

ESET Endpoint Antivirus for macOS

User guide

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

Copyright ©2022 by ESET, spol. s r.o.

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

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

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

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

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

REV. 3/8/2022

| | |
|---|----|
| 1 ESET Endpoint Antivirus for macOS | 1 |
| 1.1 What's new in version 6 | 1 |
| 1.2 System requirements | 2 |
| 2 Introduction to ESET PROTECT | 2 |
| 3 Introduction to ESET PROTECT CLOUD | 4 |
| 4 Remote installation | 4 |
| 4.1 Create a remote installation package | 7 |
| 5 Local installation | 9 |
| 5.1 Typical installation | 11 |
| 5.2 Custom installation | 12 |
| 5.3 Enable system extensions locally | 14 |
| 5.4 Enable full disk access locally | 14 |
| 6 Product activation | 15 |
| 7 Uninstallation | 16 |
| 8 Basic overview | 16 |
| 8.1 Keyboard shortcuts | 17 |
| 8.2 Checking operation of the system | 17 |
| 8.3 What to do if the program does not work properly | 18 |
| 9 Computer protection | 18 |
| 9.1 Antivirus and antispyware protection | 19 |
| 9.1 General | 19 |
| 9.1 Exclusions | 19 |
| 9.1 Startup protection | 20 |
| 9.1 Real-time file system protection | 20 |
| 9.1 Advanced options | 21 |
| 9.1 When to modify the real-time protection configuration | 21 |
| 9.1 Checking real-time protection | 22 |
| 9.1 What to do if Real-time protection does not work | 22 |
| 9.1 On-demand computer scan | 23 |
| 9.1 Type of scan | 24 |
| 9.1 Smart scan | 24 |
| 9.1 Custom scan | 24 |
| 9.1 Scan targets | 24 |
| 9.1 Scan profiles | 25 |
| 9.1 ThreatSense engine parameters setup | 25 |
| 9.1 Objects | 26 |
| 9.1 Options | 27 |
| 9.1 Cleaning | 27 |
| 9.1 Exclusions | 28 |
| 9.1 Limits | 28 |
| 9.1 Others | 29 |
| 9.1 Infiltrations | 29 |
| 9.2 Web and email protection | 30 |
| 9.2 Web access protection | 31 |
| 9.2 Ports | 31 |
| 9.2 URL lists | 31 |

| | |
|--|----|
| 9.2 Email protection | 31 |
| 9.2 POP3 protocol checking | 32 |
| 9.2 IMAP protocol checking | 33 |
| 9.3 Anti-phishing | 33 |
| 10 Device control | 33 |
| 10.1 Rules editor | 34 |
| 11 Tools | 36 |
| 11.1 Log files | 36 |
| 11.1 Log maintenance | 37 |
| 11.1 Log filtering | 38 |
| 11.2 Scheduler | 38 |
| 11.2 Create new tasks | 39 |
| 11.2 Create a user-defined task | 41 |
| 11.3 Submit sample for analysis | 42 |
| 11.4 Quarantine | 42 |
| 11.4 Quarantine files | 42 |
| 11.4 Restore a quarantined file | 43 |
| 11.4 Submit a file from Quarantine | 43 |
| 11.5 Running processes | 43 |
| 11.6 Live Grid | 44 |
| 11.6 Suspicious files | 45 |
| 12 Privileges | 46 |
| 13 Presentation mode | 46 |
| 14 User interface | 47 |
| 14.1 Alerts and notifications | 47 |
| 14.1 Display alerts | 48 |
| 14.1 Protection statuses | 48 |
| 14.2 Context menu | 49 |
| 15 Update | 49 |
| 15.1 Update setup | 49 |
| 15.1 Advanced options | 51 |
| 15.2 How to create update tasks | 52 |
| 15.3 System updates | 52 |
| 15.4 Import and export settings | 53 |
| 15.5 Proxy server setup | 54 |
| 15.6 Shared Local Cache | 54 |
| 16 End User License Agreement | 55 |
| 17 Privacy Policy | 63 |

ESET Endpoint Antivirus for macOS

ESET Endpoint Antivirus for macOS 6 represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine 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 Antivirus 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 PROTECT (formerly ESET Security Management Center), 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 Antivirus 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 Antivirus for macOS version 6.9, ESET Endpoint Antivirus 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**
- **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 Antivirus 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 Antivirus for macOS, your system should meet the following hardware and software requirements:

| | System requirements: |
|------------------------|---|
| Processor architecture | Intel 64-bit, M1 |
| Operating system | macOS 10.12 and later macOS Server 10.12 and later |
| Memory | 300 MB |
| Free disk space | 200 MB |



In addition to existing Intel support, ESET Endpoint Antivirus for macOS version 6.10.900.0 and later support Apple M1 chip using Rosetta 2

Introduction to ESET PROTECT

ESET PROTECT allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location.

Using the ESET PROTECT Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or detections on remote computers. See also [ESET PROTECT architecture and infrastructure elements overview](#), [Getting started with ESET PROTECT Web Console](#), and [Supported Desktop Provisioning Environments](#).

ESET PROTECT is made up of the following components:

- [ESET PROTECT Server](#) - ESET PROTECT Server can be installed on Windows as well as Linux servers and also comes as a Virtual Appliance. It handles communication with Agents and collects and stores application data in the database.
- [ESET PROTECT Web Console](#) - ESET PROTECT Web Console is the primary interface that

allows you to manage client computers in your environment. It displays an overview of the status of clients on your network and allows you to deploy ESET solutions to unmanaged computers remotely. After you install ESET PROTECT Server, you can access the Web Console using your web browser. If you choose to make the web server available via the Internet, you can use ESET PROTECT from any place or device with an Internet connection.

- [ESET Management Agent](#) - The ESET Management Agent facilitates communication between the ESET PROTECT Server and client computers. The Agent must be installed on client computer to establish communication between that computer and the ESET PROTECT Server. Because it is located on the client computer and can store multiple security scenarios, use of the ESET Management Agent significantly lowers reaction time to new detections. Using ESET PROTECT Web Console, you can [deploy the ESET Management Agent](#) to unmanaged computers identified by Active Directory or ESET [RD Sensor](#). You can also [manually install the ESET Management Agent](#) on client computers if necessary.
- [Rogue Detection Sensor](#) - The ESET PROTECT Rogue Detection (RD) Sensor detects unmanaged computers present on your network and sends their information to the ESET PROTECT Server. This allows you to add new client computers to your secured network easily. The RD Sensor remembers computers that have been discovered and will not send the same information twice.
- [Apache HTTP Proxy](#) - Is a service that can be used in combination with ESET PROTECT to:
 - oDistribute updates to client computers and installation packages to the ESET Management Agent.
 - oForward communication from ESET Management Agents to the ESET PROTECT Server.
- [Mobile Device Connector](#) - Is a component that allows for Mobile Device Management with ESET PROTECT, permitting you to manage mobile devices (Android and iOS) and administer ESET Endpoint Security for Android.
- [ESET PROTECT Virtual Appliance](#) - The ESET PROTECT VA is intended for users who want to run ESET PROTECT in a virtualized environment.
- [ESET PROTECT Virtual Agent Host](#) - A component of the ESET PROTECT that virtualizes agent entities to allow for the management of agent-less virtual machines. This solution enables automation, dynamic group utilization and the same level of task management as ESET Management Agent on physical computers. The Virtual Agent collects information from virtual machines and sends it to the ESET PROTECT Server.
- [Mirror Tool](#) - The Mirror Tool is necessary for offline module updates. If your client computers do not have an internet connection, you can use the Mirror Tool to download update files from ESET update servers and store them locally.
- [ESET Remote Deployment Tool](#) - This tool serves to deploy All-in-one packages created in the ESET PROTECT Web Console. It is a convenient way to distribute ESET Management Agent with an ESET product on computers over a network.

- [ESET Business Account](#) - The new licensing portal for ESET business products allows you to manage licenses. See the [ESET Business Account](#) section of this document for instructions to activate your product, or see the ESET Business Account [User Guide](#) for more information about using the ESET Business Account. If you already have an ESET-issued Username and Password that you want to convert to a License Key, visit the [Convert legacy license credentials](#) section.
- [ESET Enterprise Inspector](#) - 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.

Using the ESET PROTECT Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

i For more information please see the [ESET PROTECT Online user guide](#).

Introduction to ESET PROTECT CLOUD

ESET PROTECT CLOUD enables you to manage ESET products on workstations and servers in a networked environment from one central location without the requirement to have a physical or virtual server like for ESET PROTECT or ESET Security Management Center. Using the (ESET PROTECT CLOUD Web Console), you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status, and quickly respond to problems or threats on remote computers.

- [Read more about this in the ESET PROTECT CLOUD Online user guide](#)

Remote installation

Before installation

- ▣ [macOS 10.15 and older](#)

Before installing ESET Endpoint Antivirus for macOS on macOS 10.13 and later, enable ESET kernel extensions. Also, on macOS 10.14 and later, enable full disk access on targeted computers. If these options are enabled after the installation, users will receive **System extensions blocked** and **Your computer is partially protected** notifications until ESET kernel extensions and full disk access is enabled.

To enable ESET kernel extensions and full disk access remotely, your computer must be enrolled with an [MDM \(Mobile Device Management\) server](#), such as Jamf.

Enable ESET system extensions

To remotely enable kernel extensions on your device, [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 appropriate 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 must be enrolled in the MDM server to deploy configuration profiles to those computers.

Enable full disk access

On macOS 10.14, you will receive the **Your computer is partially protected** notification from ESET Endpoint Antivirus for macOS after installation. To access all ESET Endpoint Antivirus for macOS functions and prevent the notification from appearing, you must enable **Full disk access** to ESET Endpoint Antivirus for macOS before installing the product. To enable **Full disk access** remotely:

o [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 must be enrolled in the MDM server to deploy configuration profiles to those computers.

After allowing full disk access and system extensions remotely, in **System Preferences > Security & Privacy**, these settings might appear disabled. If ESET Endpoint Antivirus for macOS does not display any warnings, full disk access and system extensions are allowed, regardless of their status in **System Preferences > Security & Privacy**.

☐ [macOS Big Sur \(11\) and newer](#)

Before installing ESET Endpoint Antivirus for macOS on macOS Big Sur, you must enable the following settings on targeted computers:

- oESET system extensions

If ESET system extensions are not enabled before the installation, users will receive **System extensions blocked** notifications until the ESET system extensions are enabled.

- oFull disk access

If full disk access is not enabled before the installation, users will receive **Your computer is partially protected** notifications until full disk access is enabled.

- oWeb access protection

For Web access protection to function, you must add the Web access protection configuration to system settings.

If the Web access protection configuration is missing after the ESET Endpoint Antivirus for macOS installation, users will receive "ESET Endpoint Antivirus for macOS" Would Like to Filter Network Content. When they receive this notification, click **Allow**. If they click **Don't Allow**, Web Access Protection will not work.

To remotely enable the above ESET settings, your computer must be enrolled with an [MDM \(Mobile Device Management\) server](#), such as Jamf.

Enable ESET system extensions

To enable system extensions on your device remotely, perform one of the following actions before the installation:

- oDownload the [.plist configuration profile](#). Deploy the `.plist` configuration profile file using your MDM service.
- oCreate your own configuration profile in your MDM, using the following settings:

| | |
|------------------------------|--|
| Team identifier (TeamID) | P8DQRXPVLP |
| Bundle identifier (BundleID) | com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices |

Enable full disk access

To enable full disk access remotely, perform one of the following actions before the installation:

- oDownload the [.plist configuration file](#). Deploy the `.plist` configuration profile file using your MDM service.
- oCreate your own configuration profile using the following settings:

| ESET Endpoint Antivirus | |
|--|---|
| Identifier | com.eset.eea.6 |
| Identifier Type | bundleID |
| Code Requirement | identifier "com.eset.eea.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| App or Service | SystemPolicyAllFiles |
| Access | Allow |
| ESET Endpoint Antivirus & ESET Endpoint Security | |
| Identifier | com.eset.devices |
| Identifier Type | bundleID |
| Code Requirement | identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| App or Service | SystemPolicyAllFiles |
| Access | Allow |
| ESET Endpoint Antivirus & ESET Endpoint Security | |
| Identifier | com.eset.endpoint |
| Identifier Type | bundleID |
| Code Requirement | identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| App or Service | SystemPolicyAllFiles |
| Access | Allow |

After allowing full disk access and system extensions remotely, in **System Preferences > Security & Privacy**, these settings might appear disabled. If ESET Endpoint Antivirus for macOS does not display any warnings, full disk access and system extensions are allowed, regardless of their status in **System Preferences > Security & Privacy**.

Web access protection

To add Web access protection configuration to system settings remotely, perform one of the following actions before the installation:

- oDownload the [.plist configuration file](#). Deploy the `.plist` configuration profile file using the MDM server. Your computer must be enrolled in the MDM server to deploy configuration profiles to those computers.
- oTo create your own configuration profile, create a VPN type configuration profile with the following settings:

| | |
|--|--|
| VPN type | VPN |
| Connection type | Custom SSL |
| Identifier Identifier for the custom SSL VPN | com.eset.sysext.manager |
| Server | localhost |
| Provider Bundle Identifier | com.eset.network |
| User authentication | Certificate |
| Provider Type | App-proxy |
| Provider Designated Requirement | identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| Enable VPN on Demand | ✓ |
| On Demand Rules Configuration XML | <array> <dict> <key>Action</key> <string>Connect</string> </dict> </array> |
| Idle Timer | Do not disconnect |
| Proxy Setup | Manual |
| Proxy Server And Port | localhost : 57856 |

Installation

Before installation, you can create a remote installation package with a preset ESET Endpoint Antivirus for macOS configuration that you can later deploy using the ESET PROTECT product or MDM of your choice.

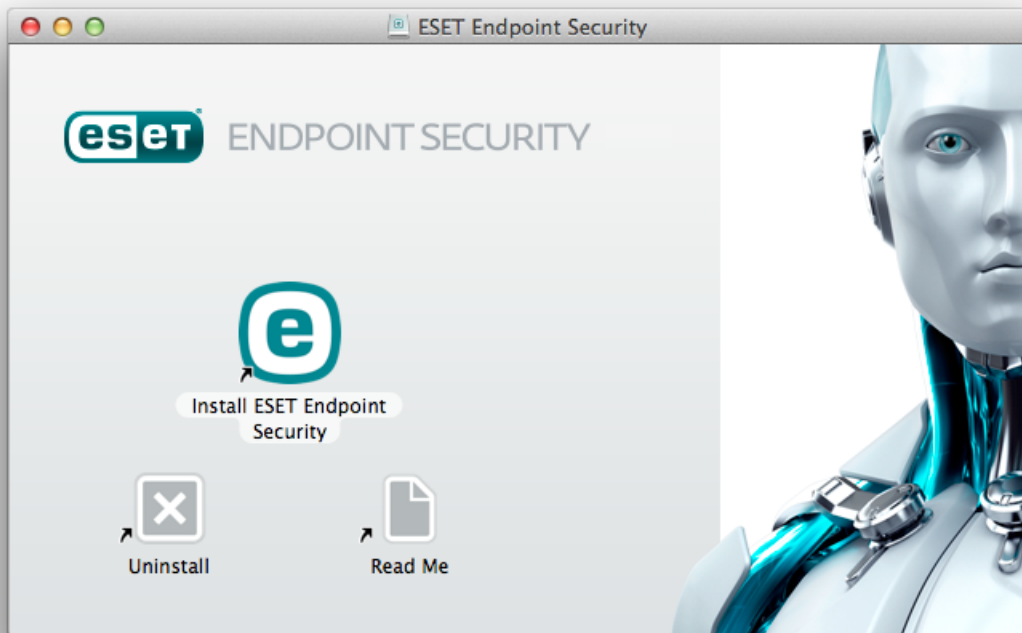
[Create a remote installation package](#). Install ESET Endpoint Antivirus for macOS remotely by creating a software install task using the ESET management system:

- oSoftware install task ESET PROTECT

Create a remote installation package

Create an installation package for Apple Remote Desktop installation

1. Download the standard installation package from the ESET website:
[ESET Endpoint Antivirus for macOS](#)
2. Launch the ESET Endpoint Antivirus for macOS installer and double-click the downloaded file.



3. Click **Install ESET Endpoint Antivirus for macOS**.
4. When prompted, click **Allow** to authorize the installer to determine if the software can be installed.
5. Click **Continue**. If you are creating a remote installation package, ESET Endpoint Antivirus for macOS will not be installed.
6. Review the system requirements and click **Continue**.
7. Read the ESET Software License Agreement and click **Continue** → **Agree** if you agree.
8. In the **Installation Mode** step, select **Remote**.

9. Choose which product components you want to install. All components are selected by default. Click **Continue**.

10. In the **Proxy Server** step, select the option that matches your internet connection. If you are unsure, use the default system settings. Click **Next**. If you are using a proxy server, in the next step you are prompted to enter the proxy address, your user name, and password.

11. Select who can modify the program configuration. Only privileged users and groups can change it. The Admin group is selected as privileged by default. Select the **Show all users** or **Show all groups** check box to display all virtual users and groups, such as programs and processes.

12. Enable ESET LiveGrid on the target computer, if applicable.

13. Enable potentially unwanted application detection on the target computer, if applicable.

14. Select a firewall mode:

Automatic mode – 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 enables 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 mode – This mode enables 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 is 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 create a new rule, all future connections of this type are allowed or blocked according to the rule.

15. Save the installation file on your computer. If you previously created an installation file in the default location, you must change the destination folder location or delete the previous files before you can continue. This finishes the first phase of remote installation. The local installer exits and creates remote installation files in the destination folder you chose.

Remote installation files are the following:

- *esets_setup.dat* - Setup data you entered in the Installer's Setup section
- *program_components.dat* - Setup information of selected program components. (This file is optional. It is created when you choose not to install certain ESET Endpoint Antivirus for macOS components.)
- *esets_remote_install.pkg* - Remote installation package

- `esets_remote_uninstall.sh` - Remote uninstall script

Install the Apple Remote Desktop

1. Open Apple Remote Desktop, and connect to the target computer. For more information, refer to [the Apple Remote Desktop documentation](#).
2. Copy the following files using **Copy file or folder** in Apple Remote Desktop to the `/tmp` folder on the target computer:

If you are installing all components, copy:

- `esets_setup.dat`

If you are not installing all product components, copy:

- `esets_setup.dat`
- `product_components.dat`

3. Use the **Install packages** command to install `esets_remote_install.pkg` to the target computer.

Remotely uninstall via Apple Remote Desktop

1. Open Apple Remote Desktop, and connect to the target computer. For more information, refer to [the Apple Remote Desktop documentation](#).
2. Copy the `esets_remote_uninstall.sh` script using **Copy file or folder** in the Apple Remote Desktop to the `/tmp` folder on the target computer.
3. In the Apple Remote Desktop, use the following **Send a UNIX shell command** to the target computer:

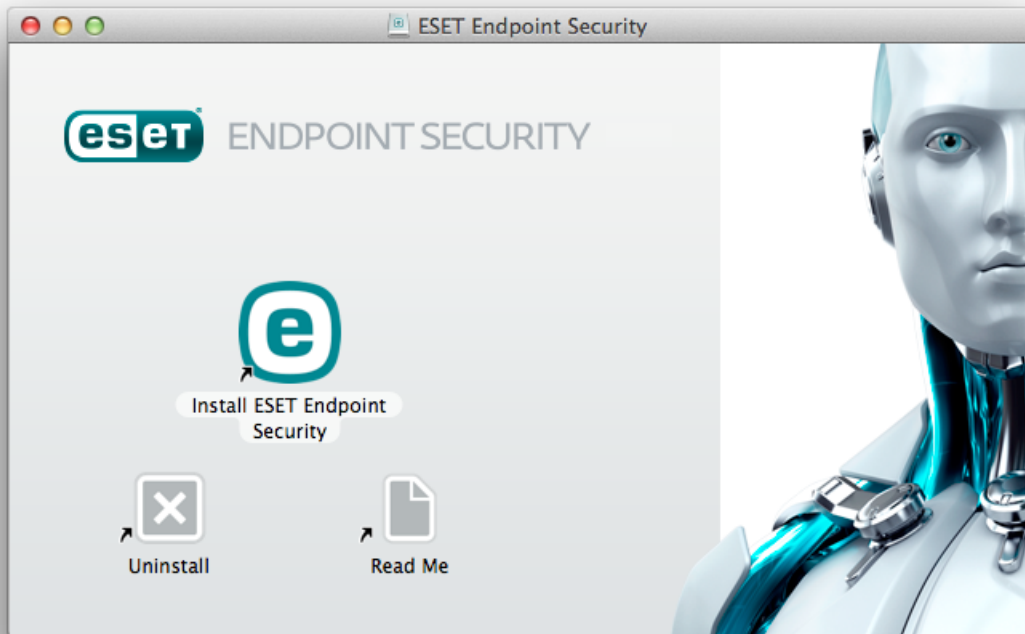
```
/tmp/esets_remote_uninstall.sh
```

After the uninstall process finishes, the console is displayed in the Apple Remote Desktop on the target computer.

Installation

The installation wizard guides you through the basic setup. For a detailed guide, see the [ESET installation Knowledgebase article](#).

1. To launch the ESET Endpoint Antivirus for macOS installer, double-click the downloaded file.



1. To begin the installation, click **Install ESET Endpoint Antivirus for macOS**.

Installing from the .pkg file

! During installation and the start-up of your ESET products for macOS, you must have internet access on your mac to allow Apple to verify ESET system extensions notarization.

2. When prompted, click **Allow** to authorize the installer to determine if the software can be installed.

3. Remove any existing security applications such as antivirus, antispyware, or firewall software from your computer if you have not done so already. Click **Continue** if no other security applications are installed.

4. Review the system requirements and click **Continue**.

5. Read the ESET Software License Agreement and click **Continue** → **Agree** if you agree.

6. Select the applicable installation type.

- [Typical installation](#)
- [Custom installation](#)
- [Remote installation](#)

Version upgrade

- i During the initial phase of installation, the installer automatically checks online for the latest product version. If a newer version is found, you have option to download the latest version before continuing the installation process.

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. To perform a typical installation:

1. In the **ESET LiveGrid** window, select your preferred option and click **Continue**. If you decide later that you would like to change this setting, you can do so using the **LiveGrid setup**. For more information about ESET Live Grid, [see the ESET Glossary](#).
2. In the **Potentially Unwanted Applications** window, select your preferred option (see [What is a potentially unwanted application?](#)) and click **Continue**. If you decide later that you would like to change this setting, use **Advanced setup**.
3. Click **Install**. If you are prompted for your macOS password, type it and click **Install Software**.

After the installation of ESET Endpoint Antivirus for macOS:

macOS Big Sur (11)

1. [Enable system extensions](#).
2. [Enable full disk access](#).
3. Allow ESET to add proxy configurations. You will receive the following notification: **"ESET Endpoint Antivirus for macOS" Would Like to Filter Network Content**. When you receive this notification, click **Allow**. If you click **Don't Allow**, Web Access Protection does not work.

macOS 10.15 and older

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 Antivirus for macOS. To access all ESET Endpoint Antivirus for macOS functions, you must allow kernel extensions on your device. To allow kernel extensions on your device, click **System Preferences > Security & Privacy** and then click **Allow** to allow system software from the developer **ESET, spol. s.r.o.** For more detailed information, refer to the ESET [Knowledgebase article](#).

2. On macOS 10.14 and later, you will receive the **Your computer is partially protected** notification from ESET Endpoint Antivirus for macOS. To access all ESET Endpoint Antivirus for macOS functions, you must enable full disk access to ESET Endpoint Antivirus for macOS. Click **Open System preferences > Security & Privacy**. Go to the **Privacy** tab and select **Full disk access**. Click the lock icon to enable editing. Click the plus icon and select the ESET Endpoint Antivirus 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 Antivirus for macOS notification window or restart your computer. For more detailed information, refer to the ESET [Knowledgebase article](#).

After the installation you are prompted to activate ESET Endpoint Antivirus for macOS. You can find multiple activation options in [the Activation chapter](#).

After installing ESET Endpoint Antivirus for macOS, 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. Following are settings you can modify:

- **Program Components**

ESET Endpoint Antivirus 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, select **I use a proxy server** to define its parameters. 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, type 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, you can use your current system settings by selecting **Use system settings (Recommended)**.

- **Privileges**

You can define privileged users or groups that can 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**

For more information about ESET Live Grid, [see the ESET Glossary](#).

- **Potentially Unwanted Applications**

For more information about potentially unwanted applications, [see the ESET Glossary](#).

After installing ESET Endpoint Antivirus for macOS:

macOS Big Sur (11)

1. [Allow system extensions](#).

2. [Enable Full disk access](#).

3. Allow ESET to add proxy configurations. You will receive the following notification: **"ESET Endpoint Antivirus for macOS" Would Like to Filter Network Content**. When you receive this notification, click **Allow**. If you click **Don't Allow**, Web Access Protection does not work.

macOS 10.15 and older

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 Antivirus for macOS. To access all ESET Endpoint Antivirus for macOS functions, you must allow kernel extensions on your device. To allow kernel extensions on your device, click **System Preferences > Security & Privacy** and then click **Allow** to allow system software from the developer **ESET, spol. s.r.o.** For more detailed information, see the ESET [Knowledgebase article](#).

2. On macOS 10.14 and later, you will receive a **Your computer is partially protected** notification from ESET Endpoint Antivirus for macOS. To access all ESET Endpoint Antivirus for macOS functions, you must enable full disk access to ESET Endpoint Antivirus for macOS. Click **Open System preferences > Security & Privacy**. Go to the **Privacy** tab and select **Full disk access**. Click the lock icon to enable editing. Click the plus icon and select the ESET Endpoint Antivirus for macOS application. Your computer displays a notification to restart your computer. Click **Later**. Do not restart your computer now. Click **Start Again** in the ESET Endpoint Antivirus for macOS notification window or restart your computer. For more detailed information, see the ESET [Knowledgebase article](#).

After the installation you are prompted to activate ESET Endpoint Antivirus for macOS. You can find multiple activation options in [the Activation chapter](#).


After installing ESET Endpoint Antivirus for macOS, 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.

Enable system extensions locally

In macOS 11 (Big Sur), kernel extensions were replaced by system extensions. These require user approval before loading new third-party system extensions.

After installing ESET Endpoint Antivirus for macOS on macOS Big Sur (11) and later, you receive the **System Extension Blocked** notification from your system and the **Your computer is not protected** notification from ESET Endpoint Antivirus for macOS. To access all ESET Endpoint Antivirus for macOS functions, you must enable system extensions on your device.

Upgrade from previous macOS to Big Sur.

 If you already installed ESET Endpoint Antivirus for macOS and you are going to upgrade to macOS Big Sur, you must enable the ESET kernel extensions manually after the upgrade. Physical access to the client machine is required. When you are accessing remotely, the **Allow** button is disabled.

When you are installing the ESET product on macOS Big Sur or later, you must enable the ESET system extensions manually. Physical access to the client machine is required. When you are accessing remotely, this option is disabled.

To enable system extensions manually:

1. Click **Open System preferences** or **Open Security Preferences** in one of the alert dialogs.
2. Click the lock icon at the bottom left to allow changes in the settings window.
3. Use your Touch ID or click **Use Password** and type your **User Name** and **Password**, and then click **Unlock**.
4. Click **Details**.
5. Select all three **ESET Endpoint Antivirus for macOS.app** options.
6. Click **OK**.

For a detailed step-by-step guide, see the [ESET Knowledgebase article](#). (Knowledgebase articles are not available in all languages.)

Enable full disk access locally

On macOS 10.14 you will receive a **Your computer is partially protected** notification from ESET Endpoint Antivirus for macOS. To access all ESET Endpoint Antivirus for macOS functions, you must enable full disk access to ESET Endpoint Antivirus for macOS:

1. Click **Open System preferences** in the alert dialog window.
2. Click the lock icon at the bottom left to allow changes in the settings window.
3. Use your Touch ID or click **Use Password** and type your **User Name** and **Password**, and then click **Unlock**.
4. Select **ESET Endpoint Antivirus for macOS.app** from the list.
5. A restart ESET Endpoint Antivirus for macOS notification is displayed. Click **Later**.
6. Select **ESET Real-time File System Protection** from the list.

ESET Real-time File System Protection not present

! If the **Real-time File System Protection** option is not in the list, you must [enable system extensions for your ESET product](#).

7. Click **Start Again** in the ESET Endpoint Antivirus for macOS alert dialog window or restart your computer. For more detailed information, see the ESET [Knowledgebase article](#).

Product activation

After the installation is complete, you are prompted to activate your product. You can use multiple activation methods. The availability of a particular activation method may vary depending on the country and the means of distribution (CD/DVD, ESET web page, and so on) for your product.

To activate your copy of ESET Endpoint Antivirus for macOS directly from the program, click the ESET Endpoint Antivirus for macOS icon (e) 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 Antivirus for macOS:

- **Activate with License Key** - A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX that identifies 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.
- **ESET Business Account** - An account created in the [ESET Business Account portal](#) with credentials (email address and password). This method allows you to manage multiple licenses from one location.
- **Offline license** - An automatically generated file that is 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.

Click **Activate later** to activate this client at a later time if your computer is a member of managed network and your administrator plans to use ESET PROTECT to activate your product.

Silent activation

i ESET PROTECT AND ESET PROTECT CLOUD can activate client computers silently using licenses made available by the administrator.

ESET Endpoint Antivirus for macOS version 6.3.85.0 (or later) provides you the option to activate the product using a 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 to activate ESET Endpoint Antivirus for macOS or is registered in [ESET Business Account](#). The command returns either the "OK" state or an error if the activation fails.

Uninstallation

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

- Open the ESET Endpoint Antivirus for macOS installation file (*.dmg*) and double-click **Uninstall**.
- Launch **Finder**, open the **Applications** folder on your hard drive, CTRL+click the **ESET Endpoint Antivirus for macOS** icon, and select **Show Package Contents**. Open the **Contents > Helpers** folder and double-click the **Uninstaller** icon.

Uninstallation

! During the uninstallation process, you must insert the administrator password multiple times to completely remove ESET Endpoint Antivirus for macOS.

Basic overview

The main program window of ESET Endpoint Antivirus 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, web and mail protection.
- **Computer scan** – Enables you to configure and launch an [on-demand computer scan](#).
- **Update** – Displays information about modules updates.
- **Setup** – Enables you to adjust your computer's security level.
- **Tools** – Provides access to the [log files](#), [scheduler](#), [quarantine](#), [running processes](#), and other program features.
- **Help** – Displays access to help files, the ESET Knowledgebase, a support request form, and additional program information.

Keyboard shortcuts

Following are keyboard shortcuts that can be used when working with ESET Endpoint Antivirus for macOS:

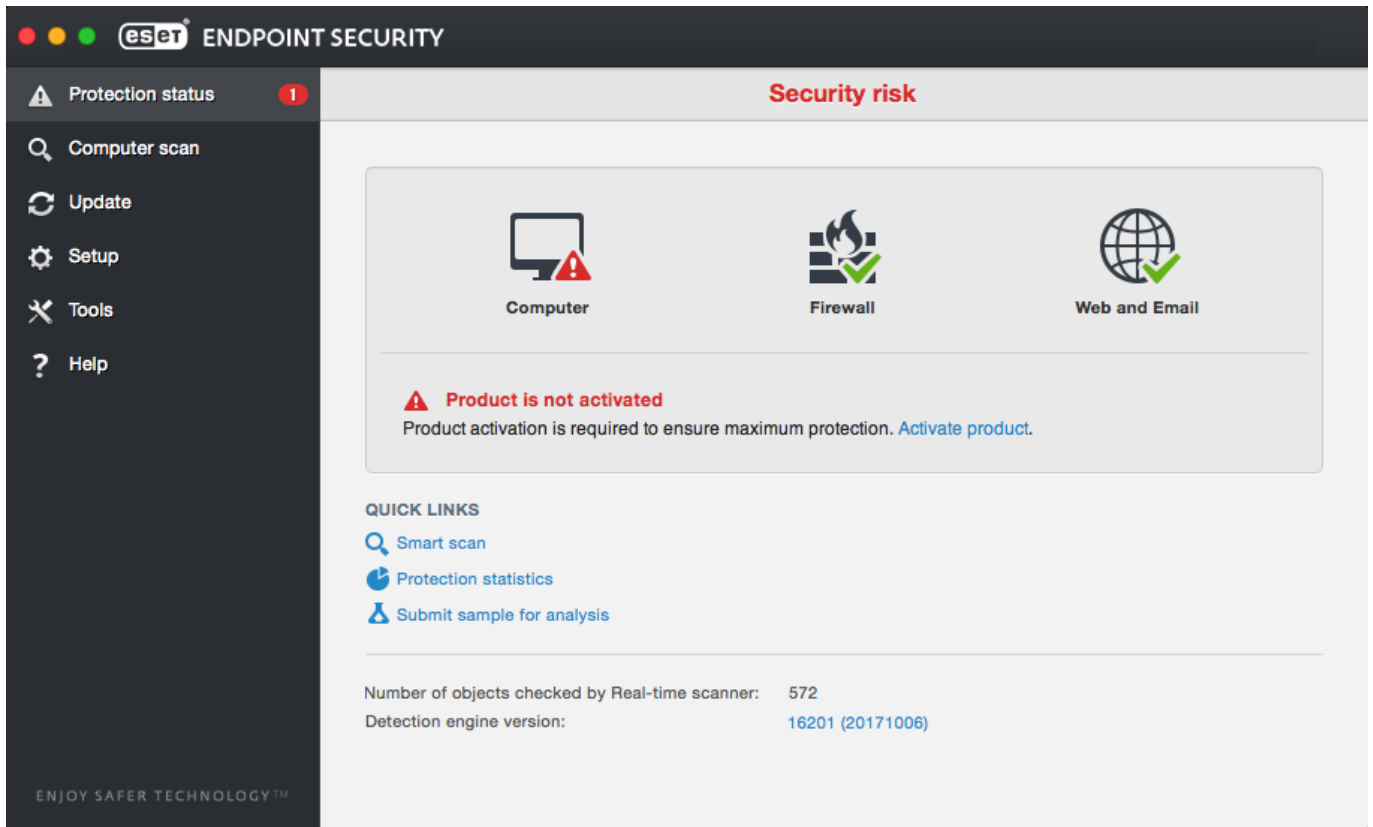
- *cmd+,* – Displays ESET Endpoint Antivirus for macOS preferences.
- *cmd+O* – Resizes the ESET Endpoint Antivirus for macOS main window to the default size and moves it to the center of the screen.
- *cmd+Q* – Hides the ESET Endpoint Antivirus for macOS main window. You can open it by clicking the ESET Endpoint Antivirus for macOS icon (Ⓜ) in the macOS menu bar (at the top of the screen).
- *cmd+W* – Closes the ESET Endpoint Antivirus for macOS main 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 Antivirus for macOS modules is 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 to fix 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 cannot solve a problem using the suggested solutions, you can search the [ESET Knowledgebase](#) for a solution or contact [ESET Customer Care](#). Customer Care responds quickly to your questions and helps resolve any issues with ESET Endpoint Antivirus for macOS.

Computer protection

Computer configuration can be found under **Setup > Computer**. This window 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 the quarantine.

General

In the **General** section (**Setup > Enter application preferences... > General**), you can enable the 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, the 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 can also 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 on the **File System** tab are excluded from all scanners: startup, real-time, and on-demand (computer scan) The following is on this tab:

- **Path** - The 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 is detected by the antivirus module.
-  – Creates a new exclusion. Type 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** – Rolls back exclusions to the last saved state.

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

Startup protection

A startup file check automatically scans files at system startup. By default, this scan runs regularly as a scheduled task after a user logon or a successful module 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. ESET recommends 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), you can end real-time protection by clicking the ESET Endpoint Antivirus for macOS icon (🛡️) located in your menu bar (at the top of the screen) and selecting **Disable Real-time File System Protection**. You can also disable real-time file system protection from the main program window (click **Setup** > **Computer** and switch **Real-time file system protection** to **DISABLED**).

You can exclude the following types of media from the Real-time scanner:

- **Local drives** – system hard drives
- **Removable media** – CDs, DVDs, USB media, Bluetooth devices, and so on
- **Network media** – all mapped drives

ESET recommends 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, click **Setup > Enter application preferences ...** (or press *cmd+,*) > **Real-Time Protection** and then 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](#).

ESET does not recommend changing the **Default archives settings** section unless you must resolve a specific issue, because higher archive nesting values can impede system performance.

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

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

When to modify the 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. ESET recommends 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 Antivirus for macOS, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click **Default** which is located at the bottom left of the **Real-Time Protection** window (**Setup > Enter application preferences ... > Real-Time Protection**).

Check 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 the Terminal utility and issue the following command:

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

The status of the real-time scanner is displayed as `RTPStatus=Enabled` or `RTPStatus=Disabled`.

The output of the Terminal bash includes the following statuses:

- Version of ESET Endpoint Antivirus for macOS installed on the client computer
- Date and version of the detection engine
- Path to the update server

Terminal usage

The 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 must 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

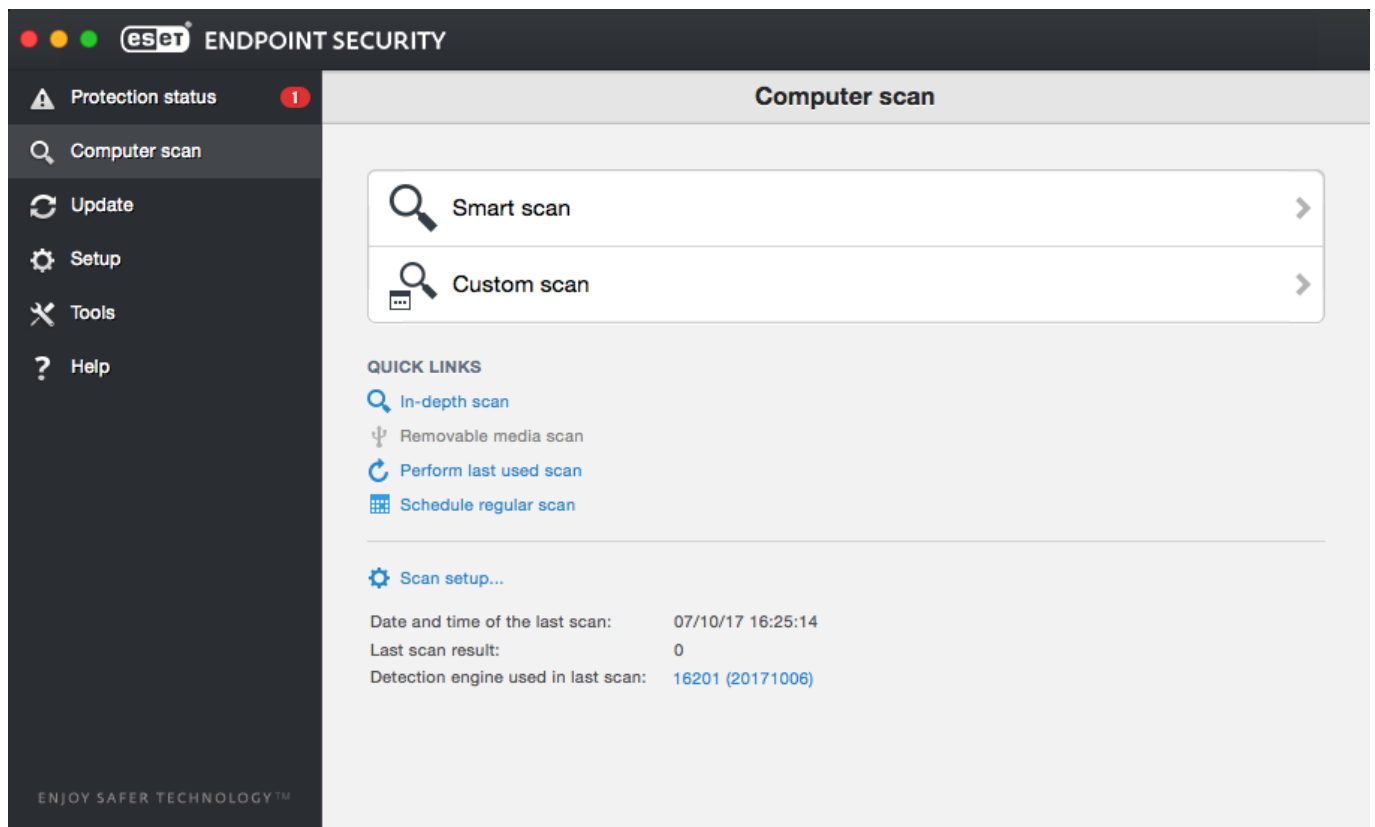
Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. ESET recommends that you remove any other antivirus programs that may be on your system.

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, run computer scans 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.



ESET recommends that you run an on-demand computer scan at least once a month. You can configure scanning 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 Antivirus for macOS main screen, Dock icon, Menu Bar icon (Ⓜ at the 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** enables you to select any of the predefined scan profiles and 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 cleaning types, 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. You can save different configurations as user-defined scan profiles, which can be useful when scanning repeatedly using the same parameters.

To select scan targets, click **Computer scan > Custom scan** and select specific **Scan Targets** from the tree structure. You can also more precisely define a scan target by entering the path to the folder or files you want to include. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. In addition, you can choose from three cleaning levels by clicking **Setup... > Cleaning**.

Custom scan

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

Scan targets

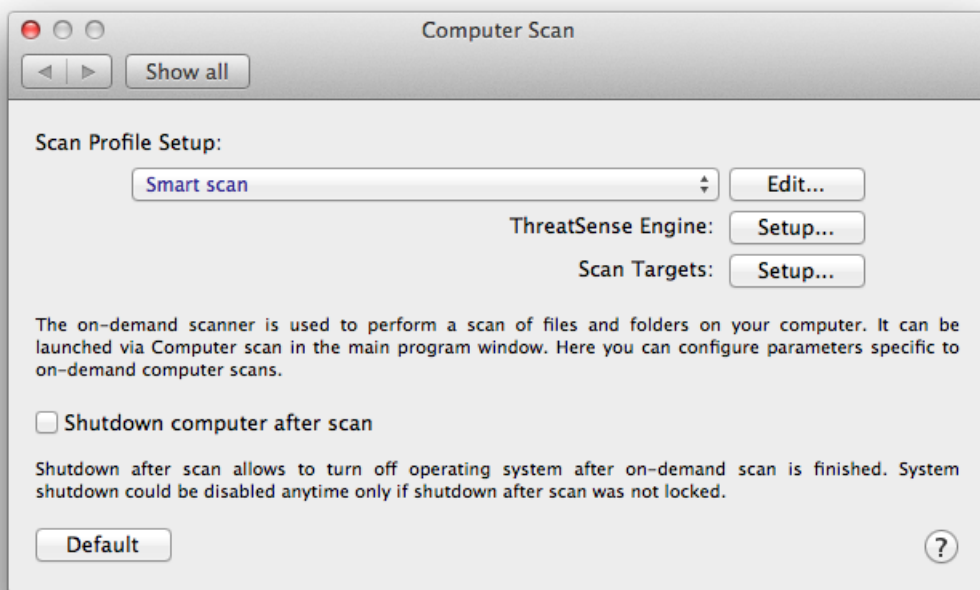
The **Scan targets** tree structure enables you to select files and folders to be scanned for viruses. You may also select folders according to a profile's settings.

You can more precisely define a scan target by entering the path to the folder or files 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

You can save your preferred scan settings for future scanning. ESET recommends 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. However, you do not want to scan runtime packers or potentially unsafe applications, and you also want to apply **Strict cleaning**. On 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. This technology uses a combination of several methods (code analysis, code emulation, generic signatures, and so on) that work together to significantly enhance system security. The scanning engine can control several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully prevents rootkits.

The ThreatSense technology setup options enable you to specify several scan parameters:

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

To display 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. 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, ESET recommends that the default ThreatSense parameters stay unchanged for all modules except **Computer scan**.

Objects

The **Objects** section enables you to define which files are scanned for infiltrations. The following are in the **Objects** section:

- **Symbolic links** – Scans files that contain a text string that is interpreted as a path to a file or directory (computer scan only).
- **Email files** – Scans email files (this is not available in real-time protection).
- **Mailboxes** – Scans user mailboxes in the system. Incorrect use of this option may result in a conflict with your email client (this is not available in real-time protection). To

learn more about advantages and disadvantages of this option, read the following [knowledgebase article](#).

- **Archives** – Scans files compressed in archives (.rar, .zip, .arj, .tar, and so on) (this is not available in real-time protection).
- **Self-extracting archives** – Scans files contained in self-extracting archive files (this is not available in real-time protection).
- **Runtime packers** – Scans standard static packers (for example, UPX, yoda, ASPack, and FGS). Note that unlike standard archive types, runtime packers decompress in memory.

Options

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


- **Heuristics** – Analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software that did not previously exist.
- **Advanced heuristics** – Detects computer worms and trojans written in high-level programming languages. The program's detection ability is significantly higher as a result of advanced heuristics.

Cleaning

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

- **No cleaning** – Infected files are not cleaned automatically. The program displays a warning window and allows you to choose an action.
- **Standard cleaning** – The program attempts to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program offers a choice of follow-up actions. The choice of follow-up actions is also displayed if a predefined action cannot be completed.
- **Strict cleaning** – The program cleans or deletes all infected files (including archives). The only exceptions are system files. If it is not possible to clean a file, you receive a notification and are 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, the archive is not deleted. If an infected archive file is detected in **Strict cleaning** mode, the entire archive is 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 enables you define the types of files to be excluded from scanning.

By default, all files are scanned regardless of their extension. You can add any extension 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 enables 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 only scans objects smaller than the specified size. ESET does 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 stops scanning an object when that time has elapsed, regardless of whether the scan has finished.
- **Maximum Nesting Level:** Specifies the maximum depth of archive scanning. ESET does 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 remains unchecked.

- **Maximum File Size:** Enables 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 remains.

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, using different scanning methods. Smart Optimization is not rigidly defined within the product. ESET is continuously implementing new changes that are integrated into ESET Endpoint Antivirus 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 alternate data stream (On-demand scanner only)

Alternate data streams (resource/data forks) used by the file system are file and folder associations that are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Infiltrations

Infiltrations can reach the system from various entry points: web pages, shared folders, email, or removable computer devices (USBs, external disks, CDs, DVDs, and so on).

If your computer shows signs of malware infection, for example it runs slower, often freezes, and so on, ESET recommends doing the following:

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 Antivirus for macOS, suppose that an infiltration is detected by the real-time file system monitor using the default cleaning level. Real-time protection attempts to clean or delete the file. If no predefined action is available for the real-time protection module, you are 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 infected files are left in their 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 is attacked by a virus that has attached malicious code to it. If this is the case, first try to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it is deleted.


Deleting files in archives

In the default cleaning mode, the entire archive is 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 is 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 Antivirus for macOS does not scan the 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 access protection

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

Web filtering can be achieved by defining [the port numbers for HTTP communication](#) or [URL addresses](#).

Ports

On the **Ports** tab you can define the port numbers used for HTTP communication. By default, 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. Web sites in the list of blocked addresses are not accessible. Web sites 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**.

You can use the special symbols * (asterisk) and ? (question mark) when building URL lists. The asterisk substitutes any character string, and the question mark substitutes any symbol. You should take particular care when specifying excluded addresses because the list should only contain trusted and safe addresses. Similarly, you must 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 Antivirus for macOS uses the advanced scanning methods included in the ThreatSense scanning engine. Scanning of the POP3 and IMAP protocol communications occur when any email client used. The following settings are available:

- **ThreatSense Engine: Setup** – Advanced virus scanner setup enables you to configure scan targets, detection methods, and so on. Click **Setup** to display the detailed scanner setup window.
- **Append tag message to email footnote** – After an email is scanned, a notification containing the scan results can be appended to the message. Tag messages cannot be

relied on exclusively because the tags may be omitted in problematic HTML messages and can be forged by some viruses. The following options are available:

oNever - No tag messages is added.

oTo infected email only - Only messages containing malicious software are tagged as checked.

oTo all scanned email - ESET Endpoint Antivirus for macOS appends 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. This feature 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. Following are available template fields you can use and their meanings:

o%avstatus% - Adds the email infection status (for example: clean, infected, and so on).

o%virus% - Adds the name of the threat.

o%product% - Adds the name of your ESET product (in this case - ESET Endpoint Antivirus for macOS).

o%product_url% - Adds the ESET web site link (www.eset.com).

In the lower section of this window, you can also enable or 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 Antivirus for macOS provides protection for this protocol, regardless of the email client.

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 you can add

other communication ports if necessary. Port numbers must be delimited by a comma.

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

IMAP protocol checking

The Internet Message Access Protocol (IMAP) is another Internet protocol for email 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 a message has been read, replied to, or deleted. ESET Endpoint Antivirus for macOS provides protection for this protocol, regardless of the email client.

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 you can add other communication ports if necessary. Port numbers must be delimited by a comma.

If you select **Enable IMAP protocol checking**, 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.

ESET recommends that you keep Anti-Phishing enabled (**Setup > Enter application preferences ... > Anti-Phishing Protection**). All potential phishing attacks coming from dangerous web sites or domains are blocked, and a warning notification is displayed informing you of the attack.

Device control

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

Device control on macOS 11 and later

- ⚠ ESET Endpoint Antivirus for macOS installed on macOS 11 and later scans only memory devices (such as USB drives, CD/DVD, and so on).

Supported external devices on macOS 10.15 and older include:

- 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, access to the device is not granted.

The Device Control Log records all incidents that trigger device control. You can view log entries from the main program window of ESET Endpoint Antivirus for macOS in **Tools** > [Log files](#).

Rules editor

You can modify device control setup options in **Setup** > **Enter application preferences...** > **Device Control**.

Clicking **Enable device control** activates the Device Control feature in ESET Endpoint Antivirus 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 or disable the rule.

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

ESET Endpoint Antivirus for macOS automatically detects all currently inserted devices and their parameters (device type, vendor, model, and serial number). Instead of creating rules manually, click **Populate**, 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 the name, device type, logging severity, and action to perform after connecting a device to your computer. Following are descriptions of the rules you can specify:

Name - Type a description of the rule into the **Name** field for better identification. The **Rule enabled** check box disables or enables this rule. Using this check box 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 a 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 enable you to select one of the following permission settings:

- **Read/Write** - Full access to the device is allowed.
- **Read Only** - Only read access to the device is allowed.
- **Block** - Access to the device is blocked.

Criteria type - Select **Device group** or **Device**. You can use additional parameters shown below to fine-tune rules and tailor them to devices:

- **Vendor** - Vendor name or ID
- **Model** - Name of the device
- **Serial** - Serial number of the device (For a CD/DVD device, this is the serial number of the given media, not the CD/DVD drive)

No parameters defined

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

TIP

i 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 are 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 are recorded.

User list - You can limit rules 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 the username from the **Selected Users** list and click **Remove**. To display all system users, select **Show all users**. If the list is empty, all users are 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).

Tools

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

This menu includes the following tools:

- [Log files](#)
- **Protection statistics**. This tool displays statistics from multiple types of protection. Click the drop-down menu to select from the following protection statistics:
 - **Antivirus protection summary** (this is selected by default)
 - **On-demand scan graph**
 - **Real-time protection graph**
 - **Email client protection graph**
 - **Web access protection graph**

The Antivirus protection summary shows statistics from the last active scan. Other protection types statistics are shown from the last computer restart (or restart of ESET Endpoint Antivirus for macOS). You can clear the statistic manually by clicking **Reset** under the statistic.

- [Scheduler](#)
- [Running processes](#)
- [Quarantine](#)
- [Submit sample for analysis](#)

Log files

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

Log files are accessible from the ESET Endpoint Antivirus 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:

- **Detected threats** – Provides information about events related to the detection of infiltrations.
- **Events** – All important actions performed by ESET Endpoint Antivirus for macOS are recorded in the Event logs.
- **Computer scan** – Displays results of all completed scans. Double-click any entry to view the details of a specific computer scan.
- **Device control** – Contains records of removable media or devices that were connected to the computer. Only devices with a device control rule are recorded to the log file. If the rule does not match a connected device, a log entry for a connected device is not created. Here you can also see details such as the device type, serial number, vendor name, and media size (if available).
- **Filtered websites** – Lists web sites that were blocked by [Web access protection](#). In these logs you can see the time, URL, status, IP address, user, and application that opened a connection to the particular web site.

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 Antivirus 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** – Automatic defragmentation of log files occurs if the specified percentage of unused records is exceeded.

You can store all the relevant information displayed in the user interface, threat, and event messages in human-readable text formats such as plain text or CSV (comma-separated values) format. 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 are 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:

- Events such as *Invalid username and password*, *Modules can not be updated*, and so on are written to the `eventslog.txt` file.
- Threats detected by the Startup scanner, Real-Time Protection, or Computer Scan are stored in the `threatslog.txt` file.
- The results of all completed scans are saved in the format `scanlog.NUMBER.txt`.
- Devices blocked by Device Control are mentioned in `devctllog.txt`.

To configure the filters for **Default Computer Scan Log Records**, click **Edit** and select or deselect log types as required. You can find further explanation of these log types in [Log Filtering](#).

Log filtering

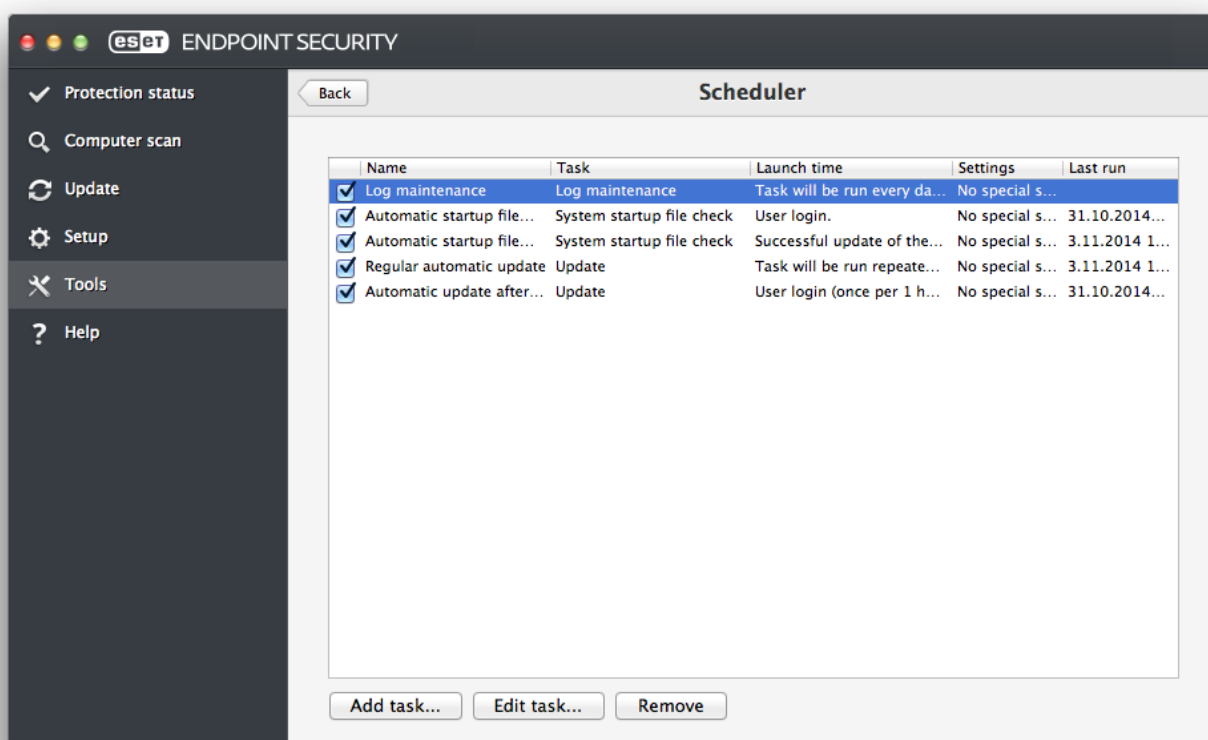
Logs store information about important system events. The log filtering feature enables you to display records about specific events.

The most frequently used log types are:

- **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, and so on
- **Diagnostic records** - Information needed to fine-tune the program and all records described above

Scheduler

The **Scheduler** is in the ESET Endpoint Antivirus 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.



The Scheduler manages and launches scheduled tasks with predefined configurations and properties. The configuration and properties contain information such as the date, time, and specified profiles to be used while executing the task.

By default, the Scheduler displays the following scheduled tasks:

- Log maintenance (after enabling **Show system tasks** in scheduler setup)
- Startup file check after a user logon
- Startup file check after a successful update of detection modules
- Regular automatic update
- Automatic update after a user logon

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

Create new tasks

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

Sandboxed application on macOS Big Sur (11)

ESET Endpoint Antivirus for macOS on macOS Big Sur (11) cannot run scheduled tasks for sandboxed applications. For example, all applications downloaded from the Apple store are sandboxed. You can find more information about the Sandbox [in the Apple documentation](#).

The Scheduler can still create tasks for ESET applications and other non-sandbox applications.

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

User defined tasks

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

Example: Run task as user

This example explains how to schedule the calculator application to start at a selected time as a user named **UserOne**:

1. In the **Scheduler**, select **Add task**.
2. Type the task name. Select **Run application** as a **Scheduled task**. On the **Run Task** window, select **Once** to run this task one time. Click **Next**.
- ✓ 3. Click **Browse** and select the Calculator application.
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 cannot run and click **Next**.
7. Click **Finish**. The ESET Scheduler starts the Calculator application at the time you selected.

Username limitations

! You cannot use spaces or blank characters in front of a username. Also, you cannot use spaces in a username. Use a blank character instead.

Scanning as a directory owner

You can scan directories as the owner of the directory:

```
i 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

This example explains how to create an update task to 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 are prompted to specify different update parameters. If you select **User-defined**, you are prompted to specify the date and time in cron format (see the [Creating a user-defined task](#) section for more details).
4. Select an alternate option if the task cannot be performed or completed at the scheduled time.
5. Click **Finish**. The new scheduled task is added to the list of currently scheduled tasks.

By default, ESET Endpoint Antivirus for macOS contains predefined 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**.

Create user-defined task

A few special parameters 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 must 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 (*) – Matches any character. For example, an asterisk in the third field (day of month) means every day.
- hyphen (-) – Defines ranges, for example, 3-9.
- comma (,) – Separates items of a list, for example, 1,3,7,8.
- slash (/) – Defines increments of ranges, for example, 3-28/5 in the third field (day of month) means the third day of the month and then every 5 days.

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

User defined tasks

- i If you define a day of the month and a day of the week, the command only executes when both fields match.

Submit sample for analysis

The sample submission dialog enables you to send a file or site to ESET for analysis. If you find a suspiciously behaving file on your computer or suspicious site on the internet, submit it to the ESET Virus Lab for analysis. If the file is a malicious application, the detection is added to an upcoming product update.

In the **Comment** section, enclose as much information about the file as possible (for example, the web site you downloaded it from). The sample you submit must meet at least one of the following criteria:

- The sample is not detected by your ESET product.
- The sample is incorrectly detected as a threat.

ESET does not accept your personal files (that you would like to scan for malware by ESET) as samples. The ESET Research Lab does not perform on-demand scans for users.

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 Antivirus for macOS.

You can quarantine any file. This practice is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. You can submit quarantined files to the ESET Threat Lab for analysis.

You can view files stored in the quarantine folder in a table displaying the date and time of the quarantine, the path to the original location of the infected file, the file size in bytes, the reason the file was quarantined (for example, the file was added by a 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 Antivirus for macOS. Quarantined files are stored in a safe encrypted form and can be restored again after installing ESET Endpoint Antivirus for macOS.

Quarantine files

ESET Endpoint Antivirus 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 Antivirus for macOS - Add files to Quarantine** from the context menu to send a file to the quarantine.

Restore from the Quarantine

You can restore quarantined files to their original location by selecting a quarantined file and clicking **Restore**. This option 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.

Submit a file from the Quarantine

If you 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, send the file to the ESET Threat Lab. To submit a file from the quarantine, CTRL+click the file and select **Submit file for analysis** from the context menu.

Running processes

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

- **Process** – The 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 Antivirus for macOS and ESET Live Grid technology assign risk levels to objects (files, processes, and so on) 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 are excluded from scanning. This improves the speed of 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 is a malicious application, its signature is added to an upcoming product update.
- **Number of Users** – The number of users who use a given application. This information is gathered by ESET Live Grid technology.
- **Time of discovery** – The period of time since the application was discovered by ESET Live Grid technology.
- **Application Bundle ID** – The name of the vendor or application process.

Click a given process to display the following information at the bottom of the window:

- **File** - The location of an application on your computer
- **File Size** - The physical size of the file on the disk
- **File Description** - File characteristics based on the description from the operating system
- **Application Bundle ID** - The name of the vendor or application process
- **File Version** - Information from the application publisher
- **Product name** - The application name and/or business name

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 one purpose - to improve the protection that ESET can offer you. The best way to ensure that ESET sees 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:

- 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 Antivirus for macOS may respond faster to new threats than a detection modules update.
- You can configure the Live Grid Early Warning System to submit anonymous information about new threats and where new threatening code is contained. You can send this information to ESET for detailed analysis. Studying these threats helps ESET update the ESET detection modules and improve the ESET threat detection ability.

The Live Grid Early Warning System collects 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, for example) to the ESET Threat Lab, this information is not be used for ANY purpose other than to help ESET 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 Antivirus for macOS is configured to submit suspicious files to the ESET Threat Lab for detailed analysis. If you do not want 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 the ESET Threat Lab for analysis by clicking **Tools > Submit file for analysis** from the main program window. If the file is a malicious application, its detection is added to an upcoming product update.

Following are options you can specify:

- **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 of the detection, 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, you may find it 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, and so on). You can add file types to the list of excluded files.
- **Contact Email (optional)** – Your email address is used if further information is required for analysis. Note that you will not receive a response from ESET unless more information is needed.

Privileges

ESET Endpoint Antivirus 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 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 specify a list of privileged users, select them from the **Users** list on the left side and click **Add**. To remove a user, select the username from the **Privileged Users** list on the right side and click **Remove**. To display all system users, select **Show all users**.

Empty privileged user list

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

Presentation mode

Presentation mode is a feature for users who 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 this mode is 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** to trigger Presentation mode automatically when applications are run in full-screen mode. When this feature is enabled, Presentation mode starts whenever you initiate a full-screen application and automatically stops 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 is automatically disabled.


Enabling Presentation mode is a potential security risk, so the ESET Endpoint Antivirus for macOS protection status icon turns orange and displays a warning.


User interface

The user interface configuration options enables 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 Antivirus for macOS splash screen at the system startup, select **Show splash-screen at startup**.

The following options are available:

- **Present application in Dock** enables you to display the ESET Endpoint Antivirus for macOS icon () in the macOS Dock and switch between ESET Endpoint Antivirus for macOS and other running applications by pressing *cmd+tab*. Changes take effect after you restart ESET Endpoint Antivirus for macOS (this is usually triggered by a computer restart).
- **Use standard menu** enables you to use certain keyboard shortcuts (see [Keyboard shortcuts](#)) and see standard menu items (User interface, Setup, and Tools) on the macOS Menu Bar (at the top of the screen).
- **Show tooltips** enables you to display tooltips when the cursor is placed over certain options in ESET Endpoint Antivirus for macOS.
- **Show hidden files** enables you to see and select hidden files in **Scan Targets** setup for a **Computer scan**.

By default, the ESET Endpoint Antivirus for macOS icon () is displayed in the Menu Bar Extras that appear at the right of the macOS Menu Bar (at the top of the screen). To disable this icon, deselect the **Show icon in menu bar extras** option. This change takes effect after you restart ESET Endpoint Antivirus for macOS (this is usually triggered by a computer restart).

Alerts and notifications

The **Alerts and notifications** section enables you to configure how threat alerts, protection statuses, and system notifications are handled by ESET Endpoint Antivirus for macOS.

Disabling **Display alerts** disables all alert windows and is only recommended in specific situations. For most users, ESET recommends leaving this option enabled (the default setting). Advanced options are described [in this chapter](#).

Selecting **Display notifications on desktop** causes 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 is displayed by adjusting the **Close notifications automatically after X seconds** value (this value is 5 seconds by default).

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

Display alerts

ESET Endpoint Antivirus 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, and so on. 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 Antivirus 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 is always displayed and **Display Conditions** do not apply. If you do not want to receive a notification about a certain event in the list, deselect this option and, additionally, you can define **Display Conditions** under which certain actions are not performed.

Protection statuses

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

You can hide protection status of the following program features:

- Anti-Phishing
- Web access protection
- Email client protection
- Presentation mode
- Operating system update
- License expiration
- Computer restart required

Context menu

To make ESET Endpoint Antivirus 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 take effect after you log out or restart your computer. Context menu options are available on the desktop and in the **Finder** window when you CTRL+click on any file or folder.

Update

Regularly updating ESET Endpoint Antivirus 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.

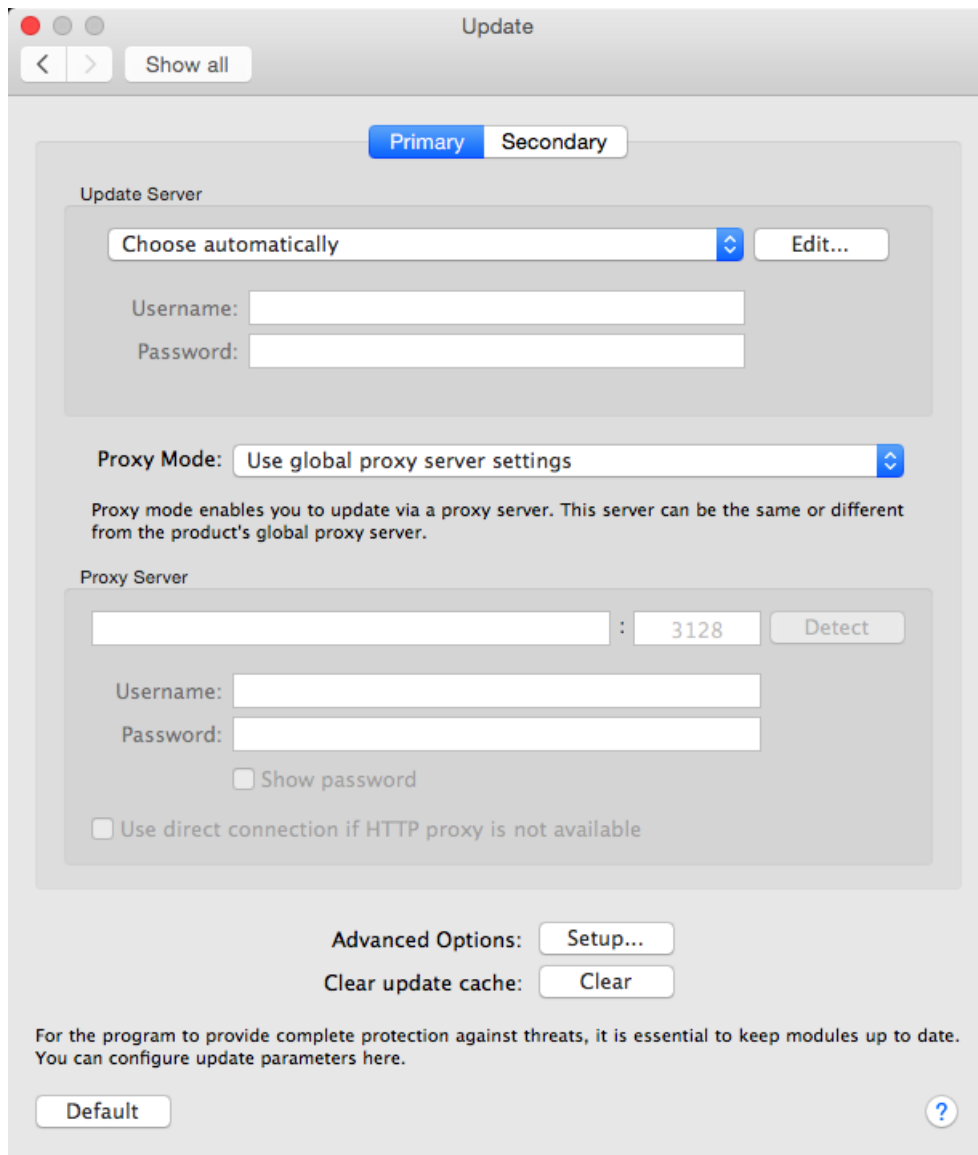
Click **Update** from the main menu to view your current update status including the date and time of the last successful update and verify if an update is needed. To begin the update process manually, click **Update modules**.

Under normal circumstances, when updates are downloaded properly, the message "Update is not necessary - the installed modules are current" is displayed in the Update window if you have the latest modules. If modules cannot be updated, ESET recommends 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 web site 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 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**, type the address of the new server in the **Update Server** input field, and click **Add**.

ESET Endpoint Antivirus for macOS enables 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, the second server is not used. If you do not specify a secondary update server, username, and password, the failover update functionality does not work. You can also select **Choose automatically** and type your username and password in the appropriate fields to have ESET Endpoint Antivirus 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 as 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 Antivirus for macOS fill out the IP address and port number (**3128** by default).
3. Type a valid **Username** and **Password** into the respective fields if communication with the proxy server requires authentication.

ESET Endpoint Antivirus for macOS detects the proxy settings from macOS system preferences. You can configure these settings in macOS under  > **System Preferences** > **Network** > **Advanced** > **Proxies**.

If you enable **Use direct connection if HTTP proxy is not available**, ESET Endpoint Antivirus for macOS automatically tries to connect to the update servers without using a proxy. This option is recommended for mobile users with MacBooks.

If you experience difficulty when trying to download detection module 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 update a few hours after they are released to ensure that your clients do not receive updates until they are confirmed to be free of any issues.

ESET Endpoint Antivirus 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 Antivirus for macOS record these snapshots automatically. If you suspect that a new detection module 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 do not resume until you restore them manually. Use caution when setting the time period to suspend updates.

The **Set maximum detection engine age automatically** setting enables you to set the maximum time (in days) after which detection modules are 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 module update.

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

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

You can modify each update task 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 Antivirus 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 Antivirus 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:

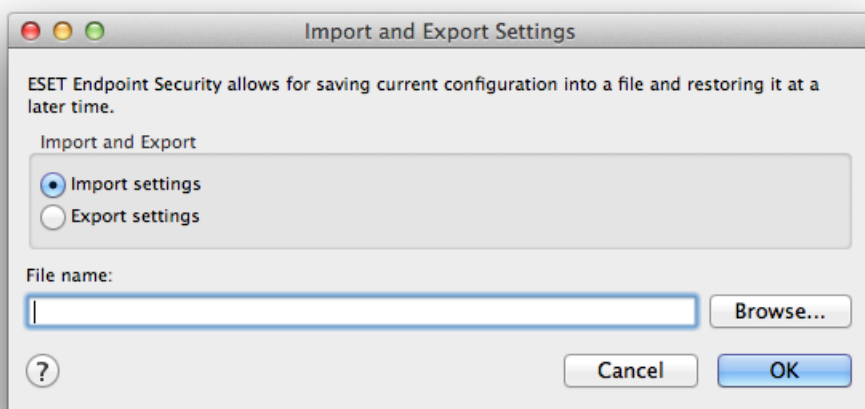
- **[recommended]** - the operating system manufacturer recommends that you install this update to increase the security and stability of the system
- **[restart]** - a computer restart is required on following installation
- **[shutdown]** - the computer must be shut down and then powered back on following 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 Antivirus 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 Antivirus 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 Antivirus 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 Antivirus for macOS functions. Parameters defined here are used by all modules that require an internet connection. ESET Endpoint Antivirus for macOS supports Basic Access and NTLM (NT LAN Manager) authentication.

To specify proxy settings for this level, select **Use proxy server** and type 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 both fields.

If communication with the proxy server requires authentication, type 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**. This feature boosts performance in virtual environments by eliminating duplicate scanning in the network. This ensures that each file is scanned only once and stored in the shared cache. When this feature is enabled, information about scans of files and folders in your network is saved to the local cache. If you perform a new scan, ESET Endpoint Antivirus for macOS searches for scanned files in the cache. If files match, they are excluded from scanning.

Shared Local Cache settings contain the following:

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

Detailed instructions

i For detailed instructions on how to install and configure the ESET Shared Local Cache, refer to the [ESET Shared Local Cache user guide](#). (This 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, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (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 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 ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

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

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

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

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

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

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

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

20. **Notices.** All notices and return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 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.

Privacy Policy

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

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

Processing of Personal Data

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

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

oinfiltrations 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;

oinformation about devices in local network such as type, vendor, model and/or name of device;

oinformation concerning the use of internet such as IP address and geographic information, IP packets, URLs and ethernet frames;

ocrash dump files and information contained.

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

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

Data Confidentiality

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

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

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

Data Subject's Rights

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

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

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

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