mapped drives

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

To modify advanced settings for Real-time file system protection, go to **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Real-Time Protection** and click **Setup...** next to **Advanced Options** (described in Advanced scan options).

Advanced options

In this window you can define which object types are scanned by the ThreatSense engine. To learn more about **Self-extracting archives**, **Runtime packers** and **Advanced heuristics**, see ThreatSense engine parameters setup.

We do not recommend making changes in the **Default archives settings** section unless required to resolve a specific issue, as higher archive nesting values can impede system performance.

ThreatSense parameters for executed files – by default, **Advanced heuristics** is used when files are executed. We strongly recommend keeping Smart optimization and ESET Live Grid enabled to mitigate impact on system performance.

Increase network volume compatibility – this option boosts performance when accessing files over the network. It should be enabled if you experience slowdowns while accessing network drives. This feature uses system file coordinator on OS X 10.10 and later. Be aware that not all applications support the file coordinator, for example Microsoft Word 2011 does not support it, Word 2016 does.

When to modify Real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Use caution when modifying the Real-time protection parameters. We recommend that you only modify these parameters in specific cases. For example, a situation in which there is a conflict with a certain application or Real-time scanner of another antivirus program.

After installing ESET Endpoint Security for macOS, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click the **Default** button located at the bottom-left of the **Real-Time Protection** window (**Setup** > **Enter application preferences ...** > **Real-Time Protection**).

Checking Real-time protection

To verify that Real-time protection is working and detecting viruses, use the eicar.com test file. This test file is a special, harmless file detectable by all antivirus programs. The file was created by the EICAR institute (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs.

To check the status of Real-time protection without using ESET Security Management Center, connect to the client computer remotely using **Terminal** and issue the following command:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

The status of the Real-time scanner will be displayed as either `RTPStatus=Enabled` or `RTPStatus=Disabled`.

The output of the Terminal bash includes the following statuses:

- the version of ESET Endpoint Security for macOS installed on the client computer
- date and version of the detection engine
- path to the update server

NOTE: Use of the Terminal utility is recommended for advanced users only.

What to do if real-time protection does not work

In this chapter we describe problem situations that may arise when using Real-time protection, and how to troubleshoot them.

Real-time protection is disabled

If Real-time protection is inadvertently disabled by a user, it will need to be reactivated. To reactivate Real-time protection, from the main menu click **Setup** > **Computer** and switch **Real-time file system protection** to **ENABLED**. Alternatively, you can enable Real-time file system protection in the application preferences window under **Real-Time Protection** by selecting **Enable real-time file system protection**.

Real-time protection does not detect and clean infiltrations

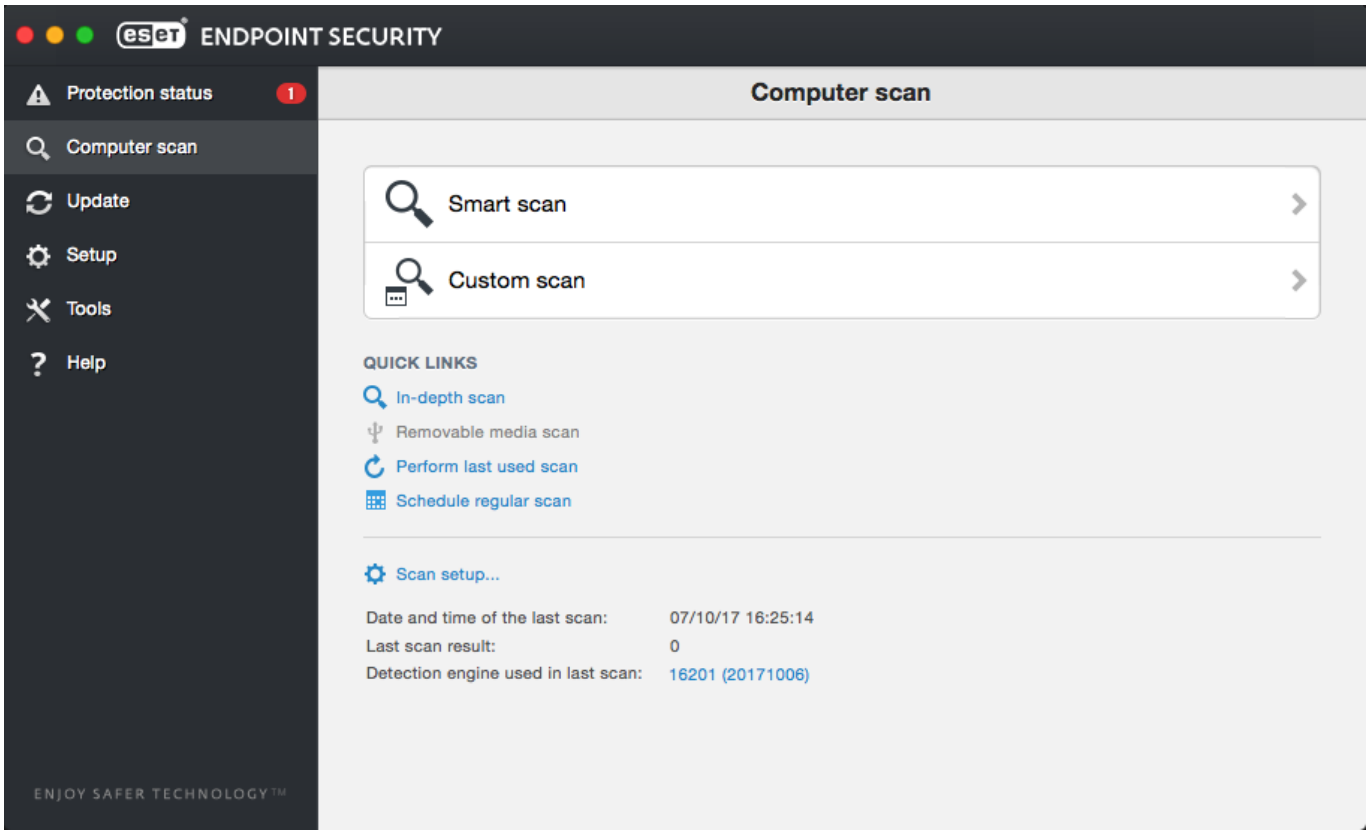
Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs that may be on your system.

Real-time protection does not start

If Real-time protection is not initiated at system startup, it may be due to conflicts with other programs. If you experience this issue, contact ESET Customer Care.

On-demand computer scan

If you suspect that your computer is infected (it behaves abnormally), run a **Smart scan** to examine your computer for infiltrations. For maximum protection, computer scans should be run regularly as part of routine security measures, not just when an infection is suspected. Regular scanning can detect infiltrations that were not detected by the Real-time scanner when they were saved to the disk. This can happen if the Real-time scanner was disabled at the time of infection, or if modules are not up-to-date.



We recommend that you run an On-demand computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**.

You can also drag and drop selected files and folders from your Desktop or **Finder** window to the ESET Endpoint Security for macOS main screen, Dock icon, Menu Bar icon (top of the screen) or the application icon (located in the */Applications* folder).

Type of scan

Two types of On-demand computer scans are available. **Smart scan** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan** allows you to select any of the predefined scan profiles, as well as choose specific scan targets.

Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantage is easy operation with no detailed scanning configuration. Smart scan checks all files in all folders and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see Cleaning.

Custom scan

Custom scan allows you to specify scanning parameters such as scan targets and scanning methods. The advantage of running a Custom scan is the ability to configure scan parameters in detail. Different configurations can be saved as user-defined scan profiles, which can be useful if scanning is repeatedly performed using the same parameters.

To select scan targets, select **Computer scan** > **Custom scan** and then select specific **Scan Targets** from the tree structure. A scan target can also be more precisely specified by entering the path to the folder or file(s) you want to include. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. Furthermore, you can choose from three cleaning levels by clicking **Setup...** > **Cleaning**.

Custom scan
Performing computer scans with Custom scan is only recommended for advanced users with previous experience using antivirus programs.

Scan targets

The Scan targets tree structure allows you to select files and folders to be scanned for viruses. Folders may also be selected according to a profile's settings.

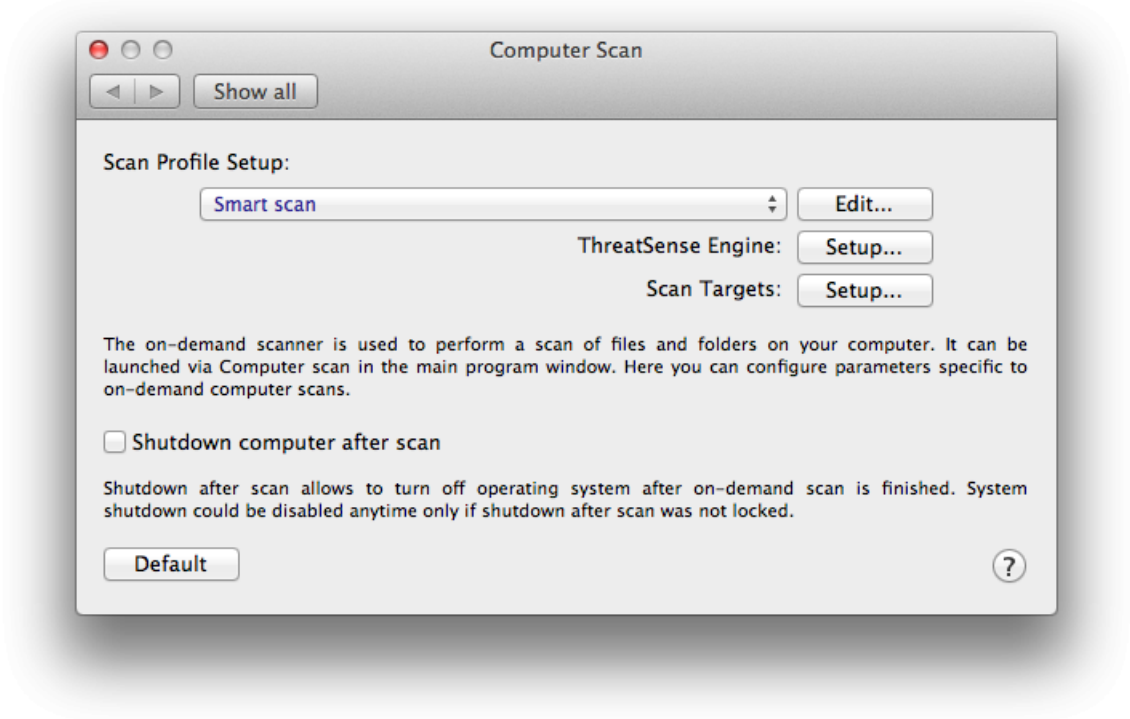
A scan target can be more precisely defined by entering the path to the folder or file(s) you

want to include in scanning. Select targets from the tree structure that lists all available folders on the computer by selecting the check box that corresponds to a given file or folder.

Scan profiles

Your preferred scan settings 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, from the main menu click **Setup** > **Enter application preferences ...** (or press *cmd*+,) > **Computer Scan** and click **Edit** next to the list of current profiles.



To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

Example: Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you do not want to scan runtime packers or potentially unsafe applications and you also want to apply Strict cleaning. In the **On-demand Scanner Profiles List** window, type the profile name, click **Add** and then confirm by clicking **OK**. Adjust the parameters to meet your requirements using the **ThreatSense Engine** and **Scan Targets** settings.

If you want to turn off the operating system and shut down the computer after the On-demand scan is finished, use the **Shutdown computer after scan** option.

ThreatSense engine parameters setup

ThreatSense is a proprietary ESET technology comprised of several complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, etc.) that 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 prevents rootkits.

The ThreatSense technology 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 > Enter application preferences ...** (or press *cmd+,*) and then click the ThreatSense Engine **Setup** button located in the **Startup Protection**, **Real-Time Protection** and **Computer Scan** modules, which all use ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- **Startup Protection** - Automatic startup file check
- **Real-Time Protection** - Real-time file system protection
- **Computer Scan** - On-demand computer scan
- **Web Access Protection**
- **Email Protection**

The ThreatSense parameters are specifically optimized for each module, and their modification can significantly influence system operation. For example, changing settings to

always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in a slower system. Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects

The **Objects** section allows you to define which files will be scanned for infiltrations.

• **Symbolic links** – (Computer scan only) scans files that contain a text string that is interpreted as a path to a file or directory.

• **Email files** – (not available in Real-time Protection) scans email files.

• **Mailboxes** – (not available in Real-time Protection) scans user mailboxes in the system. Incorrect use of this option may result in a conflict with your email client. To learn more about advantages and disadvantages of this option, read the following knowledgebase article.

• **Archives** – (not available in Real-time Protection) scans files compressed in archives (.rar, .zip, .arj, .tar, etc.).

• **Self-extracting archives** – (not available in Real-time Protection) scans files which are contained in self-extracting archive files.

• **Runtime packers** – unlike standard archive types, runtime packers decompress in memory. When this is selected, standard static packers (e.g. UPX, yoda, ASPack, FGS) are also scanned.

Options

In the **Options** section, you can select the methods used during a scan of the system. The following options are available:

• **Heuristics** – Heuristics use an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist.

• **Advanced heuristics** – Advanced heuristics is comprised of a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. The program's detection ability is significantly higher as a result of advanced heuristics.

Cleaning

Cleaning settings determine the manner in which the scanner cleans infected files. There are 3 levels of cleaning:

• **No cleaning** – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.

• **Standard cleaning** – The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow-up actions. The choice of follow-up actions will also be displayed if a predefined action cannot be completed.

• **Strict cleaning** – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean a file, you will receive a notification and be asked to select the type of action to take.

Standard cleaning mode - archive cleaning

In the default Standard cleaning mode, entire archive files are deleted only if all files in the archive are infected. If an archive contains legitimate files as well as infected files, it will not be deleted. If an infected archive file is detected in Strict cleaning mode, the entire archive will be deleted even if clean files are present.

Exclusions

An extension is the part of a file name delimited by a period. The 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 scanning.

By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. Using the + and − buttons, you can enable or prohibit the scanning of specific extensions.

Excluding files from scanning is sometimes necessary if scanning certain file types prevents the program from functioning properly. For example, it may be advisable to exclude *log*, *cfg* and *tmp* files. The correct format for entering file extensions is:

log

cfg

tmp

Limits

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

• **Maximum Size:** Defines the maximum size of objects to be scanned. The antivirus module will only scan objects smaller than the size specified. We do not recommend changing the default value, as there is usually no reason to modify it. This option should only be changed by advanced users who have specific reasons for excluding larger objects from scanning.

• **Maximum Scan Time:** Defines the maximum time allotted to scan an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, whether or not the scan has finished.

• **Maximum Nesting Level:** Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances, there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.

• **Maximum File Size:** This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If scanning is prematurely terminated as a result of this limit, the archive will remain unchecked.

Others

Enable Smart optimization

With Smart Optimization enabled, settings are optimized to ensure the most efficient level of scanning without compromising scanning speed. The various protection modules scan intelligently, making use of different scanning methods. Smart Optimization is not rigidly defined within the product. The ESET Development Team is continuously implementing new changes which are then integrated into ESET Endpoint Security for macOS through regular updates. If Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular module are applied when performing a scan.

Scan alternative data stream (On-demand scanner only)

Alternate data streams (resource/data forks) used by the file system are file and folder

associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.

An infiltration is detected

Infiltrations can reach the system from various entry points: webpages, shared folders, email or removable computer devices (USB, external disks, CDs, DVDs, etc.).

If your computer is showing signs of malware infection, for example it runs slower, often freezes, etc., we recommend that you take the following steps:

1. Click **Computer scan**.
2. Click **Smart scan** (for more information, see the Smart scan section).
3. After the scan has finished, review the log for the number of scanned, infected and cleaned files.

If you only want to scan a certain part of your disk click **Custom scan** and select targets to scan for malware.

As a general example of how infiltrations are handled by ESET Endpoint Security for macOS, suppose that an infiltration is detected by the Real-time file system monitor using the default cleaning level. Real-time protection will attempt to clean or delete the file. If there is no predefined action available for the Real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, since the infected file(s) is left in its infected state. This option is intended for situations when you are sure that the file is harmless and has been detected by mistake.

Cleaning and deleting – Apply cleaning if a file has been attacked by a virus that has attached malicious code to it. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

Deleting files in archives – In the default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if

they also contain harmless clean files. Use caution when performing a **Strict cleaning** scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

Web and email protection

To access Web and Mail protection from the main menu, click **Setup** > **Web and Mail**. From here you can also access detailed settings for each module by clicking **Setup.**

Scanning exceptions
ESET Endpoint Security for macOS does not scan encrypted protocols HTTPS, POP3S and IMAPS.

- **Web access protection** – monitors HTTP communication between web browsers and remote servers.
- **Email client protection** – provides control of email communication received through POP3 and IMAP protocols.
- **Anti-Phishing protection** – blocks potential phishing attacks coming from websites or domains.
- **Web control** – blocks webpages that may contain inappropriate or offensive material.

Web access protection

Web access protection monitors communication between web browsers and remote servers for compliance with HTTP (Hypertext Transfer Protocol) rules.

Web filtering can be achieved by defining the port numbers for HTTP communication and/or URL addresses.

Ports

In the **Ports** tab you can define the port numbers used for HTTP communication. By default, the port numbers 80, 8080 and 3128 are predefined.

URL lists

The **URL Lists** section enables you to specify HTTP addresses to block, allow or exclude from checking. Websites in the list of blocked addresses will not be accessible. Websites in the list of excluded addresses are accessed without being scanned for malicious code.

To only allow access to URLs listed in the **Allowed URL** list, select **Restrict URL addresses**.

To activate a list, select **Enabled** next to the list name. If you want to be notified when entering an address from the current list, select **Notified**.

The special symbols * (asterisk) and *?* (question mark) can be used when building URL lists. The asterisk substitutes any character string and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list.

Email protection

Email protection provides control of email communication received through the POP3 and IMAP protocols. When examining incoming messages,ESET Endpoint Security for macOS uses the advanced scanning methods included in the ThreatSense scanning engine. Scanning of the POP3 and IMAP protocol communications will occur when any email client used.

ThreatSense Engine: Setup – advanced virus scanner setup enables you to configure scan targets, detection methods, etc. Click **Setup** to display the detailed scanner setup window.

Append tag message to email footnote – after an email has been scanned, a notification containing the scan results can be appended to the message. Tag messages cannot be relied on exclusively, since the tags may be omitted in problematic HTML messages and can be forged by some viruses. The following options are available:

- **Never** – no tag messages will be added
- **To infected email only** – only messages containing malicious software will be tagged as checked

• **To all scanned email** – ESET Endpoint Security for macOS will append tag messages to all scanned email

Append note to the subject of received and read infected email – select this check box if you want email protection to include a virus warning in the infected email. This feature allows for simple filtering of infected emails. It also increases the level of credibility for the recipient, and if an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

Template added to the subject of infected email – edit this template to modify the subject prefix format of an infected email.

• %avstatus% - Adds the email infection status (for example: clean, infected...)

• %virus% - Adds the name of the threat

• %aspmstatus% - Changes the subject based on the outcome on the antispam scan

• %product% - Adds the name of your ESET product (in this case - ESET Endpoint Security for macOS)

• %product_url% - Addsthe ESET website link (www.eset.com)

In the lower section of this window, you can also enable/disable the checking of email communication received through the POP3 and IMAP protocols. To learn more, refer to the following topics:

• POP3 protocol checking

• IMAP protocol checking

POP3 protocol checking

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET Endpoint Security for macOS provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. Make sure the module is enabled for protocol filtering to work correctly, POP3 protocol checking is performed automatically with no need to reconfigure your email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a

comma.

If **Enable POP3 protocol checking** is selected, all POP3 traffic is monitored for malicious software.

IMAP protocol checking

The Internet Message Access Protocol (IMAP) is another Internet protocol for e-mail retrieval. IMAP has some advantages over POP3, for example multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. ESET Endpoint Security for macOS provides protection for this protocol, regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. Make sure that IMAP protocol checking is enabled for the module to work correctly; IMAP protocol control is performed automatically with no need to reconfigure your email client. By default, all communication on port 143 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

If **Enable IMAP protocol checking** is selected, all IMAP traffic is monitored for malicious software.

Anti-Phishing

The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, credit card numbers, PIN numbers or usernames and passwords.

We recommend that you keep Anti-Phishing enabled (**Setup** > **Enter application preferences ...** > **Anti-Phishing Protection**). All potential phishing attacks coming from dangerous websites or domains will be blocked and a warning notification will be displayed informing you of the attack.

Firewall

The firewall controls all network traffic to and from the system by allowing or denying individual network connections based on specified filtering rules. It provides protection against attacks from remote computers and enables blocking of some services. It also provides antivirus protection for HTTP, POP3 and IMAP protocols.

Firewall configuration can be found in **Setup** > **Firewall**. It allows you to adjust the filtering mode, rules and detailed settings. You can also access more detailed settings of the program from here.

If you enable **Block all network traffic: disconnect network**, all inbound and outbound communication will be blocked by the firewall. Use this option only if you suspect critical security risks require that the system be disconnected from the network.

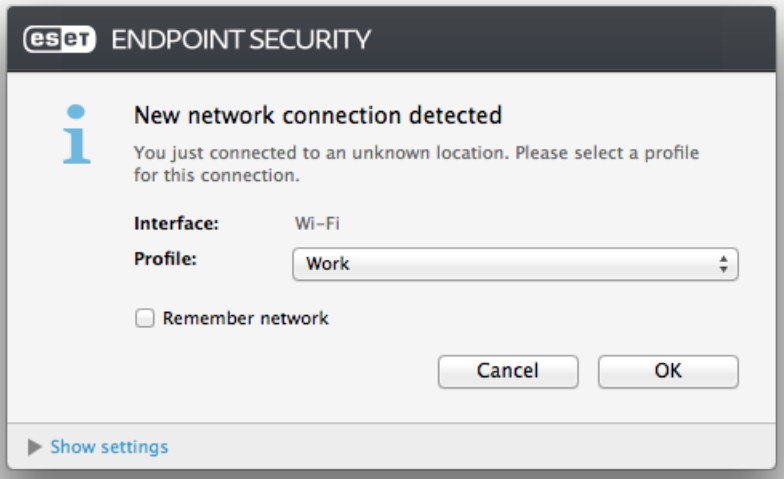
Filtering modes

Three filtering modes are available for the ESET Endpoint Security for macOS firewall. Filtering mode settings can be found under **Setup** > **Enter application preferences...** > **Firewall**. The behavior of the firewall changes based on the selected mode. Filtering modes also influence the level of user interaction required.

All traffic blocked – all inbound and outbound connections will be blocked.

Auto with exceptions – the default mode. This mode is suitable for users who prefer easy and convenient use of the firewall with no need to define rules. Automatic mode allows standard outbound traffic for the given system and blocks all non-initiated connections from the network side. You can also add custom, user-defined rules.

Interactive – allows you to build a custom configuration for your firewall. When communication is detected and no existing rules apply to that communication, a dialog window reporting an unknown connection will be displayed. The dialog window gives the option to allow or deny communication, and the decision to allow or deny can be remembered as a new rule for the firewall. If you choose to create a new rule, all future connections of this type will be allowed or blocked according to the rule.



To record detailed information about all blocked connections to a log file, select **Log all blocked connections**. To review the firewall log files, from the main menu click **Tools** > **Logs** and select **Firewall** from the **Log** drop-down menu.

Firewall rules

Rules represent a set of conditions used to test all network connections and determine the actions assigned to these conditions. Using the firewall rules, you can define the type of action to take if a connection defined by a rule is established.

Incoming connections are initiated by a remote computer attempting to establish a connection with the local system. Outgoing connections work in the opposite way – the local system contacts a remote computer.

If a new unknown communication is detected, you must carefully consider whether to allow or deny it. Unsolicited, unsecured or unknown connections pose a security risk to the system. If such a connection is established, we recommend that you pay particular attention to the remote computer and the application attempting to connect to your computer. Many infiltrations try to obtain and send private data, or download other malicious applications to host workstations. The firewall allows you to detect and terminate such connections.

Allow software signed by Apple to access the network automatically - By default, applications signed by Apple can automatically access the network. For application to be able to interact with Apple services or to be installed on devices, this application needs to be signed with a certificate issued by Apple. If you want to disable this, deselect this option.

Applications not signed with Apple certificate will require user action or a rule to be able to access the network.

When this option is disabled, network communication with Apple signed services requires user approval unless a firewall rule defines it.

Changes from previous versions, ESET Endpoint Security for macOS 6.8 and older blocked incoming communication to services with Apple certificate. In the current version, ESET Endpoint Security for macOS is able to identify the local receiver of incoming communication, and if this option is enabled, the incoming communication is allowed.

Creating new rules

The **Rules** tab contains a list of all rules applied to traffic generated by individual applications. Rules are added automatically according to user reactions to a new communication.

1. To create a new rule, click **Add...** , enter a name for the rule and drag-and-drop the application's icon into the blank field or click **Browse** to look for the program in the */Applications* folder. To apply the rule to all applications installed on your computer, select **All applications**.
2. In the next window, specify the **Action** (allow or deny the communication between selected application and network) and **Direction** of the communication (incoming, outgoing or both). Select **Log rule** to record all communications that involve this rule. To review firewall logs, click **Tools** > **Logs** from the ESET Endpoint Security for macOS main menu and select **Firewall** from the **Log** drop-down menu.
3. In the **Protocol/Ports** section, set the protocol and port that the application uses (if TCP or UDP protocol is selected) to communicate. The transport protocol layer provides secure and efficient data transfer.
4. Last, specify the **Destination** criteria (IP address, range, subnet, ethernet or Internet) for the rule.

Firewall zones

A zone represents a collection of network addresses which create one logical group. Each address in a given group is assigned similar rules defined centrally for the whole group.

These zones can be created by clicking **Add.** Enter a **Name** and **Description** (optional) for

the zone, select a profile this zone will belong to and add an IPv4/IPv6 address, address range, subnet, WiFi network or an interface.

Firewall profiles

Profiles allow you to control the behavior of the ESET Endpoint Security for macOS firewall. When creating or editing a firewall rule, you can assign it to a specific profile. When you select a profile, only the global rules (with no profile specified) and the rules that have been assigned to that profile are applied. You can create multiple profiles with different rules assigned to easily alter firewall behavior.

Firewall logs

The ESET Endpoint Security for macOS firewall saves all important events in a log file. To access firewall logs from the main menu click **Tools** > **Logs** and then select **Firewall** from the **Log** drop-down menu.

Log files are a valuable tool for detecting errors and revealing intrusions into your system. ESET firewall logs contain the following data:

- Date and time of event
- Name of event
- Source
- Target network address
- Network communication protocol
- Rule applied
- Application involved
- User

A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and can be defended against using firewall such as: frequent connections from unknown locations, multiple attempts to establish connections, unknown applications communicating or unusual port numbers.

Device control

ESET Endpoint Security for macOS allows you to scan, block or adjust extended filters and/or permissions and define a user's ability to access and work with a given device. This is useful if the computer administrator wants to prevent the use of devices containing unsolicited content.

Supported external devices:

- Disk storage (HDD, USB flash drive)
- CD/DVD
- USB printer
- Imaging Device
- Serial port
- Network
- Portable Device

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

The Device control log records all incidents that trigger Device control. Log entries can be viewed from the main program window of ESET Endpoint Security for macOS in **Tools** > **Log files**.

Rules editor

Device control setup options can be modified in **Setup** > **Enter application preferences...** > **Device Control**.

Clicking **Enable device control** activates the Device control feature in ESET Endpoint Security for macOS. Once Device control is enabled, you can manage and edit Device control roles. Select the check box next to a rule name to enable disable the rule.

Use the + or − buttons to add or remove rules. Rules are listed in order of priority with higher-priority rules closer to the top. To re-arrange the order, drag-and-drop a rule to its new position or click ⚙ and choose one of the options.

ESET Endpoint Security for macOS automatically detects all currently inserted devices and their parameters (Device type, Vendor, Model, Serial number). Instead of creating rules manually, click the **Populate** option, select the device and click **Continue** to create the rule.

Specific devices can be allowed or blocked according to their user, user group, or any of several additional parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as name, device type, logging severity and action to perform after connecting a device to your computer.

Name

Enter a description of the rule into the **Name** field for better identification. The **Rule enabled** check box disables or enables this rule—this can be useful if you do not want to delete the rule permanently.

Device Type

Choose the external device type from the drop-down menu. Device type information is collected from the operating system. Storage devices include external disks or conventional memory card readers connected via USB or FireWire. Examples of imaging devices are scanners or cameras. Because these devices only provide information about their actions and do not provide information about users, they can only be blocked globally.

Action

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

Read/Write – Full access to the device will be allowed

Read Only – Only read access to the device will be allowed

Block – Access to the device will be blocked

Criteria type

Select **Device group** or **Device**. Additional parameters shown below can be used to fine-tune rules and tailor them to devices.

Vendor – Filter by vendor name or ID

Model – The given name of the device

Serial – External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD/DVD drive

No parameters defined

If these parameters are not defined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-insensitive and no wildcards (*, ?) are supported.

TIP

To view information about a device, create a rule for that type of device and connect the device to your computer. Once the device has been connected, device details will be displayed in the Device control log.

Logging severity

Always – Logs all events

Diagnostic – Logs information needed to fine-tune the program

Information – Records informative messages plus all the records above

Warning – Records critical errors and warning messages

None – No logs will be recorded

User list

Rules can be limited to certain users or user groups by adding them to the User list:

Edit... – Opens the **Identity editor** where you can select users or groups. To define a list of users, select them from the **Users** list on the left side and click **Add**. To remove a user, select their name from the **Selected Users** list and click **Remove**. To display all system users, select **Show all users**. If the list is empty, all users will be permitted

User rules limitations
Not all devices can be filtered by user rules (for example imaging devices do not provide information about users, only about actions).

Web control

The **Web control** feature allows you to configure settings that protect your company from risk of legal liability. Web control can regulate access to websites that violate intellectual property rights. The goal is to prevent employees from accessing pages with inappropriate or harmful content, or pages that may have a negative impact on productivity. Employers or system administrators can prohibit access to more than 27 pre-defined website categories and over 140 subcategories.

By default, Web control is disabled. To activate it, click **Setup** > **Enter application preferences** > **Web control** and select the check box next to **Enable Web control**.

The rule editor window displays existing URL-based or Category-based rules. The list of rules contains several descriptions of rules such as name, type of blocking, action to perform after matching a Web control rule and log severity.

To create a new rule, click the  button. Double-click the **Name** field and enter a description of the rule for better identification.

The check box in the **Enabled** field enables/disables the rule – this can be useful if you want to use the rule later but do not want to delete it permanently.

Type

URL-based Action – access to the given website. Double-click the **URL/Category** field and enter the appropriate URL address.

In the URL address list, the special symbols * (asterisk) and ? (question mark) cannot be used. Web page addresses with multiple TLDs (top-level domains) must be entered to the created group (*examplepage.com*, *examplepage.sk* etc.). When you add a domain to the list, all content located on this domain and all subdomains (for example, *sub.examplepage.com*) will be blocked or allowed based on your choice of URL-based action.

Category-based Action – double-click the **URL/Category** field and select the categories.

Identity

Allows you to select users the rule will be applied to.

Access rights

Allow – Access to the URL address/category will be granted

Block – Blocks the URL address/category

Severity (for filtering log files)

Always – Logs all events

Diagnostic – Logs information needed to fine-tune the program

Information – Records informative messages, plus all the records above

Warning – Records critical errors and warning messages

None – No logs will be created

Tools

The **Tools** menu includes modules that help simplify program administration and offer additional options for advanced users.

Log files

Log files contain information about all important program events that have occurred and provide an overview of detected threats. Logging is an essential tool in system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. It is possible to view text messages and logs directly from the ESET Endpoint Security for macOS environment, as well as to archive logs.

Log files are accessible from the ESET Endpoint Security for macOS main menu by clicking **Tools** > **Log files**. Select the desired log type using the Log drop-down menu at the top of

the window. The following logs are available:

1. **Detected threats** – Information about events related to the detection of infiltrations.
2. **Events** – All important actions performed by ESET Endpoint Security for macOS are recorded in the Event logs.
3. **Computer scan** – Results of all completed scans are displayed in this window. Double-click any entry to view the details of a specific computer scan.
4. **Device control** – Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial number, vendor name and media size (if available).
5. **Firewall** – The firewall log displays all remote attacks detected by the firewall. Firewall logs contain information about detected attacks on your system. The **Event** column lists the detected attacks, the **Source** column tells you more about the attacker and the **Protocol** column reveals the communication protocol used for the attack.
6. **Web control** – Shows blocked or allowed URL addresses and details about how they were categorized.
7. **Filtered websites** – This list is useful if you want to view a list of websites that were blocked by Web access protection or Web control. In these logs you can see the time, URL, status, IP address, user and application that opened a connection to the particular website.

Right-click any log file and click **Copy** to copy the contents of that log file to the clipboard.

Log maintenance

The logging configuration for ESET Endpoint Security for macOS is accessible from the main program window. Click **Setup** > **Enter application preferences** > **Tools** > **Log Files**. You can specify the following options for log files:

- **Delete old log records automatically** – log entries older than the specified number of days are automatically deleted.
- **Optimize log files automatically** – enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded.

All the relevant information displayed in the graphic user interface, threat and event

messages can be stored in human readable text formats such as plain text or CSV (Comma-separated values). If you want to make these files available for processing using third-party tools, select the check box next to **Enable logging to text files.**

To define the target folder to which the log files will be saved, click **Setup** next to **Advanced setup**.

Based on the options selected under **Text Log Files: Edit**, you can save logs with the following information written:

- Events such as *Invalid username and password*, *Modules can not be updated* etc. are written to the *eventslog.txt* file.
- Threats detected by the Startup scanner, Real-Time Protection or Computer Scan are stored in the file named *threatslog.txt*.
- The results of all completed scans are saved in the format *scanlog.NUMBER.txt*.
- Devices blocked by Device Control are mentioned in devctllog.txt
- All events related to communication through the Firewall are written to firewalllog.txt
- Webpages blocked by Web control are mentioned in webctllog.txt

To configure the filters for **Default Computer Scan Log Records**, click **Edit** and select/deselect log types as required. Further explanation to these log types can be found in Log Filtering.

Log filtering

Logs store information about important system events. The log filtering feature allows you to display records about specific events.

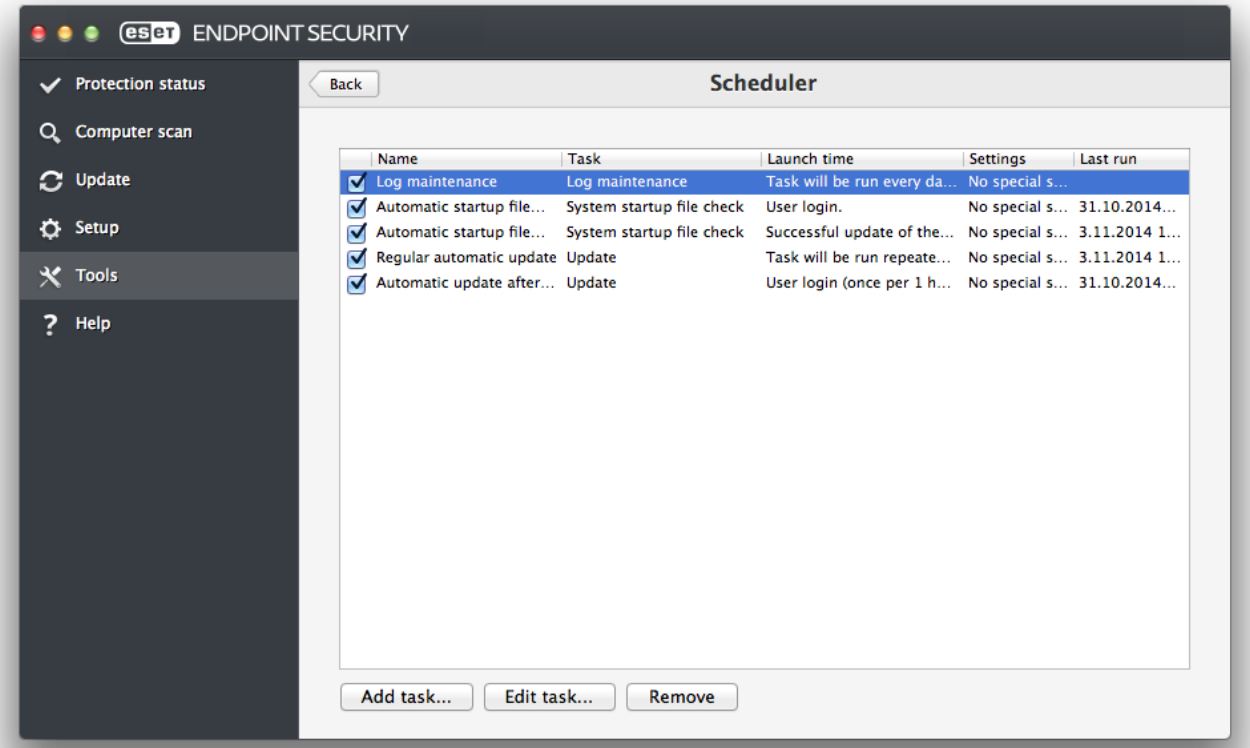
The most frequently used log types are listed below:

- **Critical warnings** – critical system errors (for example, Antivirus protection failed to start)
- **Errors** – error messages such as "*Error downloading file*" and critical errors

- **Warnings** – warning messages
- **Informative records** – informative messages including successful updates, alerts, etc.
- **Diagnostic records** – information needed to fine-tune the program as well as all records described above.

Scheduler

The **Scheduler** can be found in the ESET Endpoint Security for macOS main menu under **Tools**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used.



The Scheduler manages and launches scheduled tasks with predefined configurations and properties. The configuration and properties contain information such as the date and time as well as specified profiles to be used during execution of the task.

By default, the following scheduled tasks are displayed in the Scheduler:

- Log maintenance (after enabling **Show system tasks** in scheduler setup)
- Startup file check after user logon

- Startup file check after successful update of detection modules
- Regular automatic update
- Automatic update after user logon

To edit the configuration of an existing scheduled task (both default and user-defined), CTRL+click the task you want to modify and select **Edit** or select the task and click **Edit task**.

Creating new tasks

To create a new task in Scheduler, click **Add task** or press control+click in the blank field and select **Add** from the context menu. Four types of scheduled tasks are available:

- **Run application**
- **Update**
- **On-demand computer scan**
- **System startup file check**

User defined tasks

By default, applications are run by a special ESET-created user that has restricted rights. To change the user from the default, type the user name followed by a colon (:) in front of the command. You can also use the **root** user in this feature.

Example: Run task as user

In this example we will schedule the calculator app to start at a selected time as a user named **UserOne**:

1. In the **Scheduler**, select **Add task**.
2. Type in the task name. Select **Run application** as a **Scheduled task**. In the **Run Task** window, select **Once** to run this task a single time. Click **Next**.
3. Click Browse and select the Calculator app.
4. Type **UserOne:** before the application path (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') and click **Next**.
5. Select a time to execute the task and click **Next**.
6. Select an alternate option if the task is unable to run and click **Next**.
7. Click **Finish**.
8. The ESET Scheduler will start the Calculator app at the time you selected.

User name limitations

Spaces or white space characters cannot be used in front of a user name. Spaces also cannot be used in the user name. A blank character should be used instead.

Scanning as an directory owner

You can scan directories as the owner of the directory:
root:for VOLUME in /Volumes/; do sudo -u \#`stat -f %u "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done*

You can also scan the /tmp folder as a currently logged-in user:
root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

Example: Update Task

In this example we will create an update task that will run at a specified time.

1. Select **Update** from the **Scheduled task** drop-down menu.
2. Type a name for the task in the **Task name** field.
3. Select the frequency of the task from the **Run task** drop-down menu. Based on the frequency selected, you will be prompted to specify different update parameters. If you select **User-defined**, you will be prompted to specify date/time in the cron format (see the Creating a user-defined task section for more details).
4. In the next step, select an alternate option if the task cannot be performed or completed at the scheduled time.
5. Click **Finish**. The new scheduled task will be added to the list of currently scheduled tasks.

By default ESET Endpoint Security for macOS contains pre-defined scheduled tasks that are configured to ensure correct product functionality. These tasks should not be modified and are hidden by default. To view these tasks, go to the main menu and click **Setup** > **Enter application preferences** > **Scheduler** and then select **Show system tasks**.

Creating user-defined task

There are a few special parameters that must be defined when you select **User-defined** as the task type from the **Run task** drop-down menu.

The date and time of a **User-defined** task has to be entered in year-extended cron format (a string comprising 6 fields separated by white space):

```
minute(0-59) hour(0-23) day of month(1-31) month(1-12) year(1970-2099) day of
week(0-7)(Sunday = 0 or 7)
```

Example:

```
30 6 22 3 2012 4
```

The following special characters are supported in cron expressions:

- asterisk (*) – expression will match for all values of the field; e.g. asterisk in the 3rd field

(day of month) means every day

• hyphen (`-`) – defines ranges; e.g. `3-9`

• comma (`,`) – separates items of a list; e.g. `1,3,7,8`

• slash (`/`) – defines increments of ranges; e.g. `3-28/5` in the 3rd field (day of month) means 3rd day of the month and then every 5 days.

Day names (Monday-Sunday) and month names (January-December) are not supported.

NOTE:

> **User defined tasks**
> If you define both a day of the month and day of the week, the command will only be executed when both fields match.

Live Grid

The Live Grid Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional Live Grid Early Warning System has a single purpose – to improve the protection that we can offer you. The best way to ensure that we see new threats as soon as they appear is to “link“ to as many of our customers as possible and use the information they collect to keep our detection modules constantly up-to-date. Select one of two options for Live Grid:

1. You can choose not to enable the Live Grid Early Warning System. You will not lose any functionality in the software, but, in some cases, ESET Endpoint Security for macOS may respond faster to new threats than a detection modules update.
2. You can configure the Live Grid Early Warning System to submit anonymous information about new threats and where new threatening code is contained. This information can be sent to ESET for detailed analysis. Studying these threats will help ESET update its detection modules and improve our threat detection ability.

The Live Grid Early Warning System 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.

While there is a chance this may occasionally disclose some information about you or your computer (usernames in a directory path, etc.) to the ESET Threat Lab, this information will not be used for ANY purpose other than to help us respond immediately to new threats.

To access Live Grid setup from the main menu, click **Setup** > **Enter application preferences** > **Live Grid**. Select **Enable ESET Live Grid reputation system (recommended)** to activate Live Grid and then click **Setup** next to **Advanced Options**.

Suspicious files

By default, ESET Endpoint Security for macOS is configured to submit suspicious files to the ESET Threat Lab for detailed analysis. If you do not wish to submit these files automatically, deselect **Submission of Suspicious Files (Setup** > **Enter application preferences** > **Live Grid > Setup)**.

If you find a suspicious file, you can submit it to our Threat Lab for analysis. To do so, click **Tools** > **Submit file for analysis** from the main program window. If it is a malicious application, its detection will be added to an upcoming update.

Submission of Anonymous Statistical Information – The ESET Live Grid Early Warning System collects anonymous information about your computer related to newly detected threats. This information includes the name of the infiltration, the date and time it was detected, the ESET security product version, your operating system version and the location setting. These statistics are typically delivered to ESET servers once or twice daily.

Example: Submitted statistical package

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"

# language="ENGLISH"

# osver=9.5.0

# engine=5417

# components=2.50.2

# moduleid=0x4e4f4d41

# filesize=28368

# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

Exclusion Filter – This option allows you to exclude certain file types from submission. For example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, .rtf etc.). You can add file types to the list of excluded files.

Contact Email (optional) – Your email address will be used if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

Quarantine

The main purpose 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 being falsely detected by ESET Endpoint Security for macOS.

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 to the ESET Threat Lab for analysis.

Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, the reason it was quarantined (for example, added by user) and the number of threats detected. The quarantine folder (*/Library/Application Support/Eset/esets/cache/quarantine*) remains in

the system even after uninstalling ESET Endpoint Security for macOS. Quarantined files are stored in a safe encrypted form and can be restored again after installing ESET Endpoint Security for macOS.

Quarantining files

ESET Endpoint Security for macOS automatically quarantines deleted files (if you have not deselected this option in the alert window). From the **Quarantine** window, you can click **Quarantine** to manually add any file to the quarantine. You can also ctrl-click a file at any time and select **Services** > **ESET Endpoint Security for macOS - Add files to Quarantine** from the context menu to send the file to the quarantine.

Restoring from Quarantine

Quarantined files can also be restored to their original location, to do so, select a quarantined file and click **Restore**. Restore is also available from the context menu, CTRL+click a given file in the Quarantine window and click **Restore**. You can use **Restore to** to restore a file to a location other than the one from which it was quarantined.

Submitting file from Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (for example, by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Threat Lab. To submit a file from quarantine, CTRL+click the file and select **Submit file for analysis** from the context menu.

Privileges

ESET Endpoint Security for macOS settings can be very important to your organization's security policy. Unauthorized modifications may endanger the stability and protection of your system. Consequently, you can choose which users will have permission to edit the program configuration.

You can configure privileged users under **Setup** > **Enter application preferences** > **User** > **Privileges**.

To provide maximum security for your system, it is essential that the program be configured correctly. Unauthorized modifications can result in the loss of important data. To set a list of privileged users, select them from the **Users** list on the left side and click **Add**. To remove a

user, select their name from the **Privileged Users** list on the right side and click **Remove**. To display all system users, select **Show all users**.

NOTE: If the list of privileged users is empty, all users of the system will have permission to edit the program settings.

Presentation mode

Presentation mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows and want to minimize CPU usage. Presentation mode can also be used during presentations that cannot be interrupted by antivirus activity. When enabled, all pop-up windows are disabled and scheduled tasks are not run. System protection still runs in the background, but does not require any user interaction.

To enable Presentation mode manually, click **Setup** > **Enter application preferences...** > **Presentation mode** > **Enable Presentation mode**.

Select the check box next to **Auto-enable Presentation mode in fullscreen t**o trigger Presentation mode automatically when applications are run in fullscreen mode. When this feature is enabled, Presentation mode will start whenever you initiate a fullscreen application and will automatically stop after you exit the application. This is especially useful for starting a presentation.

You can also select **Disable Presentation mode automatically after** to define the amount of time in minutes after which Presentation mode will automatically be disabled.

Enabling Presentation mode is a potential security risk, so the ESET Endpoint Security for macOS protection status icon will turn orange and display a warning.

NOTE: If the firewall is in Interactive mode and Presentation mode is enabled, you might have trouble connecting to the Internet. This can be problematic if you start an application that connects to the Internet. Normally, you would be asked to confirm such an action (if no communication rules or exceptions have been defined), but user interaction is disabled in Presentation mode. The solution is to define a communication rule for every application that might be in conflict with this behavior or to use a different Filtering mode in the firewall. Keep

in mind that if Presentation mode is enabled and you go to a webpage or an application that might be a security risk, it may be blocked but you will not see any explanation or warning because user interaction is disabled.

Running processes

The list of **Running processes** displays the processes running on your computer. ESET Endpoint Security for macOS provides detailed information on running processes to protect users using ESET Live Grid technology.

• **Process** – name of the process that is currently running on your computer. You can also use Activity monitor (found in */Applications/Utilities*) to view all processes running on your computer.

• **Risk level** – in most cases, ESET Endpoint Security for macOS and ESET Live Grid technology assign risk levels to objects (files, processes, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level. Known applications marked green are definitely clean (whitelisted) and will be excluded from scanning. This improves the speed of both the On-demand and Real-time scans. When an application is marked as unknown (yellow), it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about a file, you can submit it to the ESET Threat Lab for analysis. If the file turns out to be a malicious application, its signature will be added to an upcoming update.

• **Number of Users** – the number of users that use a given application. This information is gathered by ESET Live Grid technology.

• **Time of discovery** – period of time since the application was discovered by ESET Live Grid technology.

• **Application Bundle ID** – name of the vendor or application process.

By clicking a given process, the following information will appear at the bottom of the window:

• **File** – location of an application on your computer

• **File Size** – physical size of the file on the disk

• **File Description** – file characteristics based on the description from the operating system

• **Application Bundle ID** – name of the vendor or application process

- **File Version** – information from the application publisher
- **Product name** – application name and/or business name

User interface

The user interface configuration options allow you to adjust the working environment to fit your needs. These options are accessible from the main menu by clicking **Setup** > **Enter application preferences...** > **Interface**.

- To display the ESET Endpoint Security for macOS splash screen at system startup, select **Show splash-screen at startup**.
- **Present application in Dock** allows you to display the ESET Endpoint Security for macOS icon in the macOS Dock and switch between ESET Endpoint Security for macOS and other running applications by pressing *cmd+tab*. Changes take effect after you restart ESET Endpoint Security for macOS (usually triggered by computer restart).
- **Use standard menu** allows you to use certain keyboard shortcuts (see Keyboard shortcuts) and see standard menu items (User interface, Setup and Tools) on the macOS Menu Bar (top of the screen).
- Enable **Show tooltips** to display tooltips when the cursor is placed over certain options in ESET Endpoint Security for macOS.
- **Show hidden files** allows you to see and select hidden files in **Scan Targets** setup for a **Computer scan**.
- By default, ESET Endpoint Security for macOS icon is displayed in the Menu Bar Extras that appear at the right of the macOS Menu Bar (top of the screen). To disable this, deselect **Show icon in menu bar extras**. This change takes effect after you restart ESET Endpoint Security for macOS (usually triggered by computer restart).

Alerts and notifications

The **Alerts and notifications** section allows you to configure how threat alerts, protection status and system notifications are handled by ESET Endpoint Security for macOS.

Disabling **Display alerts** will disable all alert windows and is only recommended in specific situations. For most users, we recommend that this option be left on its default setting (enabled). Advanced options are described in this chapter.

Selecting **Display notifications on desktop** will cause alert windows that do not require user interaction to display on the desktop (in the upper-right corner of your screen by default). You can define the period for which a notification will be displayed by adjusting the **Close notifications automatically after** X **seconds** value (5 seconds by default).

Since ESET Endpoint Security for macOS version 6.2, you can also prevent certain **Protection statuses** from displaying in the program's main screen (**Protection status** window). To learn more about this, see the Protection statuses.

Display alerts

ESET Endpoint Security for macOS displays alert dialog windows informing you of new program versions, operating system updates, the disabling of certain program components, the deletion of logs etc. You can suppress each notification individually by selecting **Do not show this dialog again**.

List of Dialogs (found under **Setup** > **Enter application preferences ...** > **Alerts and notifications** > **Display alerts: Setup...**) shows the list of all alert dialogs triggered by ESET Endpoint Security for macOS. To enable or suppress each notification, select the check box left of the **Dialog Name**. When the check box is selected, the notification will be always displayed and **Display Conditions** do not apply. If you do not wish to receive notification about certain event in the list, deselect this option and additionally, you can define **Display Conditions** under which certain action will be carried out.

Protection statuses

The current protection status of ESET Endpoint Security for macOS can be altered by activating or deactivating statuses in **Setup** > **Enter application preferences ...** > **Alerts and Notifications** > **Display in Protection status screen: Setup**. The status of various program features will be displayed or hidden from the ESET Endpoint Security for macOS main screen (**Protection status** window).

You can hide protection status of the following program features:

- Firewall
- Anti-Phishing
- Web access protection
- Email client protection

- Presentation mode
- Operating system update
- License expiration
- Computer restart required

Context menu

To make ESET Endpoint Security for macOS features available from the context menu, click **Setup** > **Enter application preferences** > **Context Menu** and select the check box next to **Integrate into the context menu**. Changes will take effect after you log out or restart your computer. Context menu options will be available on the desktop and in the **Finder** window when you CTRL+click on any file or folder.

Update

Regularly updating ESET Endpoint Security for macOS is necessary to maintain the maximum level of security. The Update module ensures that the program is always up to date by downloading the most recent detection modules.

Click **Update** from the main menu to view your current update status including the date and time of the last successful update and check to see if an update is needed. To begin the update process manually, click **Update modules**.

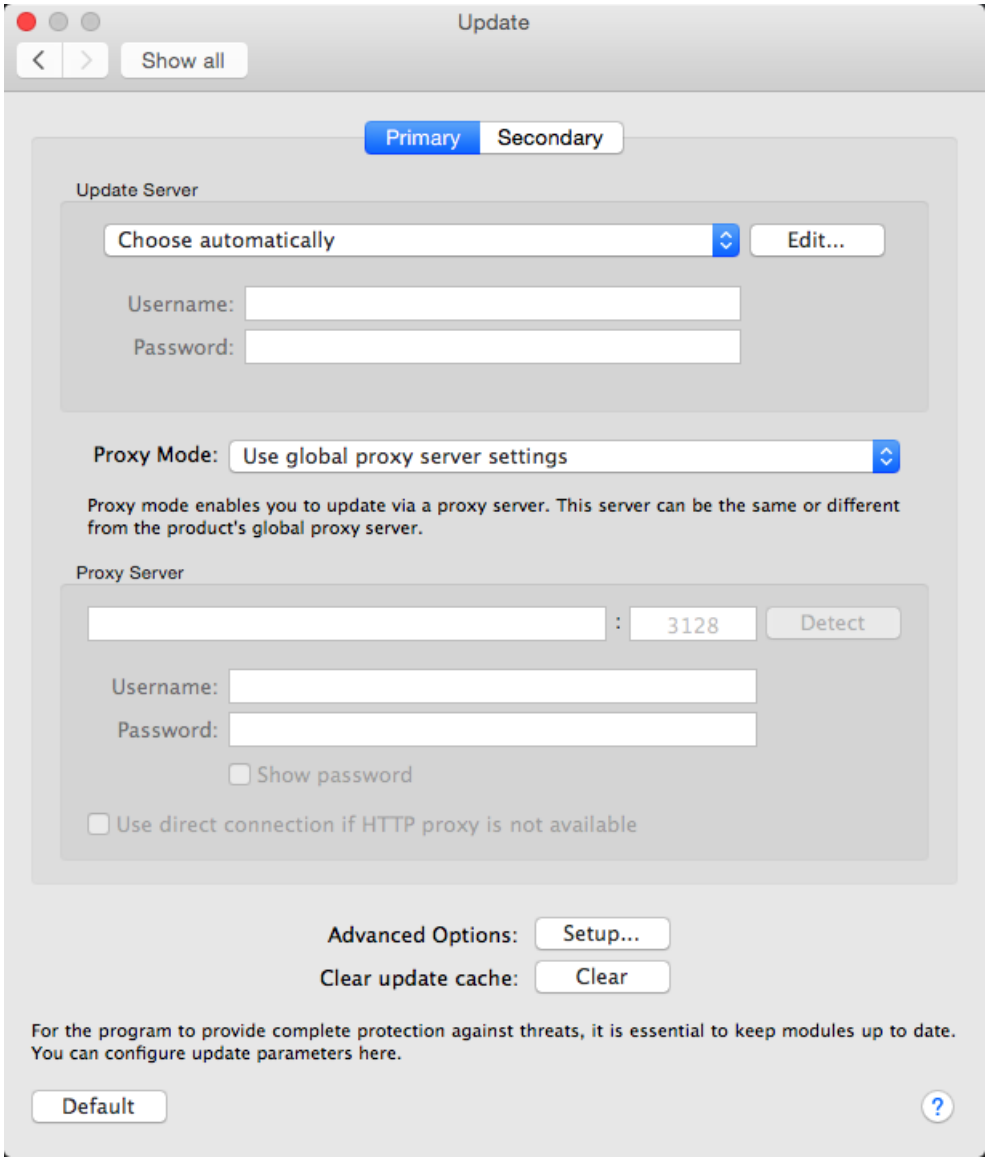
Under normal circumstances, when updates are downloaded properly, the message *Update is not necessary – the installed modules are current* will appear in the Update window if you have the latest modules. If modules cannot be updated, we recommend that you check your update settings – the most common reason for this error is incorrectly entered license data or incorrectly configured connection settings.

The **Update** window also contains the Detection engine version number. This numeric indicator is linked to the ESET website that displays Detection engine update information.

Update setup

The update setup section specifies update source information such as update servers and authentication data for these servers. By default, the **Update Server** drop-down menu is set to **Choose automatically** to ensure that update files will automatically download from the

ESET server with the least network traffic.



The list of available update servers is accessible in the **Update Server** drop-down menu. To add a new update server, click **Edit,** enter the address of the new server in the **Update Server** input field and click **Add**.

ESET Endpoint Security for macOS allows you to set an alternative or failover update server. Your **Primary** server could be your mirror server and your **Secondary server** the standard ESET update server. The secondary server must differ from the primary one, otherwise it will not be used. If you do not specify a Secondary Update Server, Username and Password, the failover update functionality will not work. You can also select **Choose automatically** and enter your Username and Password in the appropriate fields to have ESET Endpoint Security for macOS automatically select the best update server to use.

Proxy Mode enables you to update detection modules using a proxy server (for example, a

local HTTP proxy). The server can be the same or different from the global proxy server that applies to all program features that require a connection. Global proxy server settings should already have been defined during installation, or in Proxy server setup.

To configure a client to only download updates from a proxy server:

1. Select **Connection through a proxy server** from the drop-down menu.
2. Click **Detect** to let ESET Endpoint Security for macOS fill out the IP address and port number (**3128** by default).
3. Enter a valid **Username** and **Password** into the respective fields if communication with the proxy server requires authentication.

ESET Endpoint Security for macOS detects the proxy settings from macOS System Preferences. These can be configured in macOS under > **System Preferences** > **Network** > **Advanced** > **Proxies**.

If you enable **Use direct connection if HTTP proxy is not available**, ESET Endpoint Security for macOS will automatically try to connect to the Update servers without using Proxy. This option is recommended to mobile users with MacBooks.

If you are experiencing difficulty when attempting to download detection modules updates, click **Clear update cache to delete temporary update files**.

Advanced options

To disable notifications displayed after each successful update, select **Do not display notification about successful updates**.

Enable **Pre-release updates** to download development modules that are completing final testing. Pre-release updates often contain fixes for product issues. **Delayed update** downloads updates a few hours after they are released, to ensure that your clients will not receive updates until they are confirmed to be free of any issues in the wild.

ESET Endpoint Security for macOS records snapshots of detection and program modules for

use with the **Update Rollback** feature. Leave **Create snapshots of update files** enabled to have ESET Endpoint Security for macOS record these snapshots automatically. If you suspect that a new detection module and/or program module update may be unstable or corrupt, you can use the Update rollback feature to revert to a previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely. When using the Update rollback feature to revert to a previous update, use the **Set suspend period to** drop-down menu to specify the time period for which you want to suspend updates. If you select **until revoked**, normal updates will not resume until you restore them manually. Use caution when setting the time period to suspend updates.

Set maximum detection engine age automatically – Allows you to set the maximum time (in days) after which detection modules will be reported as out of date. The default value is 7 days.

How to create update tasks

Click **Update** > **Update modules** to manually trigger a detection modules update.

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET Endpoint Security for macOS:

- **Regular automatic update**
- **Automatic update after user logon**

Each of the update tasks can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see Scheduler.

System updates

The macOS system updates feature is an important component designed to protect users from malicious software. For maximum security, we recommend that you install these updates as soon as they become available. ESET Endpoint Security for macOS will notify you about missing updates according to level of importance. You can adjust the level of update importance for which notifications are displayed in **Setup** > **Enter application preferences** > **Alerts and notifications > Setup using the Display Conditions** drop-

down menu next to **Operating system updates**.

- **Show all updates** – a notification will be displayed any time that a system update is missing
- **Show only recommended** – you will be notified about recommended updates only

If you do not want to be notified about missing updates, deselect the check box next to **Operating system updates**.

The notification window provides an overview of the updates available for the macOS operating system and the applications updated through the macOS native tool – Software updates. You can run the update directly from the notification window or from the **Home** section of ESET Endpoint Security for macOS by clicking **Install the missing update**.

The notification window contains the application name, version, size, properties (flags) and additional information about available updates. The **Flags** column contains the following information:

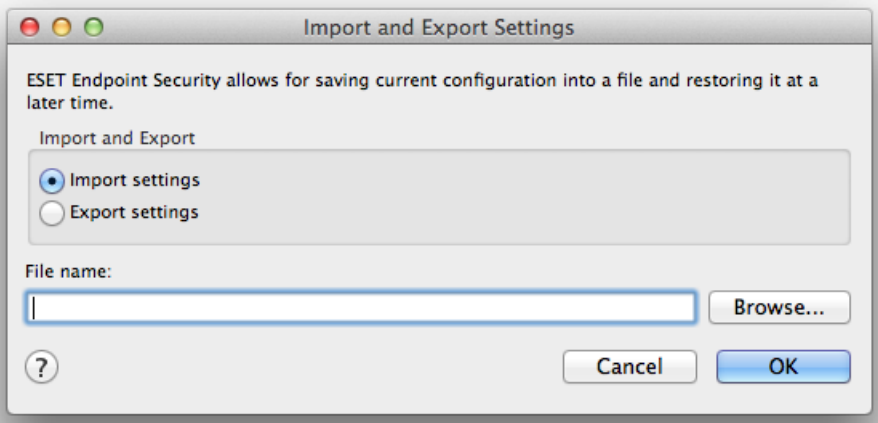
- **[recommended]** – the operating system manufacturer recommends that you install this update to increase the security and stability of the system
- **[restart]** – a computer restart is required on following installation
- **[shutdown]** – the computer must be shut down and then powered back on following installation

The notification window shows the updates retrieved by the command line tool called 'softwareupdate'. Updates retrieved by this tool can vary from the updates displayed by the 'Software updates' application. If you want to install all available updates displayed in the 'Missing system updates' window and also those not displayed by the 'Software updates' application, you have to use the 'softwareupdate' command line tool. To learn more about this tool, read the 'softwareupdate' manual by typing `man softwareupdate` into a **Terminal** window. This is recommended for advanced users only.

Import and export settings

To import an existing configuration or export your ESET Endpoint Security for macOS configuration, click **Setup** > **Import and export settings.**

Import and export are useful if you need to backup your current configuration of ESET Endpoint Security for macOS for use at a later date. Export settings is also convenient for users who want to use their preferred configuration of ESET Endpoint Security for macOS on multiple systems. You can easily import a configuration file to transfer your desired settings.



To import a configuration, select **Import settings** and click **Browse** to navigate to the configuration file you want to import. To export, select **Export settings** and use the browser to select a location on your computer to save the configuration file.

Proxy server setup

Proxy server settings can be configured in **Setup** > **Enter application preferences** > **Proxy Server**. Specifying the proxy server at this level defines global proxy server settings for all ESET Endpoint Security for macOS functions. Parameters defined here will be used by all modules that require a connection to the Internet. ESET Endpoint Security for macOS supports Basic Access and NTLM (NT LAN Manager) authentication.

To specify proxy settings for this level select **Use proxy server** and enter the IP address or URL of your proxy server in the **Proxy Server** field. In the Port field, specify the port where the proxy server accepts connections (3128 by default). You can also click **Detect** to let the

program fill out the both fields.

If communication with the proxy server requires authentication, enter a valid **Username** and **Password** into the respective fields.

Shared Local Cache

To enable the use of the Shared Local Cache, click **Setup** > **Enter application preferences** > **Shared Local Cache** and select the check box next to **Enable caching using ESET Shared Local Cache**. Use of this feature boosts 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. When enabled, information about scans of files and folders on your network is saved to the local cache. If you perform a new scan, ESET Endpoint Security for macOS will search for scanned files in the cache. If files match, they will be excluded from scanning.

Shared Local Cache settings contain the following:

- **Server address** – name or IP address of the computer where the cache is located
- **Port** – port number used for communication (3537 by default)
- **Password** – The Shared Local Cache password (optional)

Detailed instructions
For a detailed instructions on how to install and configure ESET Shared Local Cache, please refer to the ESET Shared Local Cache user guide. (The guide is available in English only.)

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: 31 333 535 (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: 31 333 535 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 provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, Livegrid®, protection against misuse of data, support, etc. To make it all work, We need to collect 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. Privacy Shield mechanism, 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. 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 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