ESET CYBER SECURITY

for Mac

Installation Manual and User Guide

Click here to download the most recent version of this document

ESET **CYBER SECURITY**

Customer Care: www.eset.com/support

REV. 11. 1. 2013

Contents

1. 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 that is 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 are capable of proactively eliminating infiltration by viruses, worms, trojan horses, spyware, adware, rootkits and other Internet-borne attacks without hindering system performance.

1.1 What's new

Email client protection
Email protection provides control of email communication received through the POP3 and IMAP protocols.

Removable media scanning
ESET Cyber Security offers on-demand scanning of removable media devices (CD, DVD, USB, iOS device etc.).

Join ESET Live Grid network
Built on the ThreatSense.NET advanced early warning system, ESET Live Grid is designed to provide additional levels of security for your computer. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. Additionally, your system scans are processed faster and more precisely as the ESET Live Grid database grows over time. This allows us to offer stronger proactive protection and faster scanning to all ESET users. We recommend that you activate this feature and we thank you for your support.

New design
The main window of ESET Cyber Security has been completely redesigned and advanced settings (Preferences) are now more intuitive for easier navigation.

1.2 System requirements

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

	System requirements
Processor architecture	32bit, 64bit Intel®
Operating system	Mac OS X 10.6 or later
Memory	300 MB
Free disk space	150 MB

2. Installation

Before you begin the installation process, please close all open programs on your computer. ESET Cyber Security contains components that may conflict with other antivirus programs that may already be installed on your computer. 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 the installation CD/DVD, insert it into your computer, open it from your Desktop or **Finder** window and double-click the **Install** icon
- If you are installing from a file downloaded from the ESET website, open the file and double-click the **Install** icon

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

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

- Typical installation 4
- Custom installation 5

2.1 Typical installation

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

Live Grid
The Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed, processed and added to the virus signature database. **Enable Live Grid Early Warning System** is selected by default. Click **Setup...** to modify detailed settings for the submission of suspicious files. For more information see Live

Grid 17.

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

After installing ESET Cyber Security, you should perform a computer scan for malicious code. From the main program window click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see the section On-demand computer scan 8.

2.2 Custom installation

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

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

Live Grid
The Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed, processed and added to the virus signature database. **Enable Live Grid Early Warning System** is selected by default. Click **Setup...** to modify detailed settings for the submission of suspicious files. For more information see Live Grid 17.

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

After installing ESET Cyber Security, you should perform a computer scan for malicious code. From the main program window click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see the section On-demand computer scan 8.

3. Product activation

After installation, the **Product Activation Type** window is displayed automatically. To access the product activation dialog at any time, click the ESET Cyber Security icon located in your menu bar (top of the screen) and then click **Product activation...**.

1. If you purchased a retail boxed version of the product, select **Activate using an Activation Key**. The Activation Key is usually located inside of or on the back of the product package. For a successful activation, the Activation Key must be entered as supplied.

2. If you received a Username and Password, select **Activate using a Username and Password** and enter the license data in the appropriate fields. You can also enter your license data by clicking **Username and Password setup ...** from the program **Update** window.

3. If you would like to evaluate ESET Cyber Security before making a purchase, select **Activate Trial License**. Fill in your email address to activate ESET Cyber Security for a limited time. Your test license will be emailed to you. Trial licenses can only be activated once per customer.

If you choose not to activate at this time, click **Activate Later**. You can activate ESET Cyber Security directly from the **Home** or **Update** section of ESET Cyber Security main program window.

If you do not have a license and would like to buy one, click **License**. This will redirect you to the website of your local ESET distributor.

4. Uninstallation

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

- insert the ESET Cyber Security installation CD/DVD into your computer, open it from your desktop or **Finder** window and double-click **Uninstall**
- 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 **Resources** folder and double-click the **Uninstaller** icon.

5. 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 to the option selected from the main menu on the left.

The following sections are accessible from the main menu:

- **Home** – provides information about the protection status of your Computer, Web and Mail protection.
- **Computer scan** – this section allows you to configure and launch the On-demand computer scan 8.
- **Update** – displays information about updates of the virus signature database.
- **Setup** – select this section to adjust your computer's security level.
- **Tools** – provides access to Log files 14, Scheduler 15, Quarantine 16, Running processes 16 and other program features.
- **Help** – displays access to help files, Internet Knowledgebase, support request form and additional program information.

5.1 Keyboard shortcuts

Keyboard shortcuts that can be used when working with ESET Cyber Security:

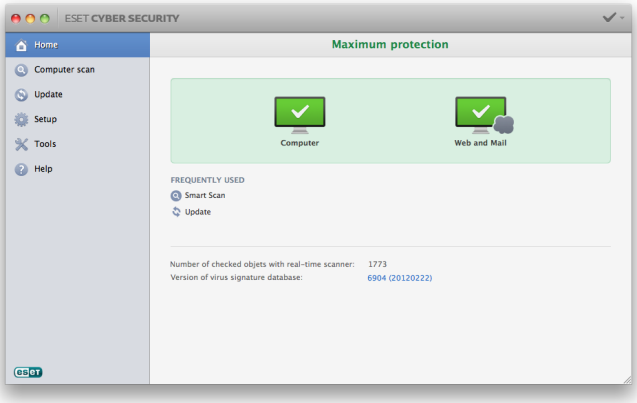
- *cmd-,* – displays ESET Cyber Security Preferences,
- *cmd-U* – opens the **Username and Password Setup** window,
- *cmd-alt-T* – opens the **Special Characters** window,
- *cmd-O* – resizes the ESET Cyber Security main GUI window to the default size and moves it to the center of the screen,
- *cmd-alt-H* – hides all open windows except ESET Cyber Security,
- *cmd-H* – hides ESET Cyber Security.

The following keyboard shortcuts work only if the **Use standard menu** option is enabled in **Setup** > **Enter application preferences ...** (or press *cmd-,*) > **Interface**:

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

5.2 Checking protection status

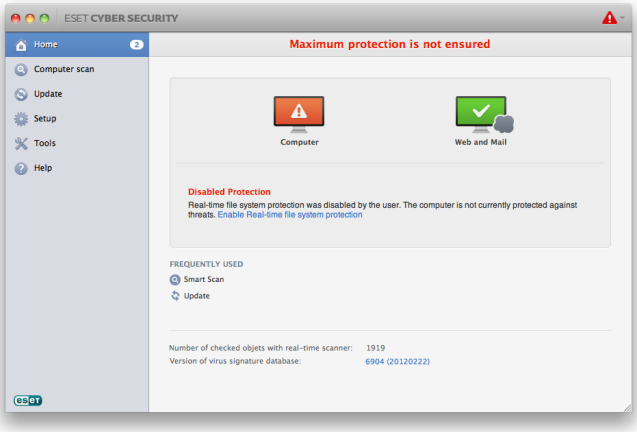
To view your protection status click **Home** from the main menu. A status summary about the operation of ESET Cyber Security modules will be displayed in the primary window.



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



6. Computer protection

Computer configuration can be found in **Setup** > **Computer**. It 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...**.

6.1 Antivirus and antispyware protection

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

6.1.1 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 the section titled ThreatSense engine parameter setup 9), Real-time file system protection may vary for newly created files and existing files. For newly created files, it is possible to apply a deeper level of control.

By default, Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (e.g., if there is a conflict with another Real-time scanner), Real-time protection can be terminated by clicking the ESET Cyber Security icon located in your menu bar (top of the screen) and then selecting **Disable Real-time File System Protection**. Real-time file system protection can also be disabled from the main program window (click **Setup** > **Computer** and switch **Real-time file system protection** to **DISABLED**).

To modify advanced settings for Real-time file system protection, go to **Setup** > **Enter application preferences ...** (or press *cmd-,*) > **Real-Time Protection** and click **Setup...** next to **Advanced Options** (described in the section titled Advanced scan options 7).

6.1.1.1 Scan on (Event triggered scanning)

By default, all files are scanned upon file opening, file creation or file execution. We recommend that you keep these default settings, as they provide the maximum level of Real-time protection for your computer.

6.1.1.2 Advanced options

In this window you can define object types to be scanned by the ThreatSense engine and enable/disable **Advanced heuristics** as well as modify settings for archives and file cache.

We do not recommend changing the default values in the **Default archives settings** section unless this is necessary to resolve a specific issue, as higher archive nesting values can impede system performance.

You can toggle ThreatSense Advanced heuristics scanning for executed, created and modified files separately by selecting the **Advanced heuristics** checkbox in each of the respective ThreatSense parameters sections.

To minimize system footprint when using Real-time protection, you can define the size of the optimization cache. **Enable clean file cache** must be enabled for this setting to take effect. If **Enable clean file cache** is disabled, all files are scanned each time they are accessed. Files will not be scanned repeatedly after being cached (unless they have been modified), until the cache is full. Files are scanned again immediately after each virus signature database update. Click **Enable clean file cache** to enable/disable this function. To set the amount of files to be cached simply enter the desired value in the input field next to **Cache size**.

Additional scanning parameters can be set in the **ThreatSense Engine Setup** window. You can define what type of **Objects** should be scanned, using which **Options** and **Cleaning** level, as well as defining **Extensions** and file-size **Limits** for Real-time file system protection. You can enter the ThreatSense engine setup window by clicking **Setup...** next to **ThreatSense Engine** in the Advanced Setup window. For more detailed information about ThreatSense engine parameters see ThreatSense engine parameter setup 9.

6.1.1.3 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. We recommend that you only modify these parameters in specific cases. For example, a situation in which there is a conflict with a certain application.

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**).

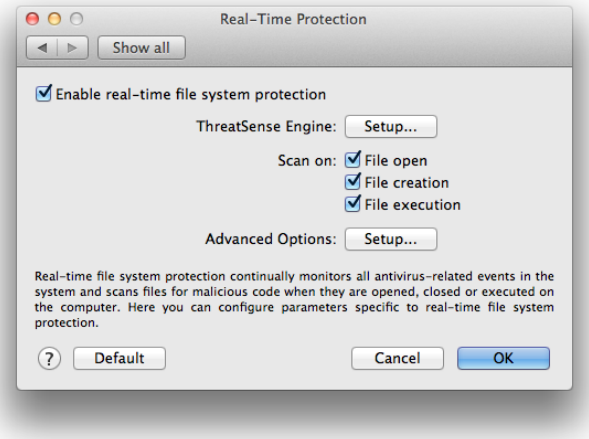
6.1.1.4 Checking Real-time protection

To verify that Real-time protection is working and detecting viruses, download the eicar.com test file and check to see 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.

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

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

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



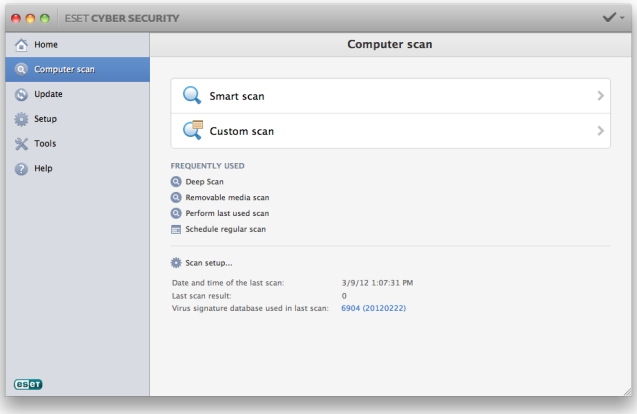
Real-time protection does not detect and clean infiltrations
Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs that may be on your system.

Real-time protection does not start
If Real-time protection is not initiated at system startup, it may be due to conflicts with other programs. If this is the case, please contact ESET Customer Care.

6.1.2 On-demand computer scan

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

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



You can also drag and drop selected files and folders from your Desktop or **Finder** window to the ESET Cyber Security main screen, dock icon, menu bar icon (top of the screen) or the application icon (located in the */Applications* folder).

6.1.2.1 Type of scan

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

6.1.2.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantage is easy operation with no detailed scanning configuration. Smart scan checks all files in all folders and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see the section on Cleaning 10.

6.1.2.1.2 Custom scan

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

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

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

6.1.2.2 Scan targets

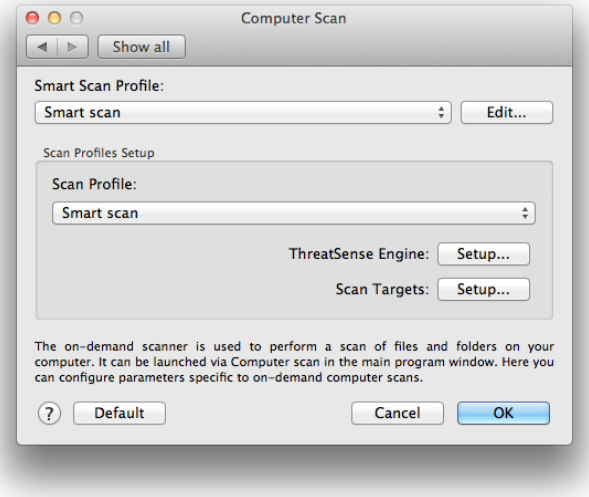
The Scan targets tree structure allows you to select files and folders to be scanned for viruses. Folders may also be selected according to a profile's settings.

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

6.1.2.3 Scan profiles

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

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



To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup 9 section for a description of each parameter of the scan setup.

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

6.1.3 Exclusions

This section (**Setup** > **Enter application preferences ...** > **Exclusions**) enables you to exclude certain files/folders, applications or IP/IPv6 addresses from scanning.

Files and folders listed in the **FileSystem** list will be excluded from all scanners: System (startup), Real-time and On-Demand.

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

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

6.1.4 ThreatSense engine parameters setup

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

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

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

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

- **System Protection** - Automatic startup file check
- **Real-Time Protection** - Real-time file system protection
- **Computer Scan** - On-demand computer scan.

The ThreatSense parameters are specifically optimized for each module, and their modification can significantly influence system operation. For example, changing settings to always scan runtime packers, or enabling advanced heuristics in the

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

6.1.4.1 Objects

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

- **Files** – scans all common file types (programs, pictures, audio, video files, database files, etc.).
- **Symbolic links** - (On-demand scanner 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** - (not available in Real-time protection) scans user mailboxes in the system. Incorrect use of this option may result in a conflict with your email client. To learn more about advantages and disadvantages of this option, read the following knowledgebase article.
- **Archives** - (not available in Real-time protection) scans files compressed in archives (.rar, .zip, .arj, .tar, etc.).
- **Self-extracting archives** - (not available in Real-time protection) scans files which are contained in self-extracting archive files.
- **Runtime packers** - unlike standard archive types, runtime packers decompress in memory. When this is selected, standard static packers (e.g. UPX, yoda, ASPack, FGS) are also scanned.

6.1.4.2 Options

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

- **Heuristics** – Heuristics use an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist, or was not included in the list of known viruses (virus signatures database).
- **Advanced heuristics** – Advanced heuristics is comprised of a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. The program's detection ability is significantly higher as a result of advanced heuristics.
- **Potentially unwanted applications** – These applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the way it behaved before these applications were installed). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.
- **Potentially unsafe applications** – These applications are commercial, legitimate software that can be abused by attackers if installed without user consent. This classification includes programs such as remote access tools, for this reason this option is disabled by default.

6.1.4.3 Cleaning

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

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

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

6.1.4.4 Extensions

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

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

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

6.1.4.5 Limits

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

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

6.1.4.6 Others

Enable Smart optimization
With Smart Optimization enabled, settings are optimized to ensure the most efficient level of scanning without compromising scanning speed. The various protection modules scan intelligently, making use of different scanning methods. Smart Optimization is not rigidly defined within the product. The ESET Development Team is continuously implementing new changes which are then integrated into ESET 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 (resource/data forks) used by the file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.

6.1.5 An infiltration is detected

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

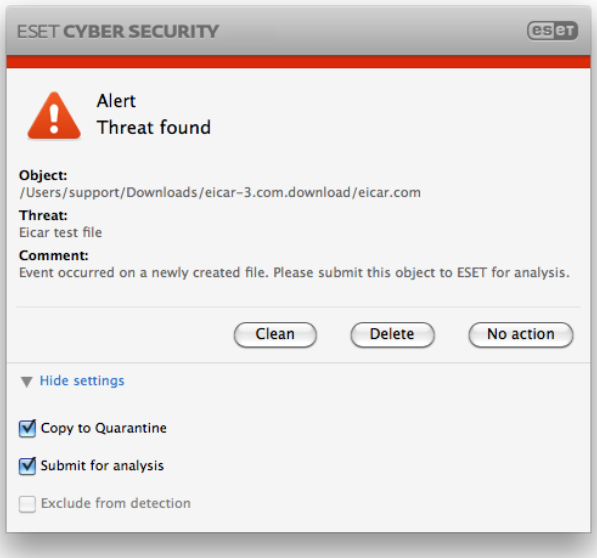
If your computer is showing signs of malware infection, for example it runs slower, often freezes, etc., we recommend that you take the following steps:

1. Click **Computer scan**.
2. Click **Smart scan** (for more information, see the Smart scan 8 section).
3. After the scan has finished, review the log for the number of scanned, infected and cleaned files.

If you only wish 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 will attempt to clean or delete the file. If there is no predefined action available for the Real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, since the infected file(s) is left in its infected state. This option is intended for situations when you are sure that the file is harmless and has been detected by mistake.

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



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

6.2 Removable media scanning and blocking

ESET Cyber Security can run an on-demand scan of inserted removable media devices (CD, DVD, USB, iOS device etc.).

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 allow access to certain types of media, deselect your desired media volumes.

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

7. Web and mail protection

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

Web access and phishing protection - if enabled (recommended), Real-time file system protection constantly monitors all antivirus related events.

Email client protection - provides control of email communication received through POP3 and IMAP protocols.

7.1 Web protection

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

7.1.1 Ports

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

7.1.2 Active mode

ESET Cyber Security also contains the **Active Mode** submenu, which defines the checking mode for web browsers. Active mode examines transferred data from applications accessing the Internet as a whole, regardless of whether they are marked as web browsers or not. If it is not enabled, communications from applications are monitored gradually in batches. This decreases the effectiveness of the data verification process, but also provides higher compatibility for listed applications. If no problems occur while using it, we recommend that you enable active checking mode by selecting the checkbox next to the desired application.

When a controlled application downloads data, it is first saved to a temporary file created by ESET Cyber Security. Data is not available for the given application at that time. Once downloading is complete, it is checked for malicious code. If no infiltration is found, data is sent to the original application. This process provides complete control of the communications made by a controlled application. If passive mode is activated, data is trickle-fed to the original application to avoid timeouts.

7.1.3 URL lists

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

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

7.2 Email protection

Email protection provides control of email communication received through POP3 and IMAP protocols. When examining incoming messages, the program uses all the advanced scanning methods included in the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 and IMAP protocol communications is independent of the email client used.

ThreatSense Engine - advanced virus scanner setup enables

you to configure scan targets, detection methods, etc. Click **Setup...** to display the detailed scanner setup window.

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

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

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

Append tag message to the email footnote - select this checkbox if you want email protection to include a virus warning in the infected email. This feature allows for simple filtering of infected emails. It also increases the level of credibility for the recipient and, if an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

7.2.1 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 used.

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

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

7.2.2 IMAP protocol checking

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

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

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

8. Update

Regularly updating ESET Cyber Security is necessary to maintain the maximum level of security. The Update module ensures that the program is always up to date by downloading the most recent virus signature database.

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 virus signature database**.

Under normal circumstances, when updates are downloaded properly, the message **Virus signature database is up to date** will appear in the Update window. If the virus signature database cannot be updated, we recommend that you check the update settings 13 - the most common reason for this error is incorrectly entered authentication data (Username and Password) or incorrectly configured connection settings 18.

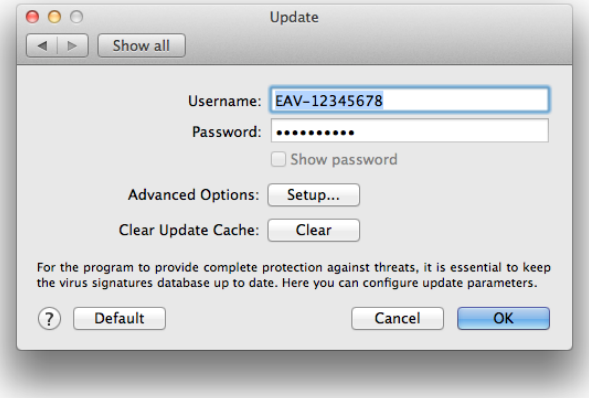
The Update window also contains information about the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added during the given update.

NOTE: Your Username and Password are provided by ESET after purchasing ESET Cyber Security.

8.1 Update setup

Authentication for the ESET update server is based on the Username and Password generated and sent to you after purchase.

To enable the use of test mode (downloads pre-release updates) click **Setup** > **Enter application preferences ...** (or press *cmd-,*) > **Update**, click **Setup...** next to **Advanced Options** and then select the **Enable pre-release updates** checkbox. We recommend the use of test mode only in situations where a pre-release update is available to fix an issue you are having with ESET Cyber Security.



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

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

8.2 How to create update tasks

Updates can be triggered manually by clicking Update from the main menu and then clicking **Update virus signature database**.

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

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

Each of the update tasks can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see the Scheduler 15 section.

8.3 Upgrading 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 will be displayed. Click **Learn more...** to display a new window containing the version number of the new build and the changelog.

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 will be downloaded to your downloads folder (or the default folder set by your browser). When the file has finished downloading, launch the file and follow the installation directions. Your Username and Password will be automatically transferred to the new installation. We recommend that you check for upgrades regularly, especially when installing ESET Cyber Security from a CD or DVD.

9. Tools

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

9.1 Log files

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

1. **Detected threats** – use this option to view all information about events related to the detection of infiltrations.
2. **Events** – this option is designed to help system administrators and users solve problems. All important actions performed by ESET Cyber Security are recorded in the Event logs.
3. **Computer scan** – results of all completed scans are displayed in this log. Double-click any entry to view details for the respective On-demand computer scan.

In each section, the displayed information can be directly copied to the clipboard by selecting the entry and clicking on the **Copy** button.

9.1.1 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.
- **Optimize log files automatically** - enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded.

To configure the **Computer Scan Log Records Default Filter** click **Edit...** and select/deselect log types as required.

9.1.2 Log filtering

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

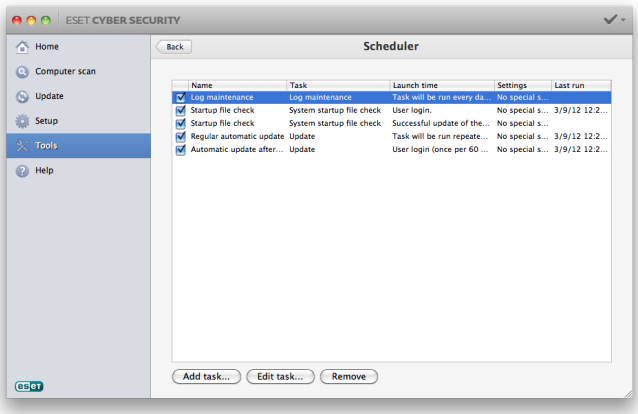
The most frequently used log types are listed below:

- **Critical warnings** – critical system errors (e.g., Antivirus protection failed to start)

- **Errors** - error messages such as "*Error downloading file*" and critical errors
- **Warnings** – warning messages
- **Informative records** - informative messages including successful updates, alerts, etc.
- **Diagnostic records** - information needed for fine-tuning the program as well as all records described above.

9.2 Scheduler

The **Scheduler** can be found 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 used.



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

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

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

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

9.2.1 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**

Since Update is one of the most frequently used scheduled tasks, we will explain how to add a new update task.

From the **Scheduled task** drop-down menu select **Update**. Enter the name of the task into the **Task name** field. Select the frequency of the task from the **Run task** drop-down menu. Based on the frequency selected, you will be prompted to specify different update parameters.

If you select **User-defined**, you will be prompted to specify date/time in cron format (see the Creating user-defined task 15 section for more details).

In the next step, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

- **Wait until the next scheduled time**
- **Run the task as soon as possible**
- **Run the task immediately if the time since its last execution exceeds specified interval** (the interval can be defined using the **Minimum task interval** option)

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish**.

The new scheduled task will be added to the list of currently scheduled tasks.

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

9.2.2 Creating user-defined tasks

Date and time of the **User-defined** task has to be entered in year-extended cron format (a string containing 6 fields each separated by a space):

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

Example:

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

Special characters supported in cron expressions:

- asterisk (`*`) - expression will match for all values of the field; e.g. asterisk in the 3rd field (day of month) means every day
- hyphen (`-`) - defines ranges; e.g. `3-9`

- comma (,) - separates items of a list; e.g. `1,3,7,8`
- slash (/) - defines increments of ranges; e.g. `3-28/5` in the 3rd field (day of month) means 3rd day of the month and then every 5 days.

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

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

9.3 Quarantine

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

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

Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (e.g., added by user…) and number of threats (e.g., if it is an archive containing multiple infiltrations). The quarantine folder with quarantined files (*/Library/Application Support/Eset/esets/cache/quarantine*) remains in the system even after uninstalling ESET Cyber Security. Quarantined files are stored in a safe encrypted form and can be restored again after installing ESET Cyber Security.

9.3.1 Quarantining files

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

9.3.2 Restoring from Quarantine

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

9.3.3 Submitting file from Quarantine

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

9.4 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.

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

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

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

9.5 Live Grid

The Live Grid Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional Live Grid Early Warning System has a single purpose – to improve the protection that we can offer you. The best way to ensure that we see new threats as soon as they appear is to "link" to as many of our customers as possible and use them as our threat scouts. There are two options:

1. 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 we offer.
2. You can configure the Live Grid Early Warning System to submit anonymous information about new threats and where new threatening code is contained. This information can be sent to ESET for detailed analysis. Studying these threats will help ESET update its database of threats and improve the program's threat detection ability.

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

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

To access Live Grid setup from the main menu, click **Setup** > **Enter application preferences ...** (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**.

9.5.1 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 wish to submit these files automatically, deselect **Submission of Suspicious Files**.

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

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

Below is an example of a statistical package submitted:

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

Exclusion Filter – This option allows you to exclude certain file types from submission. For example, it may be useful to exclude files which may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, .rtf etc.). You can add file types to the list of excluded files.
Contact Email (optional) – Your email address will be used if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

10. User interface

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

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

Present application in Dock allows you to display the ESET Cyber Security icon in the Mac OS Dock and switch between ESET Cyber Security and other running applications by pressing *cmd-tab*. Changes take effect after you restart ESET Cyber Security (usually triggered by computer restart).

The **Use standard menu** option allows you to use certain keyboard shortcuts (see Keyboard shortcuts 6) and see standard menu items (User interface, Setup and Tools) on the Mac OS menu bar (top of the screen).

To enable tooltips for certain options of ESET Cyber Security, select **Show tooltips**.

Show hidden files allows you to see and select hidden files in the **Scan Targets** setup of a **Computer scan**.

10.1 Alerts and notifications

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

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

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

displayed by adjusting the **Close notifications automatically after** X **seconds** value.

To see only notifications requiring user interaction when running applications in full screen, select **Enable full screen mode**. This is useful when giving presentations, playing games or doing other activities that require the entire screen.

10.1.1 Alerts and notifications advanced setup

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 etc. 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 **Notification Name**. Additionally, you can define **Display Conditions** under which notifications about new program versions and operating system updates will be displayed.

10.2 Privileges

ESET Cyber Security settings can be very 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**.

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

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

10.3 Context menu

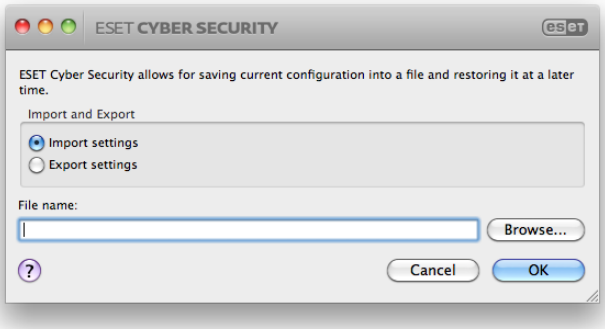
Context menu integration can be enabled by clicking **Setup** > **Enter application preferences ...** (or press *cmd-,*) > **Context Menu** section by selecting the **Integrate into the context menu** option. Logging out or restarting the computer is required for changes to take effect. Context menu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

11. Miscellaneous

11.1 Import and export settings

Importing and exporting configurations of ESET Cyber Security can be done from the **Setup** section.

Import and export are useful if you need to backup your current configuration of ESET Cyber Security for use at a later date. **Export settings** 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.



11.1.1 Import settings

To import a configuration click **Setup** > **Import and export settings ...** from the main menu and then select **Import settings**. Enter the name of your configuration file or click **Browse...** to browse for the configuration file you want to import.

11.1.2 Export settings

To export a configuration, click **Setup** > **Import and export settings ...** from the main menu. Select **Export settings** and enter the name of your configuration file. Use the browser to select a location on your computer to save the configuration file.

11.2 Proxy server setup

Proxy server settings can be configured 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 will be used by all modules that require a connection to the Internet.

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

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

12. Glossary

12.1 Types of infiltration

An Infiltration is a piece of malicious software that attemtps to enter and/or damage a user's computer.

12.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses typically attack executable files, scripts and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. Conversely, some viruses do not cause any damage, they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term "virus" is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term "malware" (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state, usually by cleaning them using an antivirus program.

12.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves; they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours of their release, in some cases, even in minutes. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend that you delete the infected files because they likely contain malicious code.

12.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations that attempt to present themselves as useful programs, tricking users into letting them run. Today, there is no longer a need for trojan horses to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

- Downloader – A malicious program with the ability to download other infiltrations from the Internet
- Dropper – A type of trojan horse designed to drop other types of malware onto compromised computers
- Backdoor – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it
- Keylogger – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers
- Dialer – Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection has been created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.
- Trojan horses usually take the form of executable files. If a file on your computer is detected as a trojan horse, we recommend deleting it, since it most likely contains malicious code.

12.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system while concealing their presence. After accessing a system (usually exploiting a system vulnerability), rootkits use functions built into the operating system to avoid detection by antivirus software: they conceal processes and files. For this reason it is almost impossible to detect them using ordinary testing techniques.

12.1.5 Adware

Adware is a shortened term for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing creators of freeware programs to cover development costs of their (usually useful) applications.

Adware itself is not dangerous, users may only be bothered by the advertisements. The danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This often means that adware may access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry. If there is a file detected as adware on your computer, it is advisable that you delete it, since there is a high probability that it contains malicious code.

12.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory, they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, we recommend deleting it, since there is a high probability that it contains malicious code.

12.1.7 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands they may be misused for malicious purposes. ESET Cyber Security provides the option to detect such threats.

Potentially unsafe applications are typically commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

12.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the way it behaved before their installation). The most significant changes are:

- new windows you haven't seen previously are opened
- activation and running of hidden processes
- increased usage of system resources
- changes in search results
- applications communicate with remote servers

12.2 Types of remote attacks

There are many special techniques that allow attackers to compromise remote systems. These are divided into several categories.

12.2.1 DoS attacks

DoS, or Denial of Service, is an attempt to make a computer or network unavailable for its intended users. The communication between afflicted users is obstructed and can no longer continue in a functional way. Computers exposed to DoS attacks usually need to be restarted in order to work properly.

In most cases, the targets are web servers and the aim is to make them unavailable to users for a certain period of time.

12.2.2 DNS Poisoning

Using DNS (Domain Name Server) poisoning, hackers can trick the DNS server of any computer into believing that the fake data they supplied is legitimate and authentic. The fake information is cached for a certain period of time, allowing attackers to rewrite DNS replies of IP addresses. As a result, users trying to access Internet websites will download computer viruses or worms instead of their original content.

12.2.3 Port scanning

Port scanning is used to determine which computer ports are open on a network host. A port scanner is software designed to find such ports.

A computer port is a virtual point that handles incoming and outgoing data; this is crucial from a security point of view. In a large network, the information gathered by port scanners may help to identify potential vulnerabilities. Such use is legitimate.

Still, port scanning is often used by hackers attempting to compromise security. Their first step is to send packets to each port. Depending on the response type, it is possible to determine which ports are in use. The scanning itself causes no damage, but be aware that this activity can reveal potential vulnerabilities and allow attackers to take control of remote computers.

Network administrators are advised to block all unused ports and protect those that are in use from unauthorized access.

12.2.4 TCP desynchronization

TCP desynchronization is a technique used in TCP Hijacking attacks. It is triggered by a process in which the sequential number in incoming packets differs from the expected sequential number. Packets with an unexpected sequential number are dismissed (or saved in the buffer storage, if they are present in the current communication window).

In desynchronization, both communication endpoints dismiss received packets, at which point remote attackers are able to infiltrate and supply packets with a correct sequential number. The attackers can even manipulate or modify communication.

TCP Hijacking attacks aim to interrupt server-client, or peer-to-peer communications. Many attacks can be avoided by using authentication for each TCP segment. It is also advised that you use the recommended configuration for your network devices.

12.2.5 SMB Relay

SMBRelay and SMBRelay2 are special programs that are capable of carrying out attacks against remote computers. These programs take advantage of the Server Message Block file sharing protocol, which is layered onto NetBIOS. A user sharing any folder or directory within a LAN most likely uses this file sharing protocol.

Within local network communication, password hashes are exchanged.

SMBRelay receives a connection on UDP port 139 and 445, relays the packets exchanged by the client and server, and modifies them. After connecting and authenticating, the client is disconnected. SMBRelay creates a new virtual IP address. SMBRelay relays SMB protocol communications except for negotiation and authentication. Remote attackers can use the IP address, as long as the client computer is connected.

SMBRelay2 works on the same principle as SMBRelay, except it uses NetBIOS names rather than IP addresses. Both can carry out “man-in-the-middle” attacks. These attacks allow remote attackers to read, insert and modify messages exchanged between two communication endpoints without being noticed. Computers exposed to such attacks often stop responding or unexpectedly restart.

To avoid attacks, we recommend that you use authentication passwords or keys.

12.2.6 ICMP attacks

The ICMP (Internet Control Message Protocol) is a popular and widely-used Internet protocol. It is used primarily by networked computers to send various error messages.

Remote attackers attempt to exploit the weaknesses of the ICMP protocol. The ICMP protocol is designed for one-way communication requiring no authentication. This enables remote attackers to trigger DoS (Denial of Service) attacks, or attacks which give unauthorized individuals access to incoming and outgoing packets.

Typical examples of an ICMP attack are ping floods, ICMP_ECHO floods and smurf attacks. Computers exposed to an ICMP attack are significantly slower (this applies to all applications that use the Internet) and have problems connecting to the Internet.

12.3 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990‘s.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, do not publish your email address on the Internet
- only give your email address to trusted individuals
- if possible, do not use common aliases. With more complicated aliases, the probability of tracking is lower
- do not reply to spam that has already arrived in your inbox
- be careful when filling out Internet forms, be especially cautious of options such as *Yes, I want to receive information*
- use “specialized” email addresses, for example one for business, one for communication with your friends, etc.
- from time to time, change your email address
- use an Antispam solution

12.3.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what is more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with their current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

12.3.2 Hoaxes

A hoax is misinformation that is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

12.3.3 Phishing

The term phishing defines a criminal activity that uses social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email that impersonates a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

12.3.4 Recognizing spam scams

Generally, there are a few indicators that can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message.

- Sender address does not belong to someone on your contact list
- you are offered a large sum of money, but you have to provide a small sum first
- you are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- it is written in a foreign language
- you are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer)
- some of the words are misspelled in an attempt to trick your spam filter. For example *vaigra* instead of *viagra*, etc.