



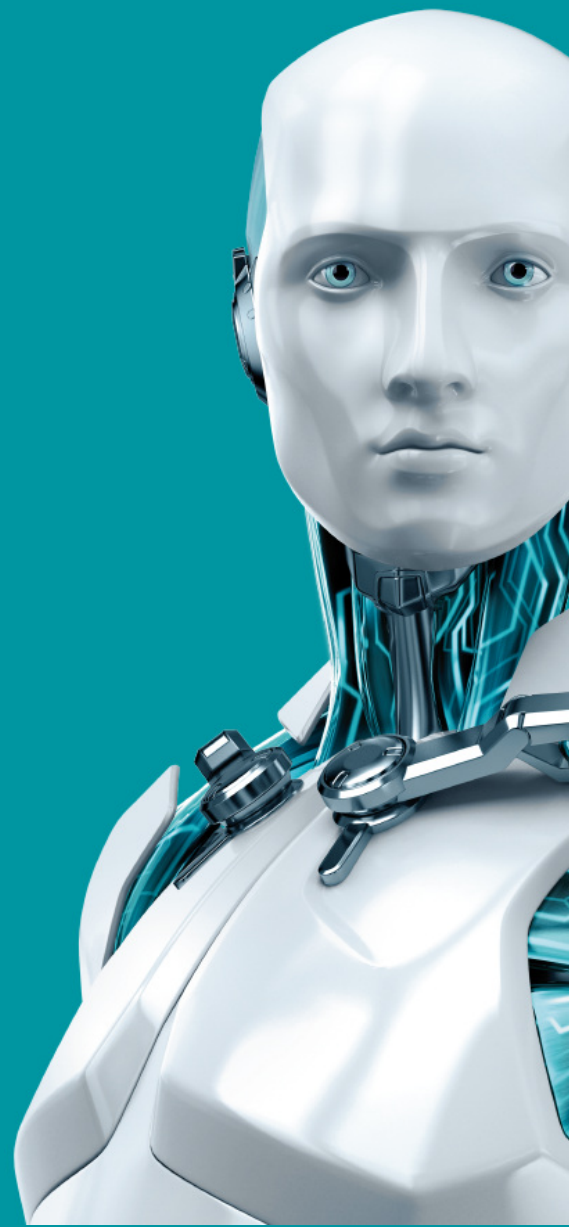
ENDPOINT ANTIVIRUS

FOR macOS

USER GUIDE

(intended for product version 6.5 and higher)

[Click here to download the most recent version of this document](#)





©ESET, spol. s.r.o.

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

For more information visit 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.

Customer Care: www.eset.com/support

REV. 10/13/2017

Contents

1. ESET Endpoint Antivirus.....	5
1.1 What's new in version 6.....	5
1.2 System requirements.....	5
2. Users connecting via ESET Remote Administrator	6
2.1 ESET Remote Administrator Server.....	6
2.2 Web Console	7
2.3 Proxy.....	7
2.4 Agent.....	8
2.5 RD Sensor.....	8
3. Installation.....	9
3.1 Typical installation.....	9
3.2 Custom installation.....	10
3.3 Remote installation.....	10
3.3.1 Creating a remote installation package	11
3.3.2 Remote installation on target computers	11
3.3.3 Remote uninstallation.....	12
3.3.4 Remote upgrade	12
4. Product activation.....	13
5. Uninstallation.....	15
6. Basic overview.....	16
6.1 Keyboard shortcuts.....	16
6.2 Checking operation of the system.....	17
6.3 What to do if the program does not work properly.....	17
7. Computer protection	18
7.1 Antivirus and antispyware protection.....	18
7.1.1 General.....	18
7.1.1.1 Exclusions.....	18
7.1.2 Startup protection	19
7.1.3 Real-time file system protection.....	19
7.1.3.1 Advanced options	19
7.1.3.2 When to modify Real-time protection configuration.....	20
7.1.3.3 Checking Real-time protection.....	20
7.1.3.4 What to do if Real-time protection does not work.....	20
7.1.4 On-demand computer scan.....	21
7.1.4.1 Type of scan.....	21
7.1.4.1.1 Smart scan.....	21
7.1.4.1.2 Custom scan	22
7.1.4.2 Scan targets.....	22
7.1.4.3 Scan profiles.....	22
7.1.5 ThreatSense engine parameters setup.....	23
7.1.5.1 Objects	23
7.1.5.2 Options.....	24
7.1.5.3 Cleaning.....	24
7.1.5.4 Exclusions	24
7.1.5.5 Limits.....	25
7.1.5.6 Others.....	25
7.1.6 An infiltration is detected	25
7.2 Web and email protection.....	26
7.2.1 Web access protection	26
7.2.1.1 Ports	26
7.2.1.2 URL lists	26
7.2.2 Email protection	27
7.2.2.1 POP3 protocol checking.....	27
7.2.2.2 IMAP protocol checking.....	27
7.3 Anti-Phishing.....	28
8. Device control.....	29
8.1 Rules editor.....	29
9. Tools.....	31
9.1 Log files.....	31
9.1.1 Log maintenance	31
9.1.2 Log filtering.....	32
9.2 Scheduler.....	32
9.2.1 Creating new tasks.....	33
9.2.2 Creating a user-defined task.....	33
9.3 Live Grid.....	34
9.3.1 Suspicious files	34
9.4 Quarantine.....	35
9.4.1 Quarantining files	35
9.4.2 Restoring a quarantined file.....	35
9.4.3 Submitting a file from Quarantine	35
9.5 Privileges.....	35
9.6 Presentation mode.....	36
9.7 Running processes.....	36
10. User interface.....	37
10.1 Alerts and notifications.....	37
10.1.1 Display alerts.....	37
10.1.2 Protection statuses	37
10.2 Context menu.....	38
11. Update.....	39
11.1 Update setup.....	39
11.1.1 Advanced options	40
11.2 How to create update tasks.....	41
11.3 Upgrading to a new build	41
11.4 System updates.....	41
12. Miscellaneous.....	43
12.1 Import and export settings.....	43
12.2 Proxy server setup.....	43
12.3 Shared Local Cache.....	44

1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 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 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 Remote Administrator 6, allowing you to easily manage any number of client workstations, apply policies and rules, monitor detections and remotely administer changes from any networked computer.

1.1 What's new in version 6

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

- **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 in the background and suppresses pop-up windows and scheduled tasks
- **Shared local cache** – allows for scanning speed improvements in virtualized environments

1.2 System requirements

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

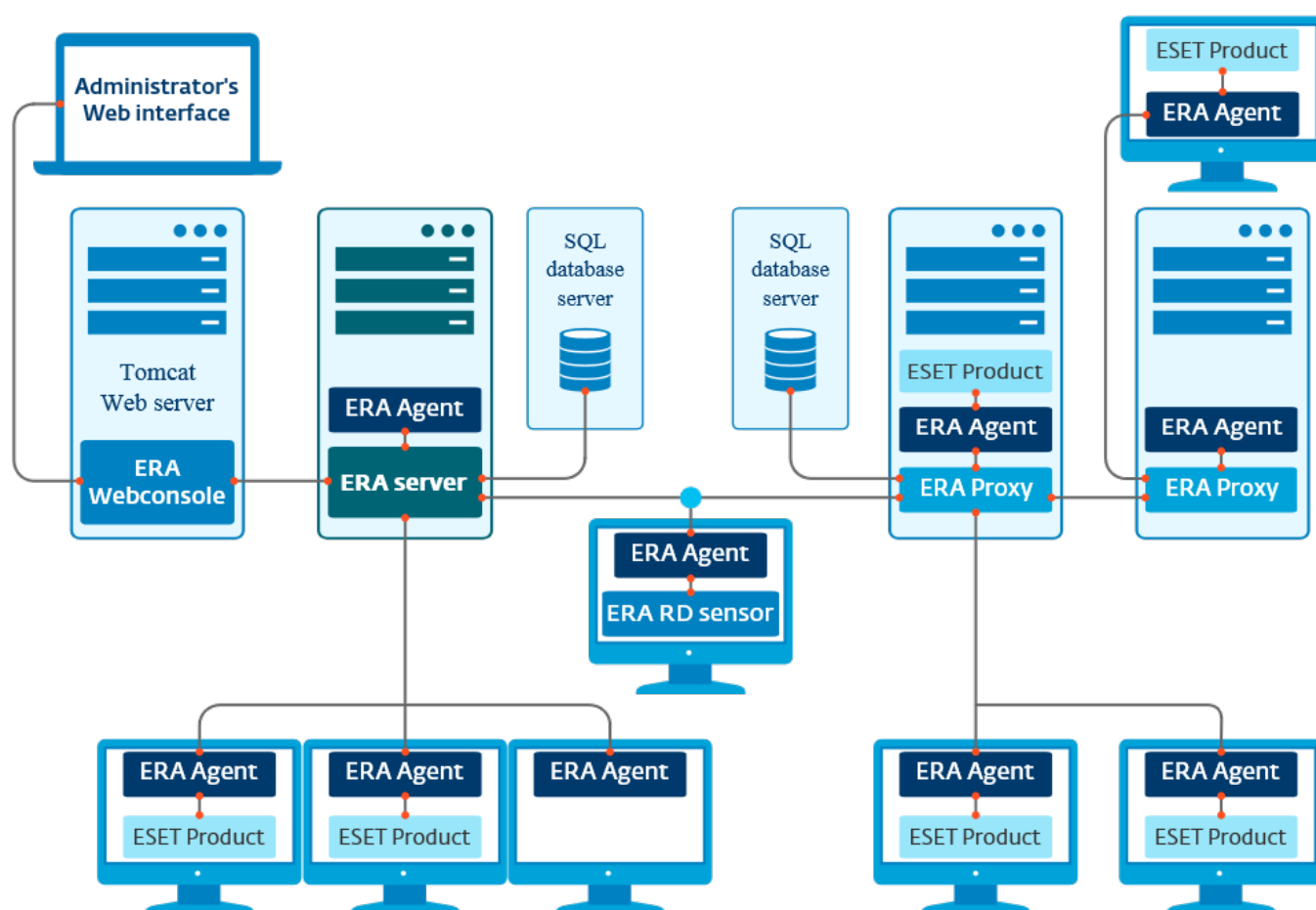
	System requirements:
Processor architecture	Intel 32-bit, 64-bit
Operating system	macOS 10.9 and later macOS Server 10.7 and later
Memory	300 MB
Free disk space	200 MB

2. Users connecting via ESET Remote Administrator

ESET Remote Administrator (ERA) 6 is an application that allows you to manage ESET products in a networked environment from one central location. The ESET Remote Administrator task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET Remote Administrator does not provide protection against malicious code on its own, it relies on the presence of an ESET security solution on each client.

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

The picture below depicts a sample architecture for a network protected by ESET security solutions managed by ERA:



NOTE: For more information see the [ESET Remote Administrator online documentation](#).

2.1 ESET Remote Administrator Server

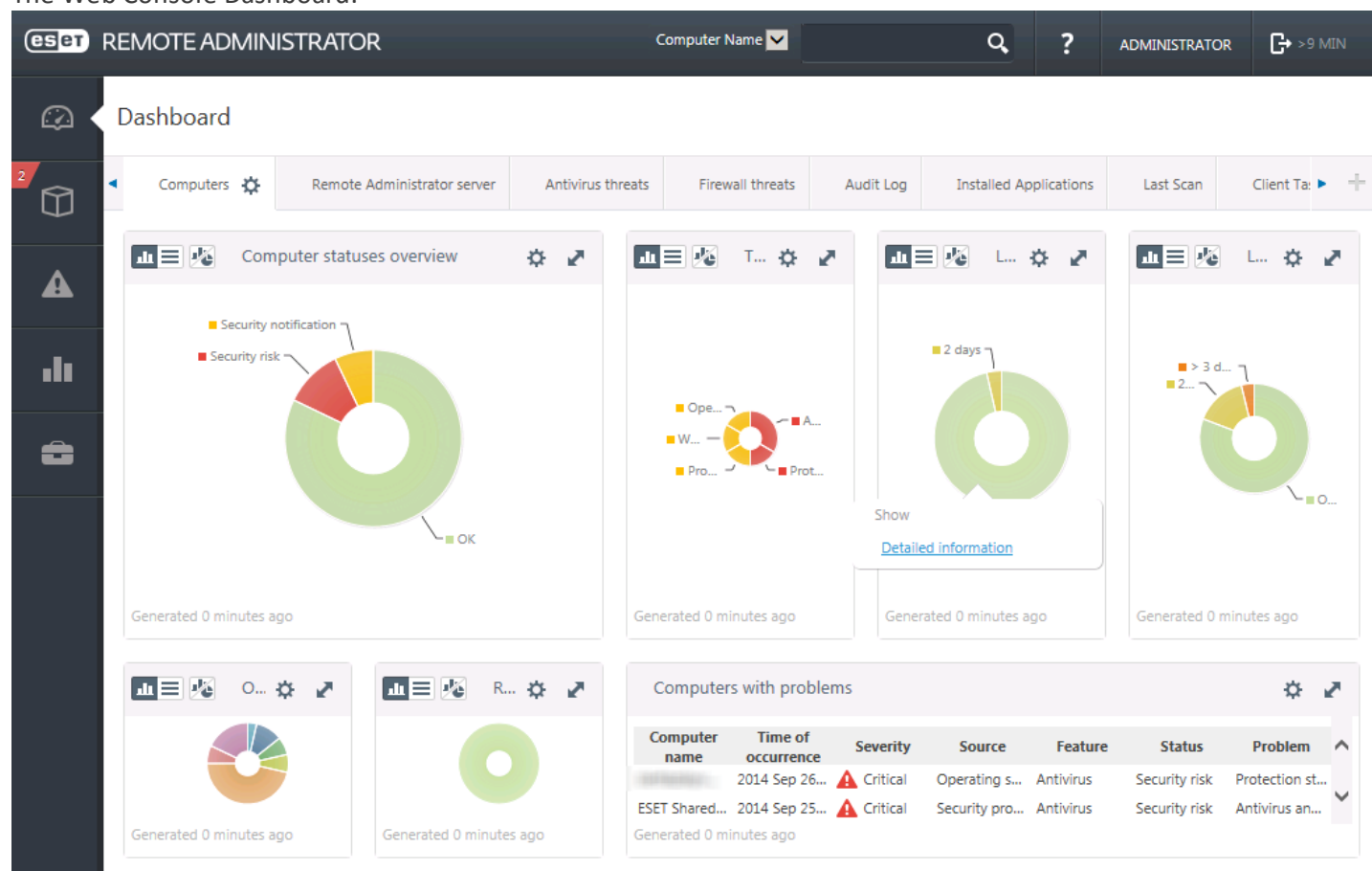
ESET Remote Administrator Server is the executive component of ESET Remote Administrator. It processes all data received from clients that connect to the Server (through the [ERA Agent](#)⁸). The ERA Agent facilitates communication between the client and the server. Data (Client logs, configuration, agent replication, etc.) are stored in a database that ERA accesses to provide reporting.

To correctly process the data, the ERA Server requires a stable connection to a Database server. We recommend that you install ERA Server and your database on separate servers to optimize performance. The machine on which ERA Server is installed must be configured to accept all Agent/Proxy/RD Sensor connections which are verified using certificates. Once ERA Server is installed, you can open [ERA Web Console](#)⁷ which allows you to manage endpoint workstations with ESET solutions installed.

2.2 Web Console

ERA Web Console is a web-based user interface that presents data from [ERA Server](#)^[6] and allows you to manage ESET security solutions in your network. Web Console can be accessed using a browser. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. You can choose to make the web server accessible from the internet to allow for the use of ESET Remote Administrator from virtually any place or device.

The Web Console Dashboard:



The **Quick Search** tool is located at the top of the Web Console. Select **Computer Name**, **IPv4/IPv6 Address** or **Threat Name** from the drop-down menu, type your search string into the text field and then click the magnifier symbol or press **Enter** to search. You will be redirected to the **Groups** section, where your search result will be displayed.

2.3 Proxy

ERA Proxy is another component of ESET Remote Administrator with two main purposes. In a medium-sized or enterprise network with many clients (for example, 10,000 clients or more), you can use ERA Proxy to distribute load between multiple ERA Proxies facilitating the main [ERA Server](#)^[6]. The other advantage of the ERA Proxy is that you can use it when connecting to a remote branch office with a weak link. This means that the ERA Agent on each client is not connecting to the main ERA Server directly via ERA Proxy, which is on the same local network as the branch office. This configuration frees up the link to the branch office. The ERA Proxy accepts connections from all local ERA Agents, compiles data from them and uploads it to the main ERA Server (or another ERA Proxy). This allows your network to accommodate more clients without compromising the performance of your network and database queries.

Depending on your network configuration, it is possible for ERA Proxy to connect to another ERA Proxy and then connect to the main ERA Server.

For proper function of the ERA Proxy, the host computer where you install ERA Proxy must have an ESET Agent installed and must be connected to the upper level (either ERA Server or an upper ERA Proxy, if there is one) of your network.

2.4 Agent

ERA Agent is an essential part of the ESET Remote Administrator product. ESET security solutions on client machines (for example ESET Endpoint Antivirus) communicate with ERA Server through the Agent. This communication allows for the management of ESET security solutions on all remote clients from a one central location. The Agent collects information from the client and sends it to the Server. When the Server sends a task to a client, the task is sent to the Agent which then communicates with the client. All network communication happens between the Agent and the upper part of the ERA network – Server and Proxy.

The ESET Agent uses one of the following three methods to connect to the Server:

1. The Client's Agent connected directly to the Server.
2. The Client's Agent connects via a Proxy that is connected to the Server.
3. The Client's Agent connects to the Server through multiple Proxies.

The ESET Agent communicates with ESET solutions installed on a client, collects information from programs on that client and passes configuration information received from the Server to the client.

NOTE: The ESET proxy has its own Agent which handles all communication tasks between clients, other proxies and the Server.

2.5 RD Sensor

RD (Rogue Detection) Sensor is a part of ESET Remote Administrator designed to find computers on your network. It provides a convenient way of adding new computers to ESET Remote Administrator without the need to find and add them manually. Every computer found on your network is displayed in the Web Console and added to the default **All** group. From here, you can take further actions with individual client computers.

RD Sensor is a passive listener that detects computers that are present on the network and sends information about them to the ERA Server. The ERA Server evaluates whether the PCs found on the network are unknown or already managed.

3. Installation

There are two ways to launch the ESET Endpoint Antivirus installer:

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



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

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

- [Typical installation](#)⁹
- [Custom installation](#)¹⁰
- [Remote installation](#)¹⁰

3.1 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 if you do not have particular requirements for specific settings.

ESET Live Grid

The ESET Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed and processed. Click **Setup** to modify detailed settings for the submission of suspicious files. For more information see [Live Grid](#)³⁴.

Potentially Unwanted Applications

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

After installing ESET Endpoint Antivirus, you should perform a computer scan for malicious code. From the main program window click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see the section [On-demand computer scan](#)^[21].

3.2 Custom installation

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

Program Components

ESET Endpoint Antivirus 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 installation.

Proxy Server

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

Privileges

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

ESET Live Grid

The ESET Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed and processed. Click **Setup** to modify detailed settings for the submission of suspicious files. For more information see [Live Grid](#)^[34].

Potentially Unwanted Applications

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

After installing ESET Endpoint Antivirus, you should perform a computer scan for malicious code. From the main program window click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see [On-demand computer scan](#)^[21].

3.3 Remote installation

Remote installation allows you to create an installation package that can be installed on target computers using remote desktop software. When installation is complete, ESET Endpoint Antivirus can be managed remotely via ESET Remote Administrator.

Remote installation is done in two phases:

1. [Creating a remote installation package using ESET installer](#)^[11]
2. [Remote installation using remote desktop software](#)^[11]

Using the latest version of ESET Remote Administrator 6, you can also perform a remote installation on macOS client computers. For detailed instructions, follow the steps described in [this Knowledgebase article](#). (The article may not be available in your language.)

3.3.1 Creating a remote installation package

Program Components

ESET Endpoint Antivirus 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 installation.

Proxy Server

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

Privileges

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

ESET Live Grid

The ESET Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed and processed. Click **Setup** to modify detailed settings for the submission of suspicious files. For more information see [Live Grid](#)³⁴.

Potentially Unwanted Applications

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

Remote Installation Files

In the last step of the installation wizard, select a destination folder for the installation package (esets_remote_Install.pkg), the setup shell script (esets_setup.sh) and the uninstallation shell script (esets_remote_UnInstall.sh).

3.3.2 Remote installation on target computers

ESET Endpoint Antivirus can be installed on target computers using Apple Remote Desktop or any other tool that supports the installation of standard macOS packages (.pkg) by copying the files and running shell scripts on target computers.

To install ESET Endpoint Antivirus using Apple Remote Desktop:

1. Click the **Copy** icon in Apple Remote Desktop.
2. Click **+**, navigate to the installation shell script (esets_setup.sh) and select it.
3. Select **/tmp** from the **Place items in** drop-down menu and click **Copy**.
4. Click **Install** to send the package to your target computers.

For a detailed instructions on how to administer client computers using ESET Remote Administrator please refer to the [ESET Remote Administrator online documentation](#).

3.3.3 Remote uninstallation

To uninstall ESET Endpoint Antivirus from client computers:


1. Using the **Copy Items** command in Apple Remote Desktop, locate the uninstallation shell script (*esets_remote_unInstall.sh* – created along with the installation package) and copy the shell script to the /tmp directory on target computers (for example, */tmp/esets_remote_uninstall.sh*).
2. Select **User** under **Run command as** and then type **root** into the **User** field.
3. Click **Send**. After successful uninstallation, a console log will be shown.

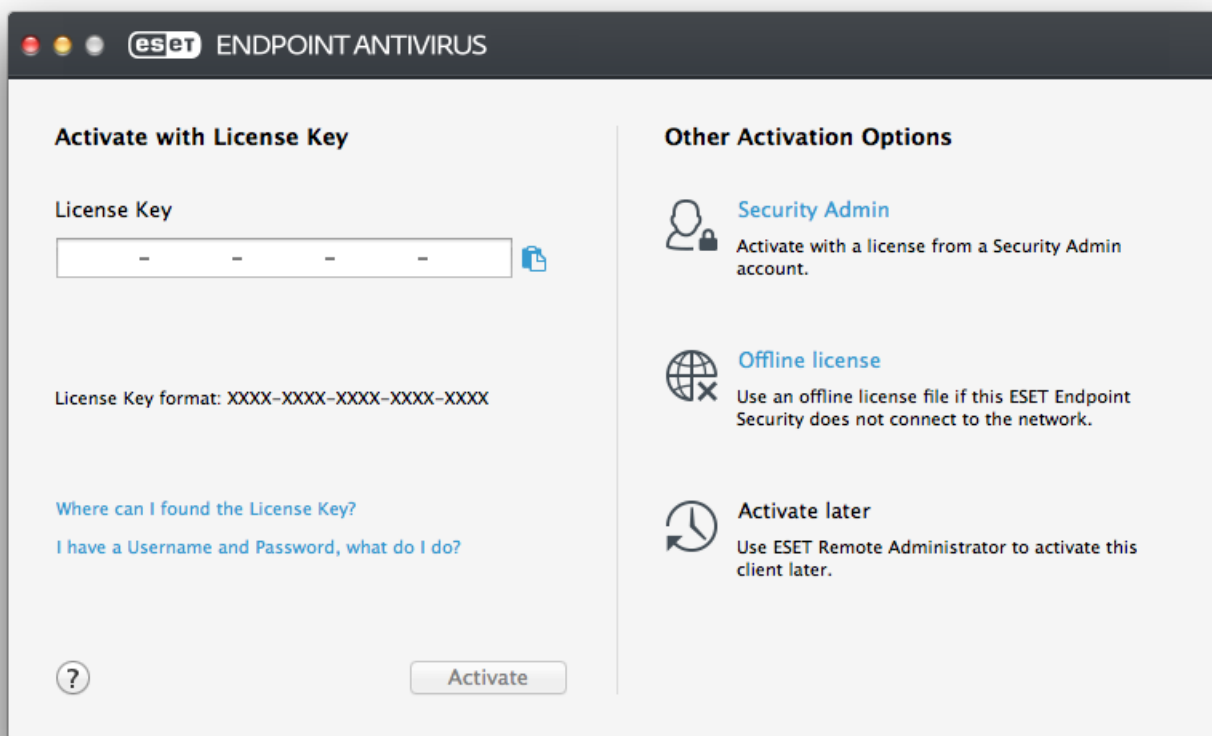
3.3.4 Remote upgrade

Use the **Install packages** command in Apple Remote Desktop to install the latest version of ESET Endpoint Antivirus when a new version becomes available.

4. Product activation

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

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



You can use any of the following methods to activate ESET Endpoint Antivirus:

- **Activate with License Key** – A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and activation of the license. You can find your License key in the email received after the purchase or on the license card included in the box.
- **Security Admin** – An account created on the [ESET License Administrator portal](#) with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- **Offline license** – An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the ESET License Administrator portal and is used in environments where the application cannot connect to the licensing authority.

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

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

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

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

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

5. Uninstallation

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

- insert the ESET Endpoint Antivirus installation CD/DVD into your computer, open it from your desktop or **Finder** window and double-click **Uninstall**
- open the ESET Endpoint Antivirus installation file (*.dmg*) and double-click **Uninstall**
- launch **Finder**, open the **Applications** folder on your hard drive, CTRL+click the **ESET Endpoint Antivirus** icon and select **Show Package Contents**. Open the **Contents > Helpers** folder and double-click the **Uninstaller** icon.

6. Basic overview


The main program window of ESET Endpoint Antivirus 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** – this section allows you to configure and launch the [On-demand computer scan](#)^[21].
- **Update** – displays information about modules updates.
- **Setup** – select this section to adjust your computer's security level.
- **Tools** – provides access to [Log files](#)^[31], [Scheduler](#)^[32], [Quarantine](#)^[35], [Running processes](#)^[36] and other program features.
- **Help** – displays access to help files, Internet Knowledgebase, support request form and additional program information.

6.1 Keyboard shortcuts

Keyboard shortcuts that can be used when working with ESET Endpoint Antivirus:

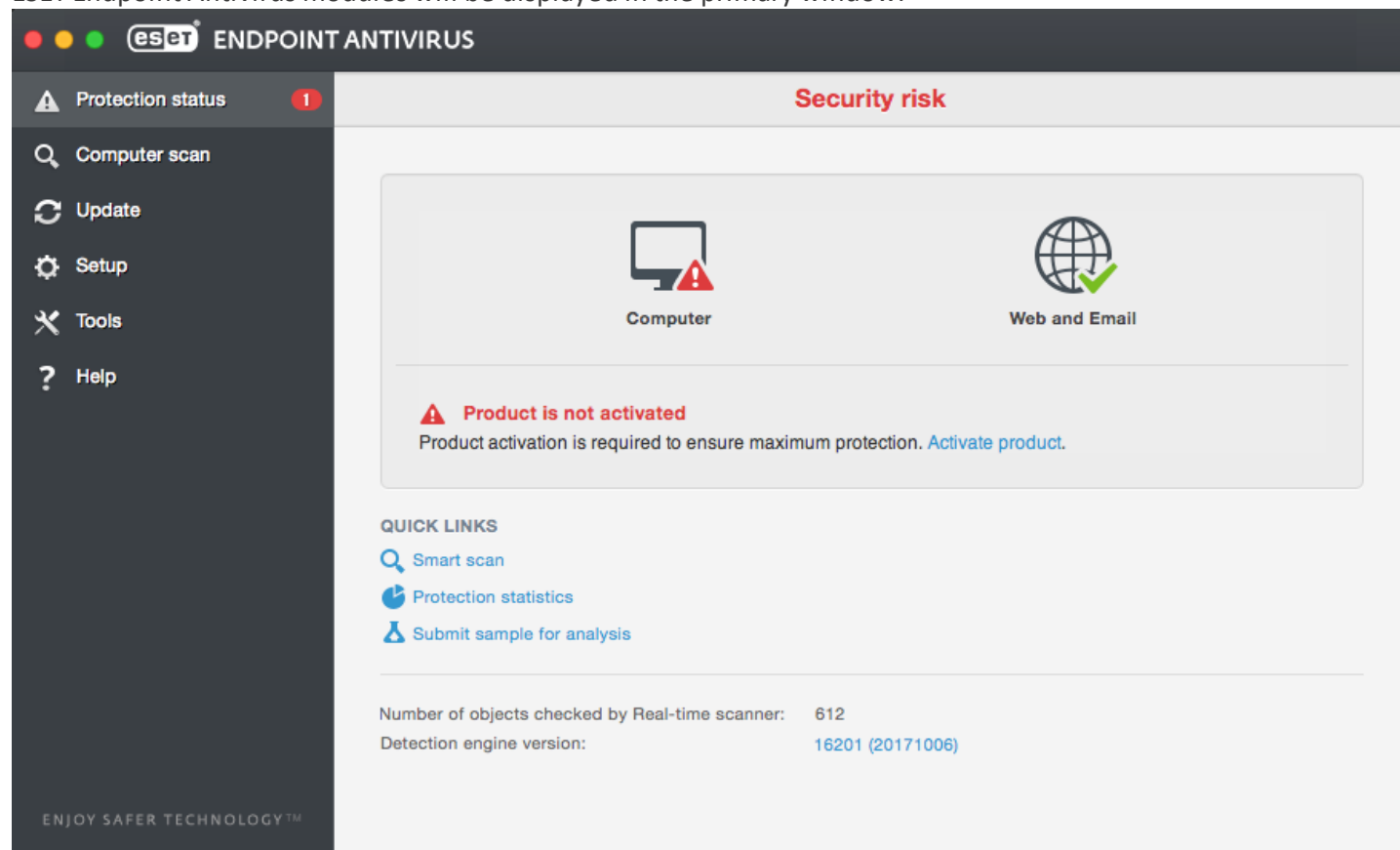
- *cmd+,* – displays ESET Endpoint Antivirus preferences,
- *cmd+O* – resizes the ESET Endpoint Antivirus main GUI window to the default size and moves it to the center of the screen,
- *cmd+Q* – hides the ESET Endpoint Antivirus main GUI window. You can open it by clicking the ESET Endpoint Antivirus icon  in the macOS Menu Bar (top of the screen),
- *cmd+W* – closes the ESET Endpoint Antivirus main GUI window.

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

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

6.2 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 modules will be displayed in the primary window.



6.3 What to do if the program does not work properly

When a module is functioning properly, a green check mark icon is displayed. When a module is not functioning properly, a red exclamation point or an orange notification icon is displayed. Additional information about the module and a suggested solution for fixing the issue is displayed in the main program window. To change the status of individual modules, click the blue link below each notification message.

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

7. Computer protection

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

7.1 Antivirus and antispyware protection

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

7.1.1 General

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



- **Potentially unwanted applications** – These applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the way it behaved before these applications were installed). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.
- **Potentially unsafe applications** – These applications are commercial, legitimate software that can be abused by attackers if installed without user consent. This classification includes programs such as remote access tools, for this reason this option is disabled by default.
- **Suspicious applications** – These applications include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection. A Packer is a runtime self-extracting executable that includes several kinds of malware in a single package. The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

To set up [File System or Web and Mail exclusions](#)¹⁸, click **Setup**.

7.1.1.1 Exclusions

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

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

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


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

7.1.2 Startup protection

Startup file check automatically scans files at system startup. By default, this scan runs regularly as a scheduled task after a user logon or after a successful modules update. To modify ThreatSense engine parameter settings applicable to the Startup scan, click **Setup**. You can learn more about ThreatSense engine setup by reading [this section](#)^[23].

7.1.3 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](#)^[23]), Real-time file system protection may vary for newly created files and existing files. Newly created files can be more precisely controlled.

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

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

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

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

To modify advanced settings for Real-time file system protection, go to **Setup > Enter application preferences ...** (or press *cmd+,*) > **Real-Time Protection** and click **Setup...** next to **Advanced Options** (described in [Advanced scan options](#)^[19]).

7.1.3.1 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](#)^[23].

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

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

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

7.1.3.2 When to modify Real-time protection configuration

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

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

7.1.3.3 Checking Real-time protection

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

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

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

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

The output of the Terminal bash includes the following statuses:

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

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

7.1.3.4 What to do if Real-time protection does not work

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

Real-time protection is disabled

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

Real-time protection does not detect and clean infiltrations

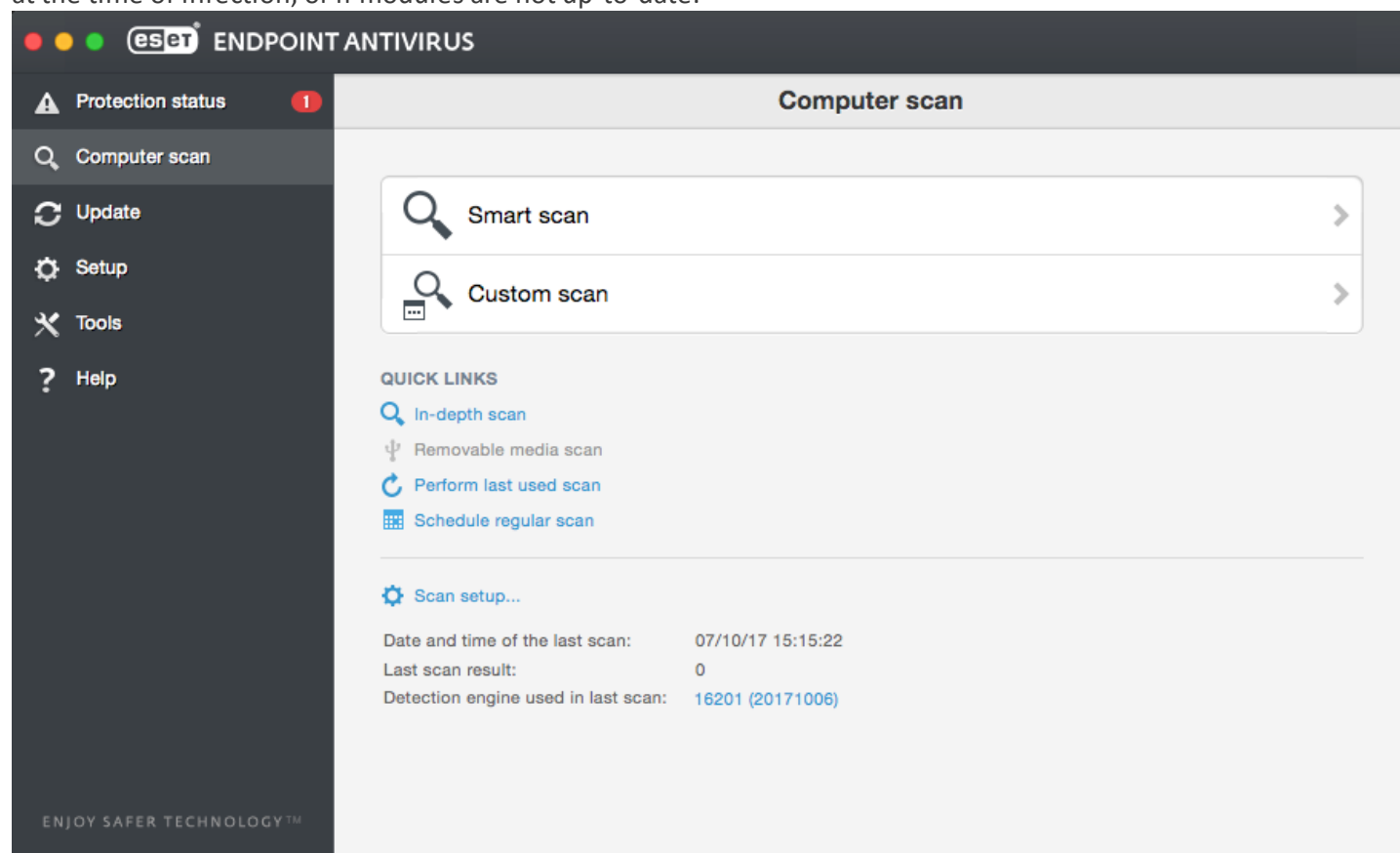
Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs that may be on your system.

Real-time protection does not start

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

7.1.4 On-demand computer scan

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



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

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

7.1.4.1 Type of scan

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

7.1.4.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantage is easy operation with no detailed scanning configuration. Smart scan checks all files in all folders and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see [Cleaning](#)^[24].

7.1.4.1.2 Custom scan

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

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

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

7.1.4.2 Scan targets

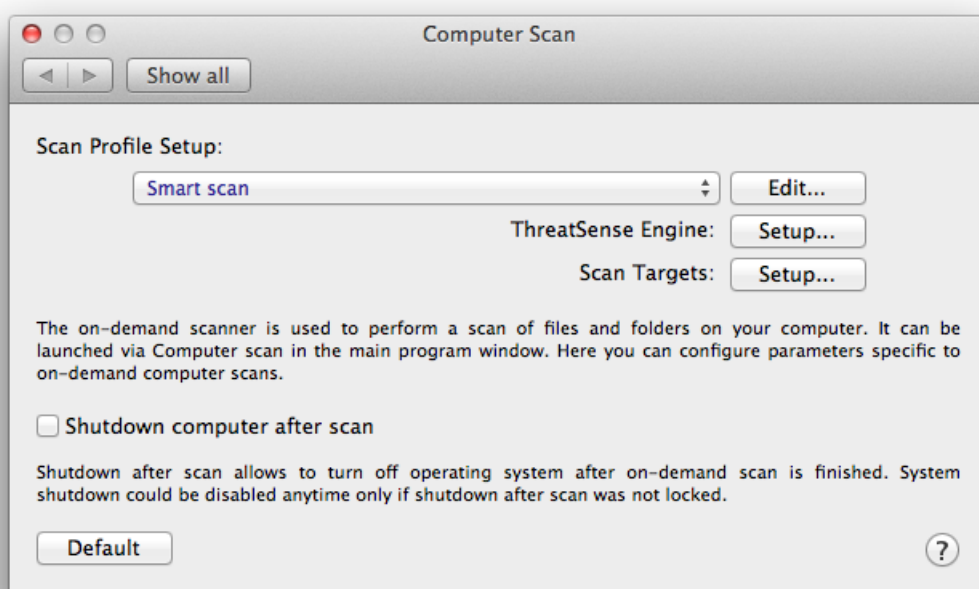
The Scan targets tree structure allows you to select files and folders to be scanned for viruses. Folders may also be selected according to a profile's settings.

A scan target can be more precisely defined by entering the path to the folder or file(s) you want to include in scanning. Select targets from the tree structure that lists all available folders on the computer by selecting the check box that corresponds to a given file or folder.

7.1.4.3 Scan profiles

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

To create a new profile, from the main menu click **Setup > Enter application preferences ...** (or press *cmd+,*) > **Computer Scan** and click **Edit** next to the list of current profiles.



To help you create a scan profile to fit your needs, see the [ThreatSense engine parameters setup](#)^[23] section for a description of each parameter of the scan setup.

Example: Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you do not want to scan runtime packers or potentially unsafe applications and you also want to apply Strict cleaning. In the **On-demand Scanner Profiles List** window, type the profile name, click **Add** and then confirm

by clicking **OK**. Adjust the parameters to meet your requirements using the **ThreatSense Engine** and **Scan Targets** settings.

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

7.1.5 ThreatSense engine parameters setup

ThreatSense is a proprietary ESET technology comprised of several complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, etc.) that work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully prevents rootkits.

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

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

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

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

The ThreatSense parameters are specifically optimized for each module, and their modification can significantly influence system operation. For example, changing settings to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in a slower system. Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

7.1.5.1 Objects

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

- **Symbolic links** – (Computer scan only) scans files that contain a text string that is interpreted as a path to a file or directory.
- **Email files** – (not available in Real-time Protection) scans email files.
- **Mailboxes** – (not available in Real-time Protection) scans user mailboxes in the system. Incorrect use of this option may result in a conflict with your email client. To learn more about advantages and disadvantages of this option, read the following [knowledgebase article](#).
- **Archives** – (not available in Real-time Protection) scans files compressed in archives (.rar, .zip, .arj, .tar, etc.).
- **Self-extracting archives** – (not available in Real-time Protection) scans files which are contained in self-extracting archive files.
- **Runtime packers** – unlike standard archive types, runtime packers decompress in memory. When this is selected, standard static packers (e.g. UPX, yoda, ASPack, FGS) are also scanned.

7.1.5.2 Options

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

- **Heuristics** – Heuristics use an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist.
- **Advanced heuristics** – Advanced heuristics is comprised of a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. The program's detection ability is significantly higher as a result of advanced heuristics.

7.1.5.3 Cleaning



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

- **No cleaning** – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.
- **Standard cleaning** – The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow-up actions. The choice of follow-up actions will also be displayed if a predefined action cannot be completed.
- **Strict cleaning** – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean a file, you will receive a notification and be asked to select the type of action to take.

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

7.1.5.4 Exclusions

An extension is the part of a file name delimited by a period. The extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to be excluded from scanning.

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

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

log
cfg
tmp

7.1.5.5 Limits

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

- **Maximum Size:** Defines the maximum size of objects to be scanned. The antivirus module will only scan objects smaller than the size specified. We do not recommend changing the default value, as there is usually no reason to modify it. This option should only be changed by advanced users who have specific reasons for excluding larger objects from scanning.
- **Maximum Scan Time:** Defines the maximum time allotted to scan an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, whether or not the scan has finished.
- **Maximum Nesting Level:** Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances, there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.
- **Maximum File Size:** This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If scanning is prematurely terminated as a result of this limit, the archive will remain unchecked.

7.1.5.6 Others

Enable Smart optimization

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

Scan alternative data stream (On-demand scanner only)

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

7.1.6 An infiltration is detected

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

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

1. Click **Computer scan**.
2. Click **Smart scan** (for more information, see the [Smart scan](#) ²¹ 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, suppose that an infiltration is detected by the Real-time file system monitor using the default cleaning level. Real-time protection will attempt to clean or delete the file. If there is no predefined action available for the Real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, since the infected file(s) is left in its infected state. This option is intended for situations when you are sure that the file is harmless and has been detected by mistake.

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

Deleting files in archives – In the default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. Use caution when performing a **Strict cleaning** scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

7.2 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**.

- **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.

7.2.1 Web access protection

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

Web filtering can be achieved by defining [the port numbers for HTTP communication](#)^[26] and/or [URL addresses](#)^[26].

7.2.1.1 Ports

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

7.2.1.2 URL lists

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

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

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

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

7.2.2 Email protection

Email protection provides control of email communication received through the POP3 and IMAP protocols. When examining incoming messages, the program uses all the advanced scanning methods included in the ThreatSense scanning engine. Scanning of the POP3 and IMAP protocol communications is independent of the email client used.

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

Append tag message to email footnote – after an email has been scanned, a notification containing scan results can be appended to the message. Tag messages cannot be relied on without question, since they may be omitted in problematic HTML messages and can be forged by some viruses. The following options are available:

- **Never** – no tag messages will be added at all
- **To infected email only** – only messages containing malicious software will be marked as checked
- **To all scanned email** – the program will append messages to all scanned email

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

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

In the bottom part of this window, you can also enable/disable checking of email communication received through the POP3 and IMAP protocols. To learn more about this, see the following topics:

- [POP3 protocol checking](#)^[27]
- [IMAP protocol checking](#)^[27]

7.2.2.1 POP3 protocol checking

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

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

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

7.2.2.2 IMAP protocol checking

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

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

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

7.3 Anti-Phishing

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

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

8. Device control

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

Supported external devices:

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




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

The Device control log records all incidents that trigger Device control. Log entries can be viewed from the main program window of ESET Endpoint Antivirus in **Tools** > [Log files](#)³¹.

8.1 Rules editor

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

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

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

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

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

Name

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

Device Type

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

Action

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

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

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

Block – Access to the device will be blocked

Criteria type

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

Vendor – Filter by vendor name or ID

Model – The given name of the device

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

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

TIP: To view information about a device, create a rule for that type of device and connect the device to your computer. Once the device has been connected, device details will be displayed in the [Device control log](#)³¹.

Logging severity

Always – Logs all events

Diagnostic – Logs information needed to fine-tune the program

Information – Records informative messages plus all the records above

Warning – Records critical errors and warning messages

None – No logs will be recorded

User list

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

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

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

9. Tools

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

9.1 Log files

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

Log files are accessible from the ESET Endpoint Antivirus main menu by clicking **Tools > Log files**. Select the desired log type using the **Log** drop-down menu at the top of the window. The following logs are available:

1. **Detected threats** – Information about events related to the detection of infiltrations.
2. **Events** – All important actions performed by ESET Endpoint Antivirus are recorded in the Event logs.
3. **Computer scan** – Results of all completed scans are displayed in this window. Double-click any entry to view the details of a specific computer scan.
4. **Device control** – Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial number, vendor name and media size (if available).
5. **Filtered websites** – This list is useful if you want to view a list of websites that were blocked by [Web access protection](#)^[26]. In these logs you can see the time, URL, status, IP address, user and application that opened a connection to the particular website.

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

9.1.1 Log maintenance

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

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

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

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

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

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

To configure the filters for **Default Computer Scan Log Records**, click **Edit** and select/deselect log types as required. Further explanation to these log types can be found in [Log Filtering](#)^[32].

9.1.2 Log filtering

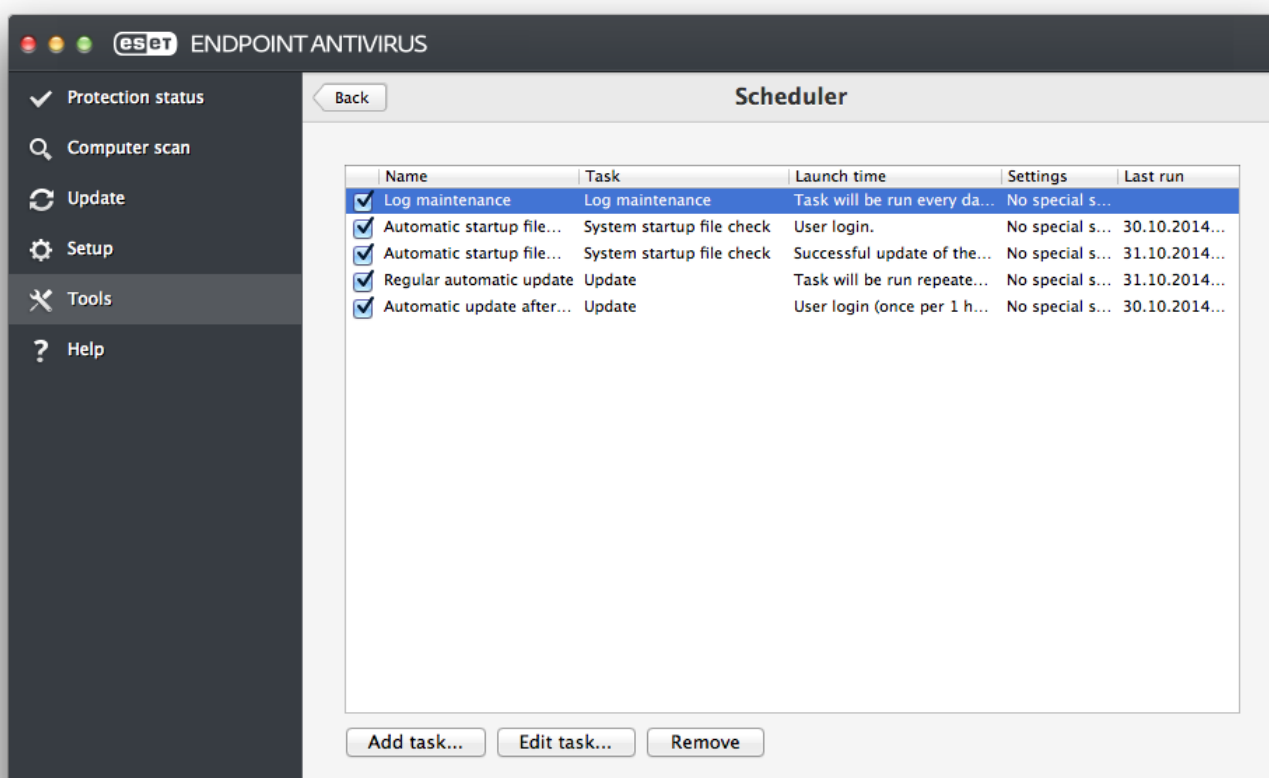
Logs store information about important system events. The log filtering feature allows you to display records about specific events.

The most frequently used log types are listed below:

- **Critical warnings** – critical system errors (for example, Antivirus protection failed to start)
- **Errors** – error messages such as "*Error downloading file*" and critical errors
- **Warnings** – warning messages
- **Informative records** – informative messages including successful updates, alerts, etc.
- **Diagnostic records** – information needed to fine-tune the program as well as all records described above.

9.2 Scheduler

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



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

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

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

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

9.2.1 Creating new tasks

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

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

NOTE: By choosing **Run application**, you can run programs as a system user called "nobody". Permissions for running applications through the Scheduler are defined by macOS.

In the example below, we will use the Scheduler to add a new update task, since update is one of the most frequently used scheduled tasks:

1. Select **Update** from the **Scheduled task** drop-down menu.
2. Type a name for the task in the **Task name** field.
3. Select the frequency of the task from the **Run task** drop-down menu. Based on the frequency selected, you will be prompted to specify different update parameters. If you select **User-defined**, you will be prompted to specify date/time in the *cron* format (see the [Creating user-defined task](#)³³ section for more details).
4. In the next step, define what action to take if the task cannot be performed or completed at the scheduled time.
5. Click **Finish**. The new scheduled task will be added to the list of currently scheduled tasks.

By default ESET Endpoint Antivirus contains pre-defined scheduled tasks to ensure correct product functionality. These should not be altered, and are hidden by default. To make these tasks visible, from the main menu click **Setup > Enter application preferences > Scheduler** and select **Show system tasks**.

9.2.2 Creating a user-defined task

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

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

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

For example:

30 6 22 3 2012 4

The following special characters are supported in cron expressions:

- asterisk (*) – expression will match for all values of the field; e.g. asterisk in the 3rd field (day of month) means every day
- hyphen (-) – defines ranges; e.g. 3-9
- comma (,) – separates items of a list; e.g. 1, 3, 7, 8
- slash (/) – defines increments of ranges; e.g. 3-28/5 in the 3rd field (day of month) means 3rd day of the month and then every 5 days.

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

NOTE: If you define both a day of the month and day of the week, the command will only be executed when both fields match.

9.3 Live Grid

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

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

The Live Grid Early Warning System will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer’s operating system.

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

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

9.3.1 Suspicious files

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

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

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

Below is an example of a statistical package submitted:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

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

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

9.4 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.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted to the ESET Threat Lab for analysis.

Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, the reason it was quarantined (for example, added by user) and the number of threats detected. The quarantine folder (*/Library/Application Support/Eset/esets/cache/quarantine*) remains in the system even after uninstalling ESET Endpoint Antivirus. Quarantined files are stored in a safe encrypted form and can be restored again after installing ESET Endpoint Antivirus.

9.4.1 Quarantining files

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

9.4.2 Restoring a quarantined file

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

9.4.3 Submitting a file from Quarantine

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

9.5 Privileges

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

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

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

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

9.6 Presentation mode

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

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

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

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

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

9.7 Running processes

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



- **Process** – name of the process that is currently running on your computer. You can also use Activity monitor (found in */Applications/Utilities*) to view all processes running on your computer.
- **Risk level** – in most cases, ESET Endpoint Antivirus and ESET Live Grid technology assign risk levels to objects (files, processes, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level. Known applications marked green are definitely clean (whitelisted) and will be excluded from scanning. This improves the speed of both the On-demand and Real-time scans. When an application is marked as unknown (yellow), it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about a file, you can submit it to the ESET Threat Lab for analysis. If the file turns out to be a malicious application, its signature will be added to an upcoming update.
- **Number of Users** – the number of users that use a given application. This information is gathered by ESET Live Grid technology.
- **Time of discovery** – period of time since the application was discovered by ESET Live Grid technology.
- **Application Bundle ID** – name of the vendor or application process.

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

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

10. User interface

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

- To display the ESET Endpoint Antivirus splash screen at system startup, select **Show splash-screen at startup**.
- **Present application in Dock** allows you to display the ESET Endpoint Antivirus icon  in the macOS Dock and switch between ESET Endpoint Antivirus and other running applications by pressing `cmd+tab`. Changes take effect after you restart ESET Endpoint Antivirus (usually triggered by computer restart).
- **Use standard menu** allows you to use certain keyboard shortcuts (see [Keyboard shortcuts](#)^[16]) and see standard menu items (User interface, Setup and Tools) on the macOS Menu Bar (top of the screen).
- Enable **Show tooltips** to display tooltips when the cursor is placed over certain options in ESET Endpoint Antivirus.
- **Show hidden files** allows you to see and select hidden files in **Scan Targets** setup for a **Computer scan**.
- By default, ESET Endpoint Antivirus icon  is displayed in the Menu Bar Extras that appear at the right of the macOS Menu Bar (top of the screen). To disable this, deselect **Show icon in menu bar extras**. This change takes effect after you restart ESET Endpoint Antivirus (usually triggered by computer restart).

10.1 Alerts and notifications

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

Disabling **Display alerts** will disable all alert windows and is only recommended in specific situations. For most users, we recommend that this option be left on its default setting (enabled). Advanced options are described [in this chapter](#)^[37].

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

Since ESET Endpoint Antivirus version 6.2, you can also prevent certain **Protection statuses** from displaying in the program's main screen (**Protection status** window). To learn more about this, see the [Protection statuses](#)^[37].

10.1.1 Display alerts

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

List of Dialogs (found under **Setup > Enter application preferences ... > Alerts and notifications > Display alerts: Setup...**) shows the list of all alert dialogs triggered by ESET Endpoint Antivirus. To enable or suppress each notification, select the check box left of the **Dialog Name**. Additionally, you can define **Display Conditions** under which notifications about new device and operating system updates will be displayed.

10.1.2 Protection statuses

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

10.2 Context menu

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

11. Update

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

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

Under normal circumstances, when updates are downloaded properly, the message *Update is not necessary – the installed modules are current* will appear in the Update window if you have the latest modules. If modules cannot be updated, we recommend that you check your [update settings](#)^[39] – the most common reason for this error is incorrectly entered [license data](#)^[13] or incorrectly configured [connection settings](#)^[43].

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

11.1 Update setup

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

The screenshot shows the 'Update' window with a title bar containing window control buttons and a 'Show all' button. Below the title bar are 'Primary' and 'Secondary' tabs. The 'Update Server' section features a dropdown menu set to 'Choose automatically' with an 'Edit...' button, and input fields for 'Username:' and 'Password:'. The 'Proxy Mode' section has a dropdown set to 'Use global proxy server settings' and a descriptive text: 'Proxy mode enables you to update via a proxy server. This server can be the same or different from the product's global proxy server.' The 'Proxy Server' section includes an input field for the proxy address, a port field set to '3128', a 'Detect' button, and input fields for 'Username:' and 'Password:'. There is a 'Show password' checkbox and an unchecked checkbox for 'Use direct connection if HTTP proxy is not available'. At the bottom, there are 'Advanced Options: Setup...' and 'Clear update cache: Clear' buttons. A footer note states: 'For the program to provide complete protection against threats, it is essential to keep modules up to date. You can configure update parameters here.' A 'Default' button and a help icon (?) are also present.


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

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

Proxy Mode enables you to update detection modules using a proxy server (for example, a local HTTP proxy). The server can be the same or different from the global proxy server that applies to all program features that require a connection. Global proxy server settings should already have been defined during installation, or in [Proxy server setup](#)⁴³.

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 fill out the IP address and port number (**3128** by default).
3. Enter a valid **Username** and **Password** into the respective fields if communication with the proxy server requires authentication.

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

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

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

11.1.1 Advanced options

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

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

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

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

11.2 How to create update tasks

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

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

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

Each of the update tasks can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see [Scheduler](#)^[32].

11.3 Upgrading to a new build

For maximum protection, it is important to use the latest build of ESET Endpoint Antivirus. To check for a new version, click **Update** from the main menu on the left. If a new build is available, a notification will be displayed at the bottom of the window. Click **Learn more** to display a new window containing the version number of the new build and the changelog.

If you clicked **Download**, the file will be downloaded to your downloads folder (or the default folder set by your browser). When the file has finished downloading, launch the file and follow the installation directions. Your license information will automatically be transferred to the new installation.

We recommend that you check for upgrades regularly, especially when installing ESET Endpoint Antivirus from CD/DVD.

11.4 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 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 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

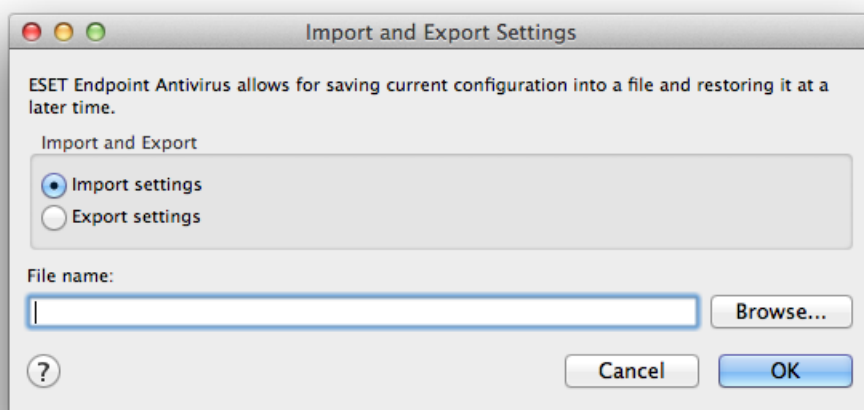
The notification window shows the updates retrieved by the command line tool called 'softwareupdate'. Updates retrieved by this tool can vary from the updates displayed by the 'Software updates' application. If you want to install all available updates displayed in the 'Missing system updates' window 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.

12. Miscellaneous

12.1 Import and export settings

To import an existing configuration or export your ESET Endpoint Antivirus 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 use at a later date. Export settings is also convenient for users who want to use their preferred configuration of ESET Endpoint Antivirus 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.

12.2 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 functions. Parameters defined here will be used by all modules that require a connection to the Internet. ESET Endpoint Antivirus supports Basic Access and NTLM (NT LAN Manager) authentication.

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

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

12.3 Shared Local Cache

To enable the use of the Shared Local Cache, click **Setup > Enter application preferences > Shared Local Cache** and select the check box next to **Enable caching using ESET Shared Local Cache**. Use of this feature boosts performance in virtualized environments by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache. When enabled, information about scans of files and folders on your network is saved to the local cache. If you perform a new scan, ESET Endpoint Antivirus will search for scanned files in the cache. If files match, they will be excluded from scanning.

Shared Local Cache settings contain the following:

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

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