ESET Cyber Security

User guide

Click here to display the online version of this document

Copyright ©2023 by ESET, spol. s r.o.

ESET Cyber Security was developed by ESET, spol. s r.o.

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

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

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

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

REV. 3/19/2023

ESET Cyber Security

ESET Cyber Security 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 constantly on alert defending your computer against attacks and malicious software.

ESET Cyber Security is a complete security solution produced from our long-term effort to combine maximum protection and a minimal system footprint. Based on artificial intelligence, the advanced technologies that comprise ESET Cyber Security can proactively eliminate infiltrations by viruses, worms, trojans, spyware, adware, rootkits, and other internet-borne attacks without hindering system performance.

What's new in version 6

ESET Cyber Security version 6 introduces the following updates and improvements:

- **64-bit architecture support**
- **Anti-Phishing** – Prevents fake websites disguised as trustworthy ones from acquiring your personal information.
- **System updates** – Provides notifications for operating system updates. To learn more about this feature, see the System updates section.
- **Protection statuses** – Hides notifications from the Protection Status window (for example, "Email protection disabled" or "Computer restart required").
- **Media to scan** – Provides the ability to exclude certain types of media from the real-time scanner (local drives, removable media, and network media).
- **Network Connections** - Displays network connections on your computer and enables you to create rules for these connections.

For more details about the new features in ESET Cyber Security, read this ESET Knowledgebase article.

System requirements

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

	System requirements:
Processor architecture	Intel 64-bit, M1, M2
Operating system	macOS 10.12 and later
Memory	300 MB
Free disk space	200 MB

In addition to existing Intel support, ESET Cyber Security version 6.10.900.0 and later support Apple M1 and M2 chips using Rosetta 2

Installation

Before you start the installation, close all open programs on your computer. ESET Cyber Security contains components that may conflict with other antivirus programs installed on your computer. Therefore, ESET strongly recommends that you remove any other antivirus programs to prevent potential problems.

To launch the Installation Wizard, do one of the following:

- If you are installing from a file downloaded from the ESET web site, open the file and double-click the **Install** icon.
- If you are installing from the installation CD/DVD, insert it into your computer, open it from your desktop or Finder window, and double-click the **Install** icon.

The installation wizard guides you through the setup. During the initial installation phase, the installer automatically checks online for the latest product version. If a newer version is found, you can download the latest version before continuing the installation.

After agreeing to the End User License Agreement, you can select one of the following installation modes:

- Typical installation
- Custom installation

Typical installation

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

1. In the **ESET LiveGrid** window, select your preferred option and click **Continue**. To change this setting later, use the **LiveGrid setup**. For more information about ESET LiveGrid, visit our Glossary.
2. In the **Potentially Unwanted Applications** window, select your preferred option (see Potentially unwanted

applications) and click **Continue**. If you decide later that you would like to change this setting, use **Advanced setup**.

3. Click **Install**. If you are prompted to type your macOS password, type it and click **Install Software**.

After installing ESET Cyber Security:

macOS Big Sur (11)

1. Allow system extensions.
2. Allow full disk access.
3. Allow ESET to add proxy configurations. You will receive the following notification: **"ESET Cyber Security" Would Like to Add Proxy Configurations**. When you receive this notification, click **Allow**. If you click **Don't Allow**, Web Access Protection will not work.

macOS 10.15 and older

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

After installation you will be prompted to activate ESET Cyber Security. You can find multiple activation options in the Activation chapter.

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

Custom installation

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

- **Proxy Server**

If you are using a proxy server, define its parameters by selecting **I use a proxy server**. In the next window, type 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). In the event that the proxy server requires authentication, type the 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 if you use a proxy server, select **Use system settings (recommended)** to use your current system settings.

- **Privileges**

You have the option to define privileged users or groups who will be given permissions 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**

For more information about ESET Live Grid, visit our Glossary.

- **Potentially Unwanted Applications**

For more information about Potentially Unwanted Applications, visit our Glossary.

After the installation of ESET Cyber Security:

macOS Big Sur (11)

1. Allow system extensions.
2. Allow Full disk access.
3. Allow ESET to Add Proxy Configurations. You will receive the following notification: **"ESET Cyber Security" Would Like to Add Proxy Configurations**. When you receive this notification, click **Allow**. If you click **Don't Allow**, Web Access Protection will not work.

macOS 10.15 and older

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

After installation you will be prompted to activate ESET Cyber Security. You can find multiple activation options in the Activation chapter.

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

Allow system extensions

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

After installation ESET Cyber Security of macOS Big Sur (11) and later, you will receive the **System Extension Blocked** notification from your system and the **Your computer is not protected** notification from ESET Cyber Security. To access all ESET Cyber Security functions, you must allow system extensions on your device.

Upgrade from previous macOS to Big Sur.

If you have already installed ESET Cyber Security and you are going to upgrade to macOS Big Sur, you will need to allow the ESET kernel extensions manually after the upgrade. Physical access to the client machine is required—when accessing remotely, the **Allow** button is disabled.

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

Allow systems extensions manually

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

For a detailed step-by-step guide, visit our Knowledgebase article. (Knowledgebase articles are not available in all languages.)

Allow Full disk access

On macOS 10.14 you will receive a **Your computer is partially protected** notification from ESET Cyber Security. To access all ESET Cyber Security functions, you must allow **Full disk access** to ESET Cyber Security.

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

ESET Real-time File System Protection not present

If **Real-time File System Protection** option is not present in the list, you need allow system extensions for your ESET product.

7. Click **Start Again** in the ESET Cyber Security alert dialog window or restart your computer. For more detailed information, visit our Knowledgebase article.

Product activation

After the installation, the **Product Activation** window is displayed automatically. To access the product activation dialog at any time, click the ESET Cyber Security icon () located in the macOS Menu Bar (at the top of the screen) and then click **Product activation**. Specify the following:

- **License Key** – Type your license key, which identifies the license owner and activates the license. The license key is a unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX or XXXX-XXXXXXXX. If you purchased a retail boxed version of the product, the license key is located inside or on the backside of the product package. If you have a username and password and do not know how to activate ESET Cyber Security, click **I have a Username and Password, what do I do?**. You are redirected to my.eset.com, where you can convert your credentials into a license key.
- **Free trial license** – Select this option if you want to evaluate ESET Cyber Security before purchasing. Type in your information and click **Register** to activate ESET Cyber Security for a limited time. Trial licenses can only be activated once per customer.
- **Purchase license** – Click this option to purchase a license. This redirects you to the web site of your local ESET distributor.
- **Activate later** – Click this option if you do not want to activate at this time.

Uninstallation

To remove ESET Cyber Security, do one of the following:

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

Basic overview

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

You can access the following sections from the main menu:

- **Home** – Provides information about the status of your computer protection and web and email protection.
- **Computer scan** – Enables you to configure and launch an on-demand computer scan.
- **Update** – Displays information about updates of detection modules.
- **Setup** – Enables you to adjust your computer's security level.
- **Tools** – Provides access to the log files, scheduler, quarantine, running processes, and other program features.
- **Help** – Provides access to the help files, ESET Knowledgebase, support request form, and additional program information.

Keyboard shortcuts

Keyboard shortcuts you can use when working with ESET Cyber Security:

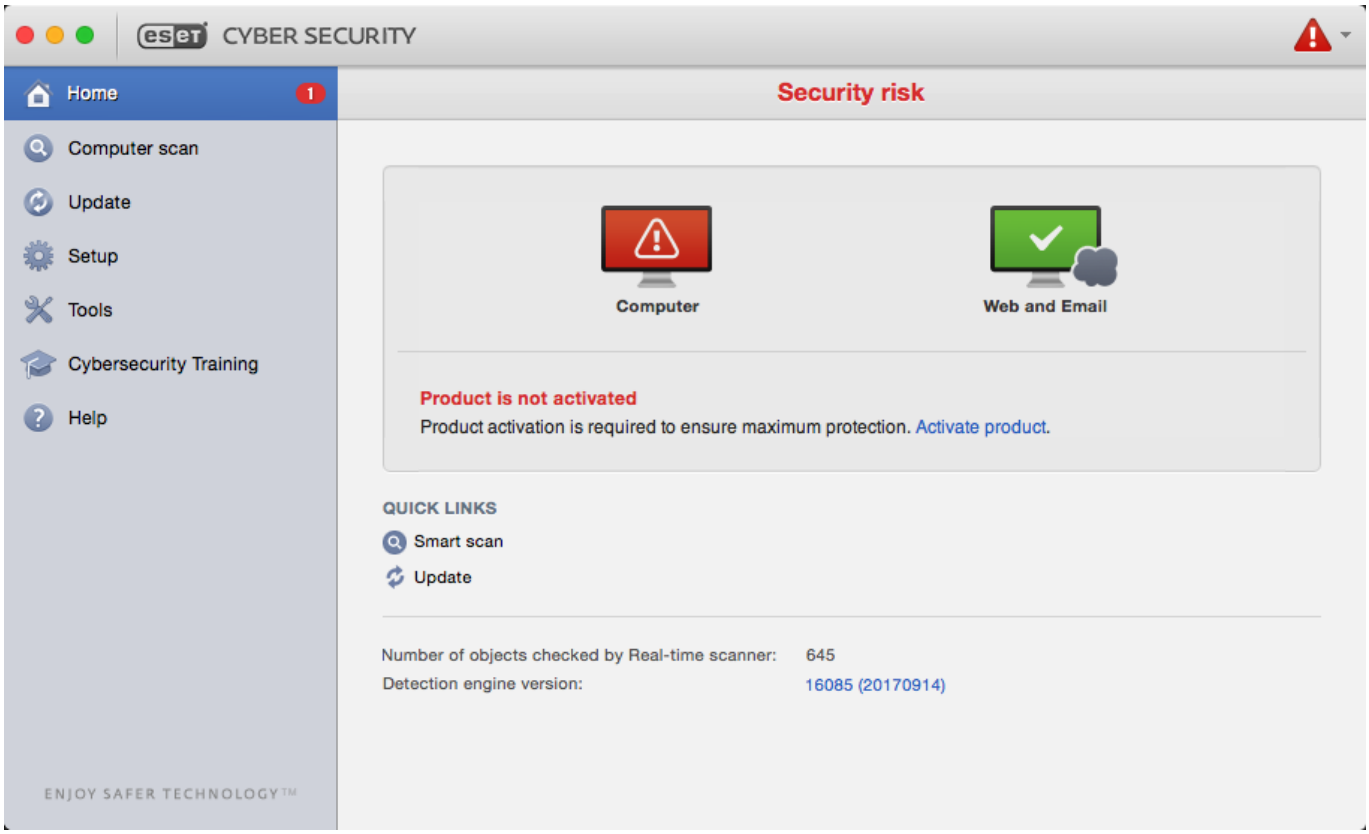
- cmd+, – d\Displays ESET Cyber Security preferences.
- cmd+O – Resizes the ESET Cyber Security main GUI window to the default size and moves it to the center of the screen.
- cmd+Q – Hides the ESET Cyber Security main GUI window. You can open it by clicking the ESET Cyber Security icon in the macOS Menu Bar (at the top of the screen),
- cmd+W – Closes the ESET Cyber Security 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.

Check the protection status

To view your protection status, click **Home** from the main menu. A status summary about the operation of ESET Cyber Security modules is displayed in the primary window.



What to do if the program does not work properly

When a module is functioning properly, a green 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 shown. To change the status of individual modules, click the blue link below each notification message.

If you cannot solve a problem using the suggested solutions, you can search the ESET Knowledgebase for a solution or contact ESET Customer Care. Customer Care responds quickly to your questions and helps resolve any issues with ESET Cyber Security.

Computer protection

You can find computer configuration under **Setup** > **Computer**. This window shows the status of **Real-time file system protection** and **Removable media blocking**. To turn off individual modules, switch the desired module's button to **DISABLED**. Note that this may decrease the level of protection of your computer. To access detailed settings for each module, click **Setup**.

Antivirus and antispyware protection

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

General

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

- **Potentially unwanted applications** – Grayware or potentially unwanted applications (PUAs) is a broad category of software whose intent is not as unequivocally malicious as other types of malware, such as viruses or trojans. However, these applications could install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by you. Read more about these types of applications in the Glossary.
- **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 rolls up several kinds of malware into a single package. The most common packers are UPX, PE_Compact, PKLite, and ASPack. The same malware may be detected differently when compressed using a different packer. Packers can also make their "signatures" mutate over time, making malware more difficult to detect and remove.

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

Exclusions

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

Files and folders listed in the **File System** tab are excluded from all scanners: startup, real-time, and on-demand (computer scan). The following information and settings are available:

- **Path** – The path to excluded files and folders.
- **Threat** – If there is a name of a threat next to an excluded file, it means that the file is only excluded for that threat, but not completely. If that file becomes infected later with other malware, it is detected by the antivirus module.
-  – Creates a new exclusion. 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.

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

Startup protection

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

Real-time file system protection

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

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

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

- **Local drives** – System hard drives
- **Removable media** – CDs, DVDs, USB media, Bluetooth devices, and so on

- **Network media** – All mapped drives

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

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

Advanced options

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

ESET does not recommend making changes in the **Default archives settings** section unless required to resolve a specific issue, as higher archive nesting values can impede system performance. The following options are available:

- **ThreatSense parameters for executed files** – By default, **Advanced heuristics** is used when files are executed. ESET strongly recommends keeping Smart optimization and ESET Live Grid enabled to mitigate the impact on system performance.
- **Increase network volumes compatibility** – This option boosts performance when accessing files over the network. Enable it if you experience slowdowns while accessing network drives. This feature uses the system file coordinator on macOS 10.10 and later. Be aware that not all applications support the file coordinator. Fr example, Microsoft Word 2011 does not support it, but Word 2016 does.

When to modify real-time protection configuration

Real-time protection is the most essential component for maintaining a secure system with ESET Cyber Security. Use caution when modifying the real-time protection parameters. ESET recommends that you only modify these parameters in specific cases, for example, a situation in which there is a conflict with a certain application.

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

Check real-time protection

To verify that Real-time protection is working and detecting viruses, download the eicar.com test file and verify that ESET Cyber Security identifies it as a threat. 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.

What to do if real-time protection does not work

Below are descriptions of 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, the protection must be reactivated. To reactivate real-time protection, from the main menu click **Setup** > **Computer** and switch **Real-time file system protection** to **ENABLED**. Alternatively, you can enable real-time file system protection in the application preferences window under **Real-Time Protection** by selecting **Enable real-time file system protection**.

Real-time protection does not detect and clean infiltrations

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

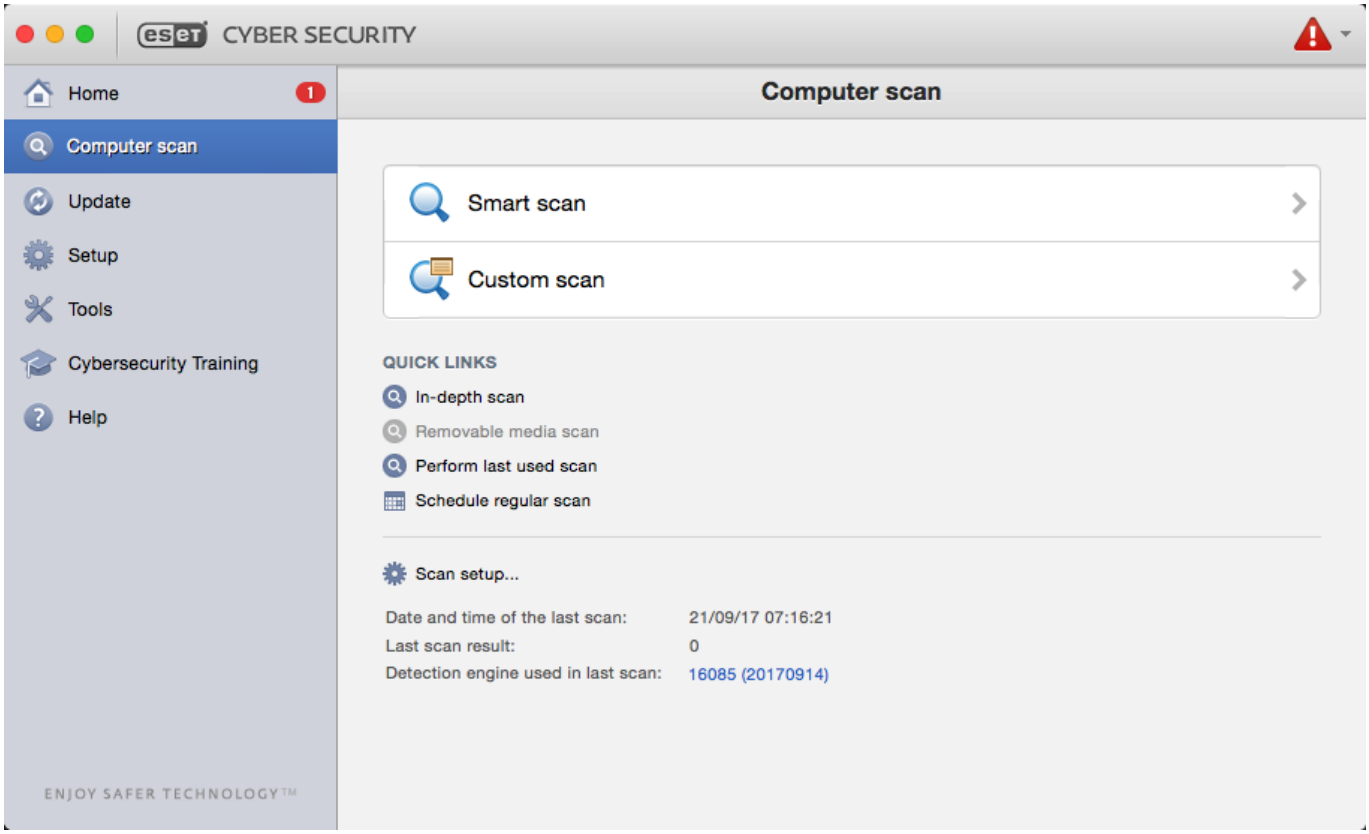
Real-time protection does not start

If real-time protection is not initiated at the system startup, there may be conflicts with other programs. If real-time protection does not start, contact ESET Customer Care.

On-demand computer scan

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

ESET recommends that you run an on-demand computer scan at least once a month. You can configure scanning as a scheduled task from **Tools** > **Scheduler**.



Type of scan

Two types of on-demand computer scans are available. **Smart scan** quickly scans the system with no need to further configure scan parameters. **Custom scan** enables you to select any of the predefined scan profiles and choose specific scan targets.

Smart scan

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

Custom scan

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

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

Custom scan

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

Scan targets

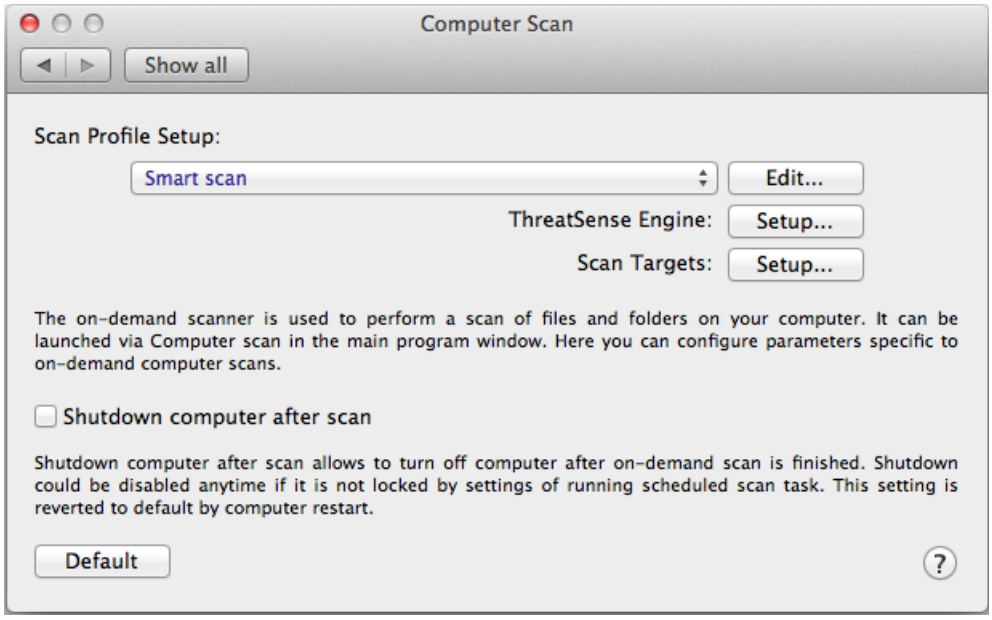
The **Scan targets** tree structure enables you to select files and folders to be scanned for viruses. Folders may also be selected according to a profile's settings.

You can define a scan target more precisely by typing the path to the folder or files you want to include in scanning. Select targets from the tree structure that lists all available folders on the computer by selecting the check box that corresponds to a given file or folder.

Scan profiles

You can save your preferred scan settings for future scanning. ESET recommends that you create a different profile (with various scan targets, scan methods, and other parameters) for each regularly used scan.

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



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

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

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

ThreatSense engine parameters setup

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

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

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

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

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

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

Objects

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

- **Symbolic links** - (Computer scan only) scans files that contain a text string that is interpreted and followed by the operating system as a path to another file or directory.
- **Email files** - (Not available in Real-time Protection) scans email files.
- **Mailboxes** - Nnot available in Real-time Protection) scans user mailboxes in the system. Incorrect use of this option may cause 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`, and so on).

- **Self-extracting archives** - (Not available in Real-time Protection) scans files which are contained in self-extracting archive files.
- **Runtime packers** - uUnlike standard archive types, runtime packers decompress in memory. When you select this option, standard static packers (for eample, UPX, yoda, ASPack, and FGS) are also scanned.

Options

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

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

Cleaning

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

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

Archive files

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

Archive scanning

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

Exclusions

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

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

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

- *log*
- *cfg*
- *tmp*

Limits

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

- **Maximum Size:** Defines the maximum size of objects to be scanned. Once the maximum size is defined, the antivirus module scans only objects smaller than the size specified. This option should only be changed by advanced users who have specific reasons to exclude larger objects from scanning.
- **Maximum Scan Time:** Defines the maximum time allotted to scan an object. If a user-defined value is entered here, the antivirus module stops scanning an object when that time is elapsed, regardless of whether the scan is finished.
- **Maximum Nesting Level:** Specifies the maximum depth of archive scanning. ESET does not recommend changing the default value of 10. Under normal circumstances there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive remains unchecked.
- **Maximum File Size:** Specifies the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If scanning is prematurely terminated as a result of this limit, the archive remains unchecked.

Other options

Following are other options you can specify:

- **Enable Smart Optimization.** With Smart Optimization enabled, settings are optimized to ensure the most efficient level of scanning without compromising scanning speed. The various protection modules scan intelligently, using different scanning methods. Smart Optimization is not rigidly defined within the product. ESET is continuously implementing new changes that are integrated into ESET Cyber Security 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 used by the file system are file and folder associations that are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.

Infiltrations

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

If your computer is showing signs of malware infection, for example, running slower, freezing often, and so on, ESET recommends taking the following steps:

1. Click **Computer scan**.
2. Click **Smart scan** (for more information, see Smart scan).
3. After the scan is 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 be scanned for viruses.

As a general example of how infiltrations are handled by ESET Cyber Security, suppose that an infiltration is detected by the real-time file system monitor using the default cleaning level. Real-time protection tries to clean or delete the file. If no predefined action is available for the Real-time protection module, you are prompted to select an option in an alert window. Usually, the options **Clean**, **Delete**, and **No action** are available. Selecting **No action** is not recommended, because infected files are left in the infected state. This option is intended for when you are sure that a file is harmless and has been detected by mistake.

Cleaning and deleting

Apply cleaning if a file is attacked by a virus that has attached malicious code to it. If this is the case, first try to clean the infected file 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 is deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. However, use caution when performing a **Strict cleaning** scan. With Strict cleaning, the archive is deleted if it contains at least one infected file, regardless of the status of other files in the archive.

Removable media scanning and blocking

ESET Cyber Security can run an on-demand scan of inserted removable memory devices (CD, DVD, USB, and so on). On macOS 10.15, ESET Cyber Security can also other external media devices.

> **Removable media scanning on macOS 11 and later**
> ESET Cyber Security installed on macOS 11 and later scans only memory devices.

Removable media may contain malicious code and put your computer at risk. To block removable media, click **Media blocking setup** (see the picture above) or from the main menu click **Setup** > **Enter application preferences** > **Media** from the main program window and select **Enable removable media blocking**. To enable access to certain types of media, deselect your desired media volumes.

> **CD-ROM access**
> To enable access to external CD-ROM drive connected to your computer via USB cable, deselect the **CD-ROM** option.

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. Find more information about phishing in ESET Glossary.

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

To test whether the Anti-Phishing is working, refer to the AMTSO test page.

Web and Email protection

To access web and mail protection from the main menu, click **Setup** > **Web and Email**. From here you can also access detailed settings for each module by clicking **Setup**. The following protection is available:

- **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 web sites or domains.

Scanning exceptions
ESET Cyber Security does not scan the encrypted protocols HTTPS, POP3S, and IMAPS.

Web protection

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

You can achieve web filtering by defining the port numbers for HTTP communication and URL addresses.

Ports

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

URL lists

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

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

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**.

In any list, you can use the special symbols *(asterisk) and ?(question mark). The asterisk substitutes any string of characters, and the question mark substitutes any symbol. Take particular care when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, you should ensure that the symbols * and ? are used correctly in this list.

Email protection

Email protection provides control of email communications received through the POP3 and IMAP protocols. When examining incoming messages, ESET Cyber Security uses all of the advanced scanning methods included in the ThreatSense scanning engine. POP3 and IMAP protocol communications scanning is independent of the email client used. The following settings are available:

- **ThreatSense Engine: Setup** – Advanced scanner setup enables you to configure scan targets, detection methods, and so on. Click **Setup** to display the detailed scanner setup window.

- **Append tag message to email footnote** – After an email is scanned, a notification containing the scan results can be appended to the message. Tag messages are a useful tool, but should not be used as the final determination of message safety, since they may be omitted in problematic HTML messages and can be forged by certain threats. The following options are available:
  - **Never** – No tag messages are added to any email.
  - **To infected email only** – Only email containing malware is tagged as checked.
  - **To all scanned email** – All scanned email is appended with tag messages.
- **Append note to the subject of received and read infected email** – Select this check box if you want email protection to include a threat 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. Following are the fields you can add:
  - %avstatus% - Adds the email infection status (for example: clean, infected, and so on).
  - %virus% - Adds the name of the threat.
  - %product% - Adds the name of your ESET product (in this case, ESET Cyber Security).
  - %product_url% - Adds the ESET web site link (www.eset.com).

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

- POP3 protocol checking
- IMAP protocol checking

POP3 protocol checking

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

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

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

IMAP protocol checking

The Internet Message Access Protocol (IMAP) is another Internet protocol for e-mail retrieval. IMAP has some advantages over POP3. For example, multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether the message has been read, replied to, or deleted. ESET Cyber Security provides protection for this protocol, regardless of the email client.

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

separated by a comma.

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

Update

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

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

Under normal circumstances, when updates download properly, the message "Update is not necessary - the installed modules are up to date" is displayed in the Update window. However, if modules cannot be updated, ESET recommends that you check the update settings. The most common reason for this error is incorrectly entered authentication data (license key) or incorrectly configured connection settings.

The update window also contains the detection engine version number. The version number links to ESET's web page that lists the detection engine update information.

Automatic upgrades

ESET Cyber Security does not upgrade automatically to the newest version. ESET Cyber Security notifies you when a new upgrade is available. To install the upgrade, you must approve the upgrade manually. You can find more information in the Upgrading topic.

Update setup

To delete all temporarily stored update data, click **Clear** next to **Clear Update Cache**. Use this option if you experience difficulty while updating.

Advanced options

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

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

ESET Cyber Security records snapshots of detection and program modules for use with the **Update Rollback** feature. Leave **Create module snapshots** enabled to have ESET Cyber Security record these snapshots automatically. If you suspect that a new detection or program module update is unstable or corrupt, use the rollback feature to revert to a previous version and disable updates for a set period of time. To revert updates to the oldest version in history, click **Rollback**. Alternatively, you can re-enable previously disabled updates.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 that you want to suspend updates. If you select **until revoked**, normal updates will not resume until you restore them manually. To restore updates manually click **Allow**. 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 seven days.

Create update tasks

Click **Update** from the main menu and then click **Update modules** to trigger updates manually.

You can also run updates as scheduled tasks by clicking **Tools** > **Scheduler**. By default, the following tasks are activated in ESET Cyber Security:

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

You can modify each update task to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see the Scheduler section.

Upgrade ESET Cyber Security to a new version

For maximum protection, it is important to use the latest build of ESET Cyber Security. To check for a new version, click **Home** from the main menu. If a new build is available, a message is displayed. Click **Learn more** to display a new window containing the version number of the new build and the change log.

Click **Yes** to download the latest build or click **Not now** to close the window and download the upgrade later.

If you click **Yes**, the file is downloaded to your downloads folder (or the default folder set by your browser). When the file finishes downloading, launch the file and follow the installation directions. Your username and password are automatically transferred to the new installation. ESET recommends that you check for upgrades regularly, especially when installing ESET Cyber Security from a CD or DVD.

System updates

The macOS system updates feature is an important component designed to protect users from malicious software. For maximum security, ESET recommends that you install these updates as soon as they become available. ESET Cyber Security notifies you about missing updates according to the level you specify. You can adjust the availability of update notifications in **Setup** > **Enter application preferences** (or press *cmd+,*) > **Alerts and notifications > Setup** by changing the **Display Conditions** options next to the **Operating system updates**. The following settings are available:

- **Show all updates** - A notification is displayed any time a system update is missing.
- **Show only recommended** - A notification is displayed 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 click **Install the missing update** to run the update directly from the notification window or the **Home** section of ESET Cyber Security.

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 system security and stability.
- **[restart]** - A computer restart is required after the installation.
- **[shutdown]** - The computer must be shut down and then powered back on following the 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. To install all available updates displayed in the **Missing system updates** window and also those not displayed by the Software updates application, you must 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.

Tools

The **Tools** menu includes modules that help simplify program administration and offer additional options for advanced users. This menu includes the following tools:

- Log files
- **Protection statistics.** This tool displays statistics from multiple types of protection. Click the drop-down menu to select from the following protection statistics:

- Antivirus protection summary (this is selected by default)
- On-demand scan graph
- Real-time protection graph
- Email client protection graph
- Web access protection graph

The Antivirus protection summary shows statistics from the last active scan. Other protection types statistics are shown from the last computer restart (or restart of ESET Cyber Security. Click **Reset** under a statistic to clear it manually.

- Scheduler
- Quarantine
- Running processes
- Submit sample for analysis

Log files

The log files contain information about important program events and provide an overview of detected threats. Logging is essential for system analysis, threat detection, and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on current log verbosity settings. You can view text messages and logs directly from the ESET Cyber Security environment, and you can archive logs.

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

- **Detected threats** – Use this option to view all information about events related to the detection of infiltrations.
- **Events** – This option is designed to help system administrators and users solve problems. All important actions performed by ESET Cyber Security are recorded in event logs.
- **Computer scan** – The results of all completed scans are displayed in this log. Double-click any entry to view details for the respective on-demand computer scan.
- **Filtered websites** – Use this option to view a list of web sites that were blocked by Web access protection. In these logs you can see the time, URL, status, IP address, user, and application that opened a connection to a particular web site.

In each section, you can copy displayed information directly to the clipboard by selecting the entry and clicking **Copy**.

Log maintenance

The logging configuration for ESET Cyber Security is accessible from the main program window. Click **Setup** > **Enter application preferences** (or press *cmd+,*) > **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 (90 days by default).
- **Optimize log files automatically** - Automatic defragmentation of log files occurs if the specified percentage of unused records is exceeded (25% by default).

You can store all the relevant information displayed in the user interface, threat, and event messages in as plain text or CSV (Comma-separated values) format. 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 log files are saved, click **Setup** next to **Advanced Options**.

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

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

To configure the filters for **Default Computer Scan Log Records**, click **Edit** and select or deselect log types as required. More explanation about these log types is in Log Filtering.

Log filtering

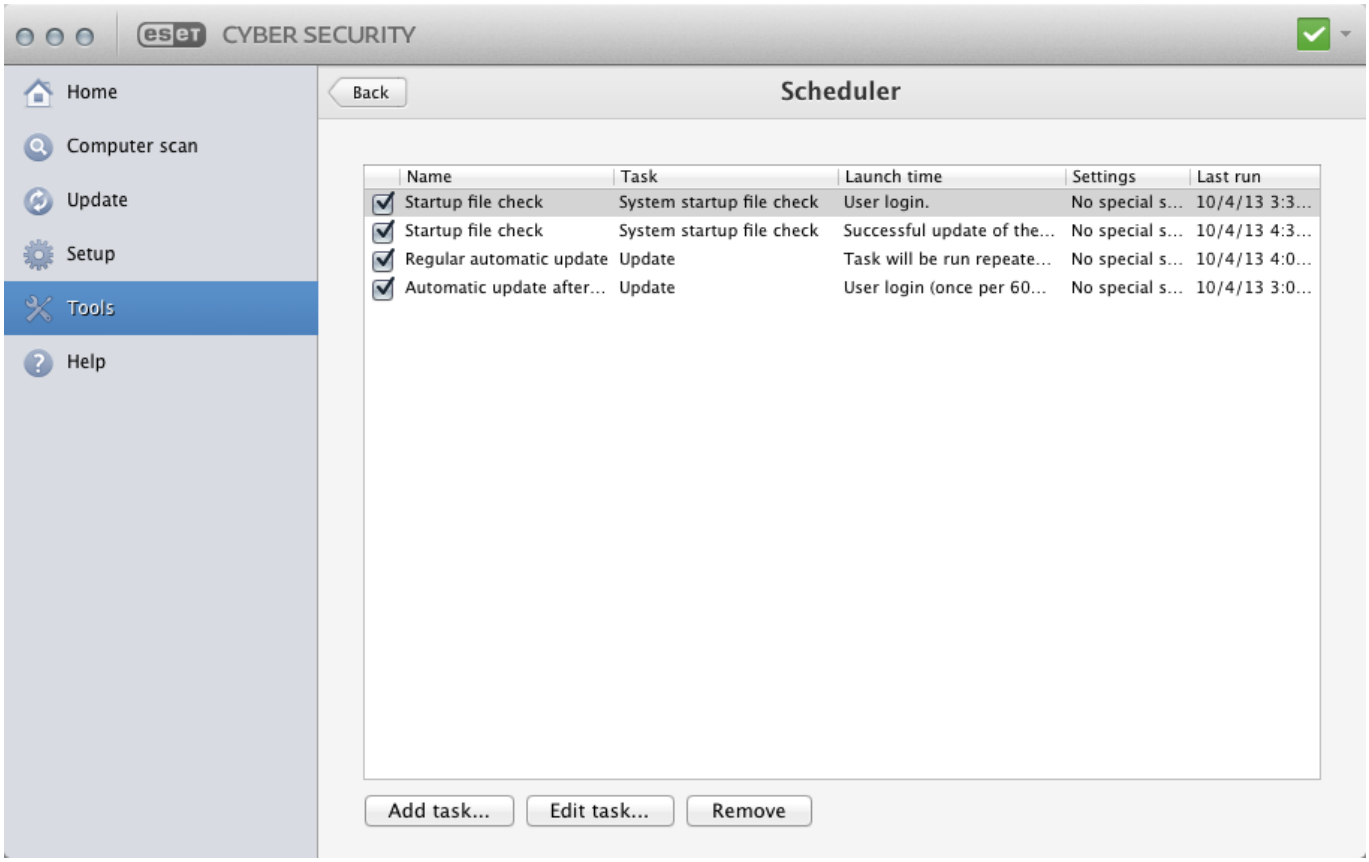
Logs store information about important system events. The log filtering feature enables you to display records about a specific type of event.

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, and so on
- **Diagnostic records** - information needed to fine-tune the software and the records described above.

Scheduler

You can find the **Scheduler** in the ESET Cyber Security main menu under **Tools**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile.



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

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

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

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

Creating new tasks

To create a new task in the **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**

Run application

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. To change the user from the default, type the username followed by a colon (:) in front of the command. You can also use the **root** user in this feature.

Example: Run a task as a user

To schedule the Calculator application to start at a selected time as a user named **UserOne**:

1. In the **Scheduler**, select **Add task**.
2. Type the task name. Select **Run application** as a **Scheduled task**. In the **Run Task** window, select **Once** to run this task one time. Click **Next**.
3. Click Browse and select the Calculator application.
4. Type **UserOne:** before the application path (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') and click **Next**.
5. Select a time to execute the task and click **Next**.
6. Select an alternate option if the task cannot run and click **Next**.
7. Click **Finish**.
8. The **Scheduler** starts the Calculator application at the time you selected.

Example: Create an update task

To create an update task to run at a specified time:

1. From the **Scheduled task** drop-down menu, select **Update**.
2. Type the name of the task into the **Task name** field.
3. Select the frequency of the task from the **Run task** drop-down menu. Based on the frequency selected, you are prompted to specify different update parameters. If you select **User-defined**, you are prompted to specify the date and time in cron format (see the Creating user-defined task section for more details).
4. Define what action to take if the task cannot be performed or completed at the scheduled time.
5. In the last step, a summary window with information about the current scheduled task is displayed. Click **Finish**. The new scheduled task is added to the list of currently scheduled tasks.

By default, ESET Cyber Security contains predefined scheduled tasks to ensure correct product functionality. These tasks should not be altered, and are hidden by default. To make these tasks visible, from the main menu click **Setup** > **Enter application preferences** (or press *cmd+,*) > **Scheduler** and select **Show system tasks**.

Scanning as a directory owner

You can scan directories as the owner of the directory:

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -
f %u "$VOLUME"` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -
f /tmp/scan_log "$VOLUME"; done
```

You can also scan the `/tmp` folder as a currently logged-in user:

```
root:sudo -u \#`stat -
f %u /dev/console` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan'
 /tmp
```

Creating user-defined tasks

You must enter the date and time of a **User-defined** task in year-extended cron format (a string containing 6 fields, with each field separated by a space as follows):

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

Example:

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

Special characters supported in cron expressions are:

- asterisk (`*`) - Matches all values of a field. For example, an asterisk in the third field (day of the month) means every day.
- hyphen (`-`) - Defines ranges, for example, `3-9`.

- comma (`,`) - Separates list items, for example: `1,3,7,8`.
- slash (`/`) - Defines increments of ranges. For example, `3-28/5` in the third field (day of the month) means the 3rd day of the month and then every 5 days.

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

> **Executing commands**
> If you define both the day of the month and the day of the week, the command is executed only when both fields match.

Quarantine

The main purpose of the quarantine is to safely store infected files. You should quarantine files if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by ESET Cyber Security.

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

You can view files stored in the quarantine folder in a table that displays the date and time of the quarantine, the path to the original location of the infected file, the size in bytes, the reason (for example, added by a user) and the number of threats (for example, if it is an archive containing multiple infiltrations). The quarantine folder with quarantined files () remains in the system even after removing ESET Cyber Security. Quarantined files are stored in a safe encrypted form and can be restored again after installing ESET Cyber Security.

Quarantine files

ESET Cyber Security automatically quarantines deleted files (if you have not deselected this option in the alert window). Click **Quarantine** to quarantine any suspicious file manually . You can also use the context menu for this purpose. CTRL+click the blank field, select **Quarantine**, select a file you want to quarantine, and click **Open**.

Restore from the quarantine

Select a quarantined file and click **Restore** to restore the file to its original location. This capability is also available from the context menu. CTRL+click a given file on the **Quarantine** window and click **Restore**. The context menu also offers the option **Restore to**, which enables you to restore a file to a location other than the one from which it was deleted.

Submit a file from the quarantine

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

Running processes

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

- **Process** – The name of the process currently running on your computer. To see all running processes you can also use the Activity Monitor (found in */Applications/Utilities*).
- **Risk level** – In most cases, ESET Cyber Security and ESET Live Grid technology assign risk levels to objects (files, processes, and so on) using a series of heuristic rules that examine the characteristics of each object and weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level. Known applications marked green are definitely clean (whitelisted) and are excluded from scanning. This exclusion improves the speed of on-demand and real-time scans. When an application is marked as unknown (yellow status), the application is not necessarily malicious software. Usually the application is just a newer software. 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 is added to one of the upcoming product updates.
- **Number of Users** – The number of users who use a given application. This information is gathered by ESET Live Grid technology.
- **Time of discovery** – The period of time since the application was discovered by ESET Live Grid technology.
- **Application Bundle ID** – The name of the vendor or application process.

Clicking a given process displays the following at the bottom of the window:

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

Network Connections

Network Connections is a list of active network connections within your computer. ESET Cyber Security provides detailed information about each connection and enables you to create a rule to block these connections.

ESET Cyber Security enables you to create blocking rule for each connection in **Network Connections** manager. You can create blocking rule by right-clicking on a connection and selecting **Create blocking rule for this connection**.

To create a blocking rule:

1. Select the connection **Profile** you want to create the rule for and type the name of the rule. Select the application the rule should apply to, or select the check-box to apply the rule to all applications.
2. Select an action for the connection, either to deny (block) the connection or allow it. Select the direction

of communication to which the rule should apply. You can also create a log file for a rule by clicking **Log rule**.

3. Select the connection protocol and port types. Select a port for service or specify a range of ports using the format: from-to.

4. Select the destination and type the information in the required field, depending on your destination.

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 ESET can offer you. The best way to ensure that ESET sees new threats as soon as they appear is for ESET to “link“ to as many ESET customers as possible and use them as threat scouts. There are two options:

- You can choose not to enable the Live Grid Early Warning System. You will not lose any functionality from your software, and you will still receive the best protection that ESET offers.
- 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 helps ESET update its detection engine and improve the program's threat detection ability.

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

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

To access Live Grid setup from the main menu, click **Setup** > **Enter application preferences** (or press *cmd+,*) > **Live Grid**. Select **Enable Live Grid Early Warning System** to activate Live Grid and then click **Setup** located next to **Advanced Options**.

Live Grid setup

By default, ESET Cyber Security is configured to submit suspicious files to the ESET Threat Lab for detailed analysis. If you do not want to submit these files automatically, deselect **Submit files**.

If you find a suspicious file, you can submit it to the ESET Threat Lab for analysis by clicking **Tools** > **Submit sample for analysis** from the main program window. If an application is malicious, its detection is added to an upcoming product update. The following settings are available:

- **Submit anonymous statistics** – 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.
- **Exclusion Filter** – This option enables 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 (for example, `.doc` and `.rtf`.). You can add file types to the list of excluded files.

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

Submit sample for analysis

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

Before submitting samples to ESET

Do not submit a sample unless it meets at least one of the following criteria:
• The sample is not detected by your ESET product at all.
• The sample is incorrectly detected as a threat.
• The sample is not a personal file. ESET does not accept your personal files (that you would like to scan for malware by ESET) as samples (ESET Research Lab does not perform on-demand scans for users).
• Your email has a descriptive subject line and includes as much information about the file as possible (for example, a snapshot of the screen or the web site you downloaded the file from).

To send a sample submission, use the sample submission form in your product, located in **Tools** > **Submit sample for analysis**.

In the **Submit sample for analysis** form, specify the following:

• **File** – The path to the file you intend to submit.

• **Comment** – The rreason why you are submitting the file.

• **Contact email** – This contact email address that is sent along with the suspicious files to ESET and may be used to contact you if more information is required for analysis. Including a contact email address is optional.

You may not get a response from ESET

You will not get a response from ESET unless more information is required from you. Each day our servers receive tens of thousands of files, making it impossible to reply to all submissions.
If the sample turns out to be a malicious application or web site, its detection will be added to an upcoming ESET product update.

User interface

The user interface configuration options enable you to adjust the working environment to fit your needs. These options are accessible from the main menu by clicking **Setup** > **Enter application preferences** (or press *cmd+,*) > **Interface**. The following options are available:

• To display the ESET Cyber Security splash screen at the system startup, select **Show splash-screen at startup**.

• **Present application in Dock** enables you to display the ESET Cyber Security icon in the macOS Dock and switch between ESET Cyber Security and other running applications by pressing *cmd+tab*. Changes take effect after you restart ESET Cyber Security (the changes are usually triggered by a computer restart).

- The **Use standard menu** option enables you to use certain keyboard shortcuts (see Keyboard shortcuts) and see standard menu items (User interface, Setup, and Tools) on the macOS Menu Bar (at the top of the screen).
- To enable tooltips for certain options of ESET Cyber Security, select **Show tooltips**.
- **Show hidden files** enables you to see and select hidden files in the **Scan Targets** setup of a **Computer scan**.
- By default, the ESET Cyber Security icon is displayed in the Menu Bar Extras at the right of the macOS Menu Bar (at the top of the screen). To disable this setting, deselect **Show icon in menu bar extras**. This change takes effect after you restart ESET Cyber Security (the change is usually triggered by a computer restart).

Alerts and notifications

The **Alerts and notifications** section enables you to configure how threat alerts and system notifications are handled by ESET Cyber Security.

Disabling **Display alerts** disables all alert windows and is only recommended in specific situations. For most users, ESET recommends that this option be left at its default setting (enabled). Advanced options are described in this chapter.

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

Since ESET Cyber Security version 6.2, you can also prevent certain **Protection statuses** from being displayed on the program's main screen (**Protection status** window). To learn more about this, see the Protection statuses.

Display alerts

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

List of Dialogs (**Setup** > **Enter application preferences** > **Alerts and notifications** > **Setup**) shows the list of all alert dialogs triggered by ESET Cyber Security. To enable or suppress each notification, select the check box left of the **Dialog Name**. In addition, you can define **Display Conditions** under which notifications about new program versions and operating system updates are displayed.

Protection statuses

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

You can hide the protection statuses of the following program features:

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

Privileges

ESET Cyber Security settings can be important to your organization's security policy. Unauthorized modifications may endanger the stability and protection of your system. For this reason, you can define which users have permission to edit the program configuration.

To specify privileged users, click **Setup** > **Enter application preferences** (or press *cmd+,*) > **Privileges**. Select the users or groups from the list on the left and click **Add**. To display all system users and groups, select **Show all users/groups**. To remove a user, select a name from the **Selected Users** list on the right and click **Remove**.

About upgrading

If you leave the **Selected Users** list empty, all users are considered privileged.

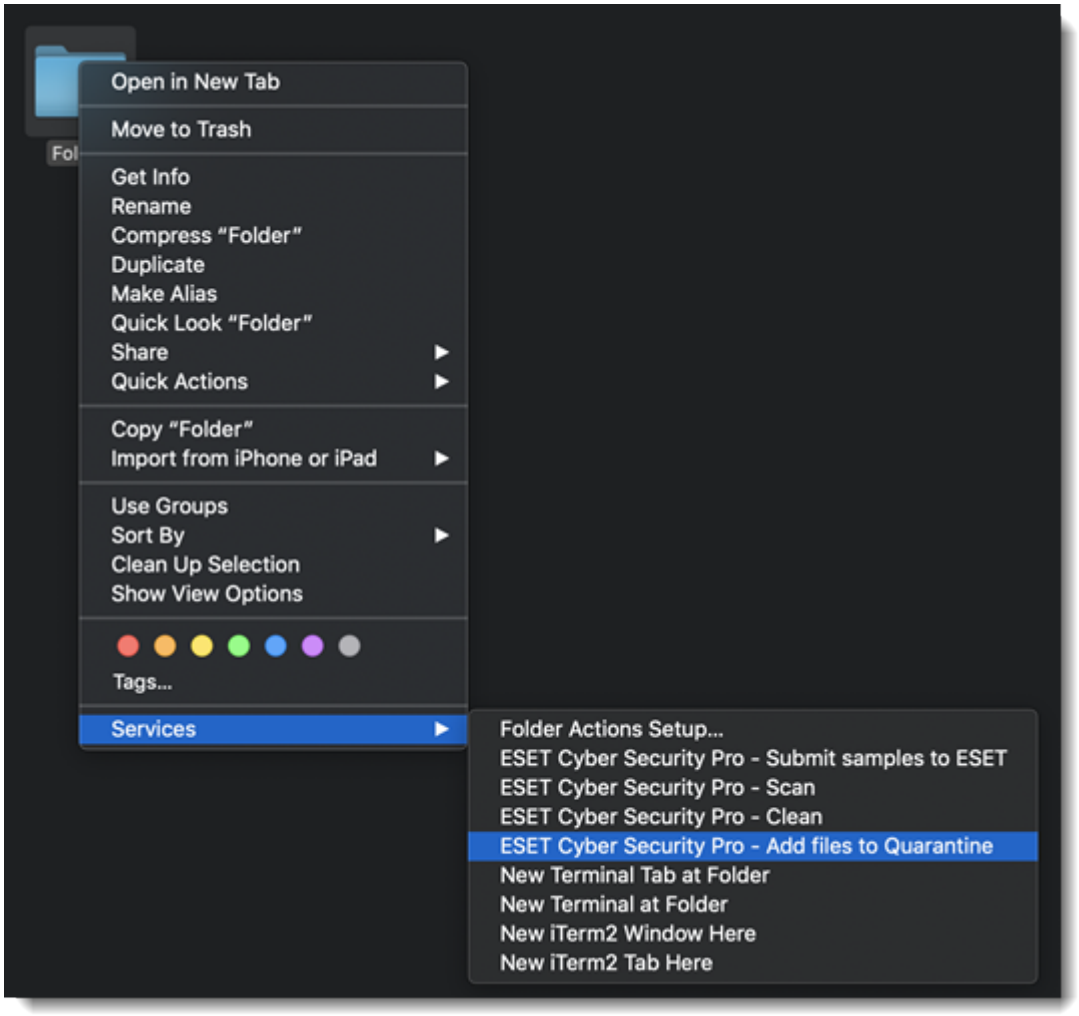
Context menu

Context menu integration can be enabled by clicking **Setup** > **Enter application preferences** (or press *cmd+,*) > **Context Menu** section by selecting the **Integrate into the context menu** option. Logging out or restarting the computer is required for changes to take effect. Context menu options will be available in the **Finder** window when you CTRL+click on any file.

You can select options that will be shown in the context menu. You can display the **Only scan** option, which enables you to scan the selected file. The **Only clean** option enables you to clean the selected file from the context menu. Apply cleaning if a file has been attacked by a virus that has attached malicious code to it. If this is the case, first try to clean the infected file to restore it to its original state. If the file consists exclusively of malicious code, it is deleted.

If you select the **All** option, you can perform following tasks from the context menu:

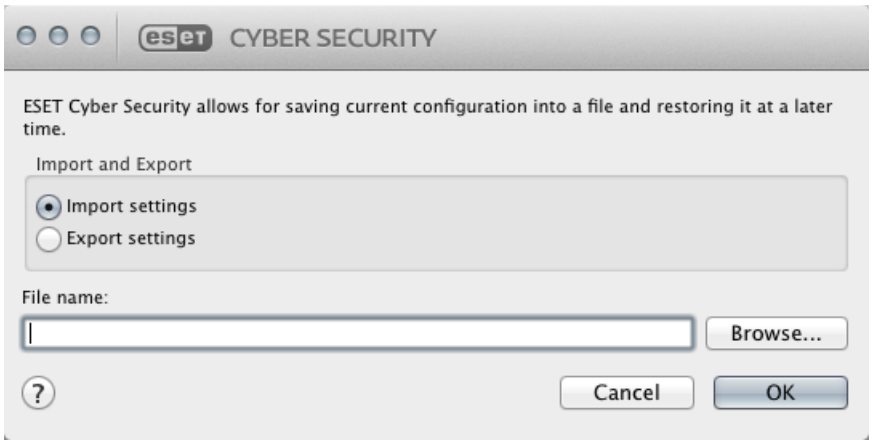
- Submit samples to ESET
- Scan
- Clean
- Add files to the quarantine



Import and export settings

To import an existing configuration or export your ESET Cyber Security configuration, click **Setup** > **Import or export settings**.

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



To import a configuration, select **Import settings** and click **Browse** to navigate to the configuration file you want

to import. To export, select **Export settings** and use the browser to select a location on your computer to save the configuration file.

Proxy server setup

You can configure proxy server settings in **Setup** > **Enter application preferences** (or press *cmd+,*) > **Proxy Server**. Specifying the proxy server at this level defines global proxy server settings for all ESET Cyber Security functions. Parameters defined here are used by all modules that require a connection to the internet. ESET Cyber Security supports the Basic Access and NTLM (NT LAN Manager) types of authentication.

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

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

End User License Agreement

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement (hereinafter referred to as "the Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement. If You do not agree to all of the terms and conditions of this Agreement, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any

attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software (hereinafter referred to as " Documentation "); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smart phones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights (hereinafter referred to as "License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one computer system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as "MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent in which has the right to use the Software in accordance the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Business Edition.** A Business Edition version of the Software must be obtained to use the Software on mail servers, mail relays, mail gateways or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** OEM Software shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall be also entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

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

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled automatic installation of Updates. For the purpose of provisioning of Updates, License authenticity verification is required including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

b) **Forwarding of infiltrations and information to the Provider.** The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames (hereinafter referred to as "Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed, information about the operations and functionality of the Software and information about devices in local network such as type, vendor, model and/or name of device (hereinafter referred to as "Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own

means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer. You hereby agree to receive notification and messages including but not limited to marketing information.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival back-up copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property

rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement**. This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all back-up copies and all related materials provided by the Provider or its business partners. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if

running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software**. The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any act, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

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

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

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

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

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

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

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

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

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. In case of a discrepancy between language versions of this Agreement, the English version shall prevail. This Agreement may only be modified in written form, signed by an authorized representative of the Provider, or a person expressly authorized to act in this capacity under the terms of a power of attorney.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

EULA ID: HOM-ECS-20-01

Privacy Policy

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

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

Processing of Personal Data

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

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

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

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

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or

another appropriate safeguard must be established without any exception.

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

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

Data Subject's Rights

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

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

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

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