

ESET SECURITY

FOR KERIO

Installation Manual and User Guide

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012

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



ESET SECURITY

Copyright ©2013 by ESET, spol. s r.o.

ESET Security for Kerio was developed by ESET, spol. s r.o.

For more information visit www.eset.com.

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

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

Customer Care: www.eset.com/support

REV. 10/28/2013

Contents

1. Introduction.....	5
1.1 System requirements.....	5
1.2 User interface.....	5
2. Installation.....	6
2.1 Typical Installation.....	6
2.2 Custom Installation.....	7
2.3 Terminal Server.....	9
2.4 License.....	9
2.5 Post-Installation Configuration.....	10
2.6 Kerio upgrade.....	10
3. ESET Security for Kerio - Kerio Connect/Control Server protection.....	11
3.1 General settings.....	11
3.1.1 Kerio Control/Connect.....	11
3.1.2 Rules.....	11
3.1.2.1 Adding new rules.....	12
3.1.2.2 Actions taken when applying rules.....	12
3.1.3 Log files.....	13
3.1.4 Performance.....	13
3.2 Antivirus and antispware settings.....	13
3.2.1 Kerio Control/Connect.....	14
3.2.2 Automatic exclusions.....	14
3.3 FAQ.....	14
4. ESET Security for Kerio - Server protection.....	15
4.1 Antivirus and antispware protection.....	15
4.1.1 Real-time file system protection.....	15
4.1.1.1 Control setup.....	15
4.1.1.1.1 Media to scan.....	16
4.1.1.1.2 Scan on (Event-triggered scanning).....	16
4.1.1.1.3 Advanced scan options.....	16
4.1.1.2 Cleaning levels.....	16
4.1.1.3 When to modify real-time protection configuration.....	17
4.1.1.4 Checking real-time protection.....	17
4.1.1.5 What to do if real-time protection does not work.....	17
4.1.2 Email client protection.....	18
4.1.2.1 POP3 checking.....	18
4.1.2.1.1 Compatibility.....	19
4.1.2.2 Integration with email clients.....	20
4.1.2.2.1 Appending tag messages to email body.....	21
4.1.2.3 Removing infiltrations.....	21
4.1.3 Web access protection.....	22
4.1.3.1 HTTP, HTTPS.....	22
4.1.3.1.1 Address management.....	23
4.1.3.1.2 Active mode.....	24
4.1.4 On-demand computer scan.....	25
4.1.4.1 Type of scan.....	25
4.1.4.1.1 Smart scan.....	25
4.1.4.1.2 Custom scan.....	26
4.1.4.2 Scan targets.....	26
4.1.4.3 Scan profiles.....	27
4.1.4.4 Command Line.....	27
4.1.5 Performance.....	29
4.1.6 Protocol filtering.....	29
4.1.6.1 SSL.....	29
4.1.6.1.1 Trusted certificates.....	30
4.1.6.1.2 Excluded certificates.....	30
4.1.7 ThreatSense engine parameters setup.....	30
4.1.7.1 Objects setup.....	31
4.1.7.2 Options.....	31
4.1.7.3 Cleaning.....	32
4.1.7.4 Extensions.....	33
4.1.7.5 Limits.....	34
4.1.7.6 Other.....	34
4.1.8 An infiltration is detected.....	35
4.2 Updating the program.....	36
4.2.1 Update setup.....	37
4.2.1.1 Update profiles.....	38
4.2.1.2 Advanced update setup.....	38
4.2.1.2.1 Update mode.....	39
4.2.1.2.2 Proxy server.....	40
4.2.1.2.3 Connecting to the LAN.....	42
4.2.1.2.4 Creating update copies - Mirror.....	43
4.2.1.2.4.1 Updating from the Mirror.....	44
4.2.1.2.4.2 Troubleshooting Mirror update problems.....	45
4.2.2 How to create update tasks.....	45
4.3 Scheduler.....	46
4.3.1 Purpose of scheduling tasks.....	46
4.3.2 Creating new tasks.....	47
4.4 Quarantine.....	48
4.4.1 Quarantining files.....	48
4.4.2 Restoring from Quarantine.....	48
4.4.3 Submitting file from Quarantine.....	49
4.5 Log files.....	50
4.5.1 Log filtering.....	51
4.5.2 Find in log.....	52
4.5.3 Log maintenance.....	53
4.6 ESET SysInspector.....	54
4.6.1 Introduction to ESET SysInspector.....	54
4.6.1.1 Starting ESET SysInspector.....	54
4.6.2 User Interface and application usage.....	55
4.6.2.1 Program Controls.....	55
4.6.2.2 Navigating in ESET SysInspector.....	56
4.6.2.2.1 Keyboard shortcuts.....	57
4.6.2.3 Compare.....	59
4.6.3 Command line parameters.....	60
4.6.4 Service Script.....	60
4.6.4.1 Generating Service script.....	60
4.6.4.2 Structure of the Service script.....	61
4.6.4.3 Executing Service scripts.....	63
4.6.5 FAQ.....	63
4.7 ESET SysRescue.....	64
4.7.1 Minimum requirements.....	65
4.7.2 How to create rescue CD.....	65
4.7.3 Target selection.....	65
4.7.4 Settings.....	66
4.7.4.1 Folders.....	66
4.7.4.2 ESET Antivirus.....	66
4.7.4.3 Advanced settings.....	66
4.7.4.4 Internet protocol.....	67
4.7.4.5 Bootable USB device.....	67
4.7.4.6 Burn.....	67
4.7.5 Working with ESET SysRescue.....	67
4.7.5.1 Using ESET SysRescue.....	68
4.8 User interface options.....	68
4.8.1 Alerts and notifications.....	70
4.8.2 Disable GUI on Terminal Server.....	71
4.9 eShell.....	71
4.9.1 Usage.....	72
4.9.2 Commands.....	75
4.10 Import and export settings.....	77
4.11 ThreatSense.Net.....	77
4.11.1 Suspicious files.....	79
4.11.2 Statistics.....	80
4.11.3 Submission.....	81

4.12 Remote administration.....	82
4.13 Licenses.....	83
5. Glossary.....	84
5.1 Types of infiltration.....	84
5.1.1 Viruses.....	84
5.1.2 Worms.....	84
5.1.3 Trojan horses.....	84
5.1.4 Rootkits.....	85
5.1.5 Adware.....	85
5.1.6 Spyware.....	85
5.1.7 Potentially unsafe applications.....	86
5.1.8 Potentially unwanted applications.....	86
5.2 Email.....	86
5.2.1 Advertisements.....	87
5.2.2 Hoaxes.....	87
5.2.3 Phishing.....	87
5.2.4 Recognizing spam scams.....	87
5.2.4.1 Rules.....	88
5.2.4.2 Bayesian filter.....	88
5.2.4.3 Whitelist.....	88
5.2.4.4 Blacklist.....	88
5.2.4.5 Server-side control.....	89

1. Introduction

ESET Security for Kerio for Kerio Control and Connect is an integrated solution that protects against various types of malware content including email attachments infected by worms or trojans, documents containing harmful scripts and phishing. ESET Security for Kerio provides two types of protection: Antivirus and the application of user-defined rules. ESET Security for Kerio for Kerio filters the malicious content at the server level. It filters email messages before they arrive in the recipient email client mailboxes.

ESET Security for Kerio supports Kerio Control as well as Kerio Connect. You can remotely manage ESET Security for Kerio in larger networks with the help of ESET Remote Administrator.

While providing protection for Kerio Control and Connect, ESET Security for Kerio also has tools to ensure protection of the server itself (resident protection, web-access protection and email client protection).

1.1 System requirements

Supported Operating Systems:

- Microsoft Windows Server 2003 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Supported Kerio Connect versions:

- Kerio Connect 7.4.x and newer

Supported Kerio Control versions:

- Kerio Control 7.4.0, 7.4.1 and 7.4.2

Hardware requirements depend on the operating system version and the version of Kerio product in use. We recommend reading the Kerio product documentation for more detailed information on hardware requirements.

1.2 User interface

ESET Security for Kerio has graphical user interface (GUI) designed to be as intuitive as possible. The GUI gives users quick and easy access to the main functions of the program.

In addition the main GUI, there is an **advanced setup tree** which is accessible from anywhere in the program by pressing the F5 key.

Once you press F5, the advanced setup tree window opens and displays a list of configurable program features. From this window, you can configure the settings and options based on your needs. The tree structure is split into two main sections: **Server protection** and **Computer protection**. Apart from that, there are several other sections such as Update, Tools, User interface and Miscellaneous. The **Computer protection** section contains the configurable items for the protection of the server itself.

2. Installation

After purchasing ESET Security for Kerio, the installer can be downloaded from ESET's website (www.eset.com) as an .msi package.

Please note that you need to execute the installer under **Built-in Administrator** account. Any other user, despite being a member of Administrators group, will not have sufficient access rights. Therefore you need to use Built-in Administrator account, as you will not be able to successfully complete the installation under any other user account than **Administrator**.

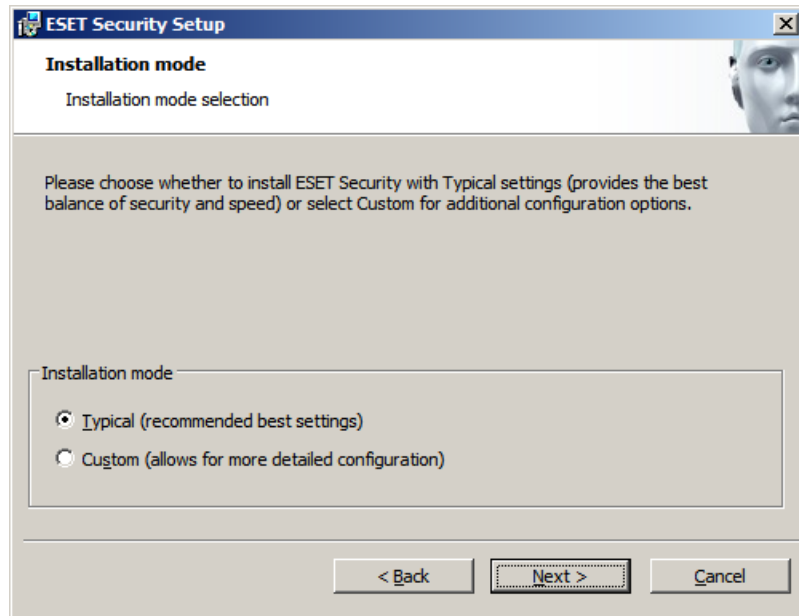
There are two ways to execute the installer:

- You can login locally using Administrator account credentials and simply run the installer
- You can be logged in as other user, but need to open command prompt with **Run as...** and type in Administrator account credentials to have the cmd running as Administrator, then type in the command to execute the installer (e.g. `msiexec /i emsk_nt64_ENU.msi` but you need to replace `emsk_nt64_ENU.msi` with the exact file name of the msi installer you have downloaded)

Once you launch the installer, the installation wizard will guide you through the basic setup. There are two types of installation available with different levels of setup details:

1. Typical Installation

2. Custom Installation



NOTE: We highly recommend installing ESET Security for Kerio on a freshly installed and configured OS, if possible. However, if you do need to install it on an existing system, the best to do is to uninstall previous version of ESET Security for Kerio, restart the server and install the new ESET Security for Kerio afterwards.

2.1 Typical Installation

Typical installation mode quickly installs ESET Security for Kerio with minimal configuration during the installation process. Typical installation is the default installation mode and is recommended if you do not have particular requirements for specific settings yet. After ESET Security for Kerio has been installed on your system, you can modify the options and configuration settings at any time. This user guide describes these settings and functionality in detail. The Typical installation mode settings provide excellent security coupled with ease of use and high system performance.

After selecting the installation mode and clicking Next, you will be prompted to enter your Username and Password. This plays a significant role in providing constant protection to your system, as your Username and Password allows automatic virus signature database [Updates](#) ^[36].

Enter the Username and Password, which you received after the purchase or registration of the product, into the corresponding fields. If you do not currently have your Username and Password available, it can be entered directly from the program at a later time.

In the next step - **License Manager** - Add the license file that was delivered via email after you purchased your product.

The next step is to configure the ThreatSense.Net Early Warning System. The ThreatSense.Net Early Warning System helps ensure that ESET is immediately and continuously informed about new infiltrations in order to quickly protect its customers. This system allows new threats to be submitted to ESET's Threat Lab, where they are analyzed, processed and added to the virus signature database. By default, the **Enable ThreatSense.Net Early Warning System** option is selected. Click **Advanced setup...** to modify detailed settings about the submission of suspicious files.

The next step in the installation process is to configure **Detection of potentially unwanted applications**. Potentially unwanted applications are not necessarily malicious, but can often negatively affect the behavior of your operating system. See the [Potentially unwanted applications](#)^[86] chapter for more details.

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.

Select the **Enable detection of potentially unwanted applications** option to allow ESET Security for Kerio to detect this type of applications. If you do not wish to use this functionality, select **Disable detection of potentially unwanted applications**.

The final step in Typical installation mode is to confirm the installation by clicking the **Install** button.

2.2 Custom Installation

Custom installation is designed for those who would like to configure ESET Security for Kerio during the installation process.

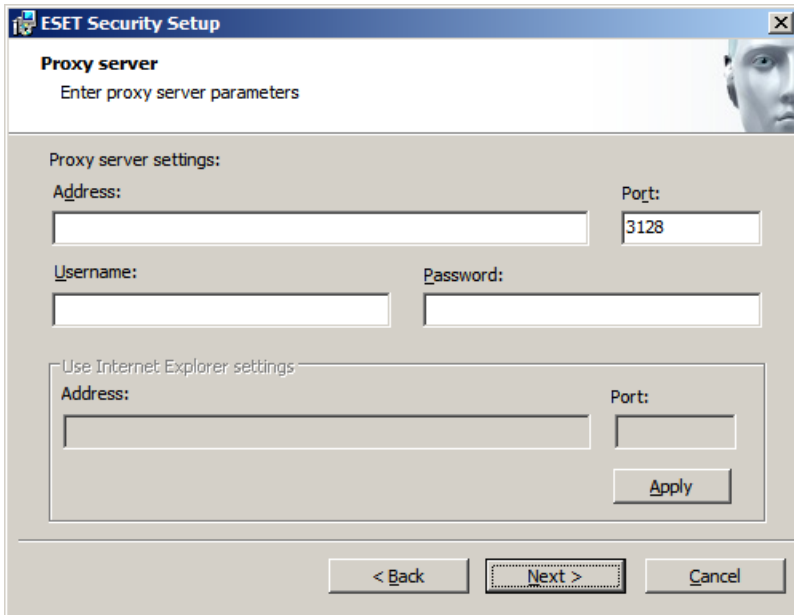
After selecting the installation mode and clicking **Next**, you will be prompted to select a destination location for the installation. By default, the program installs in `C:\Program Files\ESET\ESET Security for Kerio`. Click **Browse...** to change this location (not recommended).

Next, enter your **Username** and **Password**. This step is the same as the Typical installation mode step (see "[Typical installation](#)"^[6]).

In the next step - **License Manager** - Add the license file that was delivered via email after you purchased your product.

After entering your Username and Password, click **Next** to proceed to **Configure your Internet connection**.

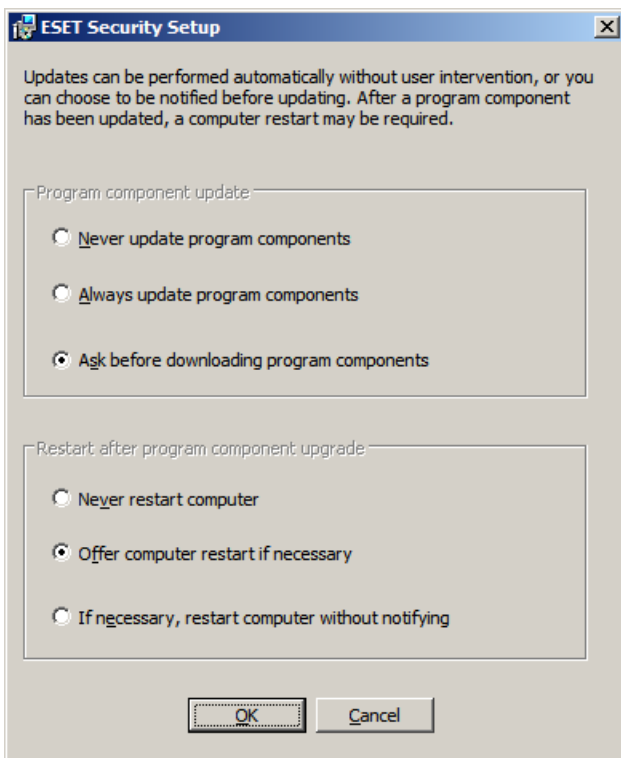
If you use a proxy server, it must be correctly configured for virus signature updates to work correctly. If you would like to have the proxy server configured automatically, select the default setting **I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer (Recommended)** and click **Next**. If you do not use a proxy server, select the **I do not use a proxy server** option.



If you prefer to enter the proxy server details yourself, you can configure the proxy server settings manually. To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address** field. In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). If your proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. Once the proxy server details are entered, click **Apply** and confirm the selection.

Click **Next** to proceed to **Configure automatic update** settings. This step allows you to designate how automatic program component updates will be handled on your system. Click **Change...** to access the advanced settings.

If you do not want program components to be updated, select the **Never update program components** option. Select the **Ask before downloading program components** option to display a confirmation window before downloading program components. To download program component upgrades automatically, select the **Always update program components** option.



NOTE: After a program component update, a restart is usually required. We recommend selecting the **Never restart computer** option. The latest component updates will come into effect after the next server restart (whether it is [scheduled](#)⁴⁶⁾, manual or otherwise). You can choose **Offer computer restart if necessary** if you would like to be reminded to restart the server after the components were updated. With this setting, you can restart the server right away or postpone the restart and perform it at a later time.

The next installation window offers the option to set a password to protect your program settings. Select the **Protect configuration settings with a password** option and choose a password to enter in the **New password** and **Confirm new password** fields.

The next three installation steps, **ThreatSense.Net Early Warning System**, **Detection of potentially unwanted applications** are the same as the Typical installation mode steps (see [“Typical installation”](#)^[6]).

Click **Install** in the **Ready to install** window to complete installation.

2.3 Terminal Server

If you are installing ESET Security for Kerio on Windows Server that acts as a Terminal Server, you might want to disable the ESET Security for Kerio GUI to prevent it from starting up every time a user logs in. See [Disable GUI on Terminal Server](#)^[7] for specific steps to disable the GUI.

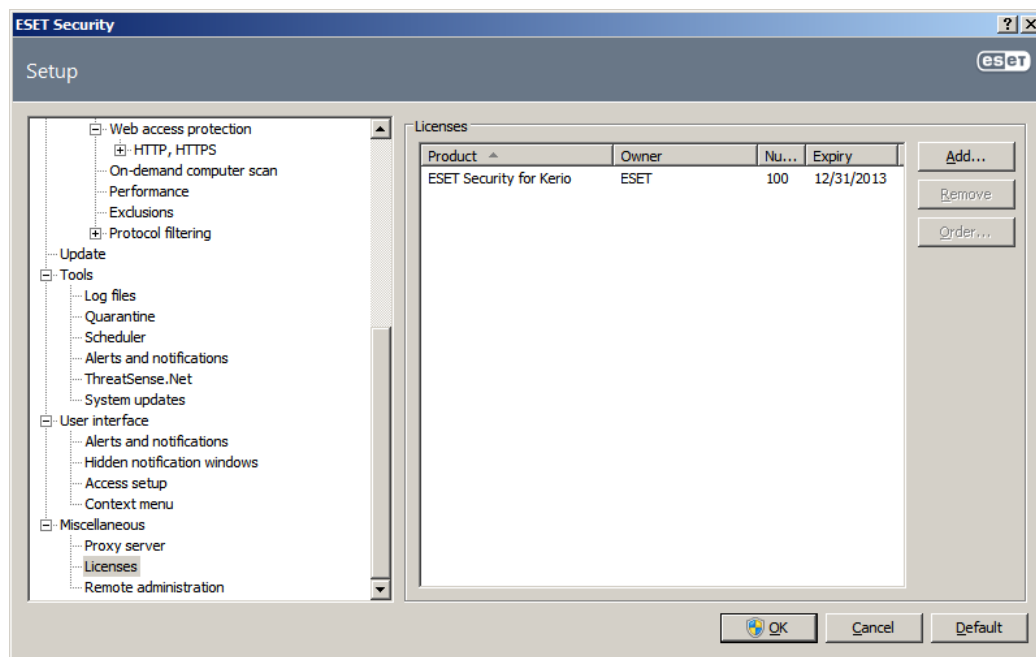
2.4 License

A very important step is to enter the license file for ESET Security for Kerio for Kerio Connect/Control. Without it, server protection on the Kerio will not work properly. If you do not add the license file during installation, you can do so later in the advanced settings, under **Miscellaneous > Licenses**.

ESET Security for Kerio allows you to use several licenses simultaneously by merging them, as is described in the following:

- 1) Two or more licenses of one customer (i.e. licenses assigned to the same customer name) are merged and the number of scanned mailboxes increases accordingly. The license manager will continue to display both licenses.
- 2) Two or more licenses of different customers are merged. This occurs exactly the same way as in the first scenario (point 1 above), with the only difference, that at least one of the licenses in question must have a special attribute. That attribute is required to merge licenses of different customers. If you are interested in using such a license, ask your local distributor to generate it for you.

NOTE: Validity period of the newly created license is determined by the earliest expiration date from among its constituents.



NOTE: For Kerio Control, only one license is sufficient as there are no checks for the number of connections. In case of a dual system (Kerio Connect and Kerio Control running on the same server), there is such license required that covers the number of mailboxes (users) of Kerio Connect plus one extra license for Kerio Control.

2.5 Post-Installation Configuration

There are several options that should to be configured after the product installation.

Performance

If there are no other restrictions, our recommendation is to increase the number of ThreatSense scan engines in the Advanced settings window (F5) under **Computer protection > Antivirus and antispyware > Performance**, according to this formula: *number of ThreatSense scan engines = (number of physical CPUs x 2) + 1*. Here is an example:

Let's say you have a server with 4 physical CPUs. For the best performance, according to formula above, you should have 9 scan engines.

NOTE: Acceptable value is 1-20, so the maximum number of ThreatSense scan engines you can use is 20. The change will be applied only after restart.

Terminal Server

If you are using ESET Security for Kerio on a Windows Server that acts as a Terminal Server and do not want the ESET Security for Kerio GUI to start up every time a user logs in, see the [Disable GUI on Terminal Server](#)^[71] chapter for specific steps to disable it.

2.6 Kerio upgrade

In a case when upgrading from Kerio Connect 8.0.2 (or older) to version 8.1.0 (which is a version that officially does not support external AV protection) the upgrade process of Kerio does not preserve ESET Security for Kerio program's registration (dll and configuration) which renders ESET Security for Kerio protection not to work and Kerio Connect is not protected even though the protection status is still shown as "Green". This is only for a period of time until ESET Security for Kerio checks for its registration. This check is performed every 30 minutes. If ESET Security for Kerio finds out that the registration is not correct, it automatically registers itself and restarts Kerio Connect. This makes the protection to work properly again. Hence the Kerio Connect may not be protected for a maximum of 30 minutes after the upgrade.

It is possible to register ESET Security for Kerio to Kerio Connect manually after the upgrade. This will turn the protection on immediately. In order to do so, follow these steps:

1. Press **F5** to enter **Setup**.
2. Expand **Server Protection > Kerio Connect**.
3. Uncheck **Register to Kerio Connect server** and press **OK** button, protection status will change to "Red".
4. Repeat steps 1. and 2., check **Register to Kerio Connect server** and press **OK** button, this registers ESET Security for Kerio to Kerio and turns the protection on and status changes back to "Green".

3. ESET Security for Kerio - Kerio Connect/Control Server protection

ESET Security for Kerio provides significant protection for your Kerio Connect/Control. There are two essential types of protection: Antivirus and the application of user-defined rules. ESET Security for Kerio protects from various types of malware content, including email attachments infected by worms or trojans, documents containing harmful scripts and phishing. ESET Security for Kerio for Kerio filters out the malicious content on the mail server level, before it arrives in the recipient's email client inbox. Following chapters describe all the options and settings available to you in order to fine-tune your Kerio Connect/Control protection.

3.1 General settings

This section describes how to administer rules, log files and performance parameters as well as antivirus and antispyware settings.

3.1.1 Kerio Control/Connect

In this section, you can specify whether ESET Security for Kerio is registered to Kerio Control/Connect server. This has direct effect on protection status. It is registered by default. When **Register to Kerio Control server** or **Register to Kerio Connect server** checkbox is ticked, it means that ESET Security for Kerio has registered its dll and configuration in Kerio Control/Connect accordingly. When you clear the **Register to Kerio Control server** or **Register to Kerio Connect server** checkbox, then the dll is unregistered from Kerio Control/Connect which means that the protection is disabled.

NOTE: By changing this setting and then pressing **OK** button, ESET Security for Kerio automatically restarts relevant Kerio service.

3.1.2 Rules

The **Rules** menu item allows administrators to manually define email filtering conditions and actions to take with filtered emails. The rules are applied according to a set of combined conditions. Multiple conditions are combined with the logical operator AND, applying the rule only if all the conditions are met. The **Number** column (next to each rule name) displays the number of times the rule was successfully applied.

- **Add...** - adds a new rule
- **Edit...** - modifies an existing rule
- **Remove** - removes selected rule
- **Clear** - clears the rule counter (the Hits column)
- **Move up** - moves selected rule up in the list
- **Move down** - moves selected rule down in the list

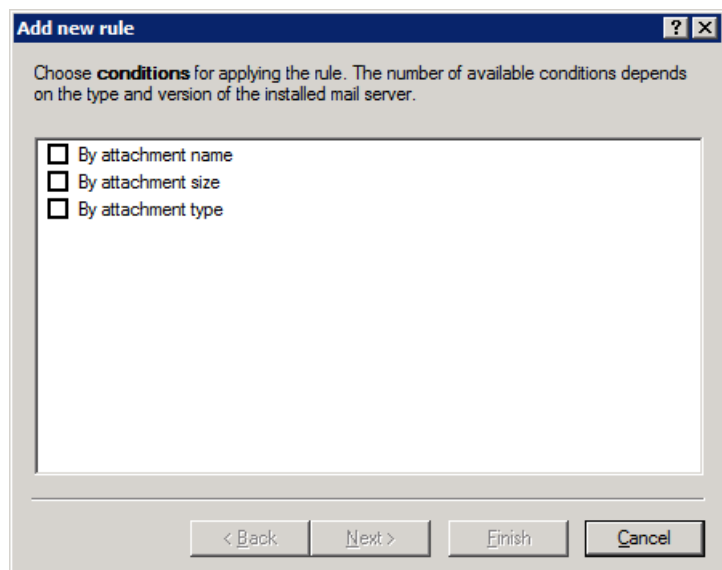
Unchecking a check box (to the left of each rule name) deactivates current rule. This allows for the rule to be reactivated again if needed.

NOTE: You can also use system variables (e.g., %PATHEXT%) when configuring Rules.

NOTE: If a new rule has been added or an existing rule has been modified, a message rescan will automatically start using the new/modified rules.

3.1.2.1 Adding new rules

This wizard guides you through adding user-specified rules with combined conditions.

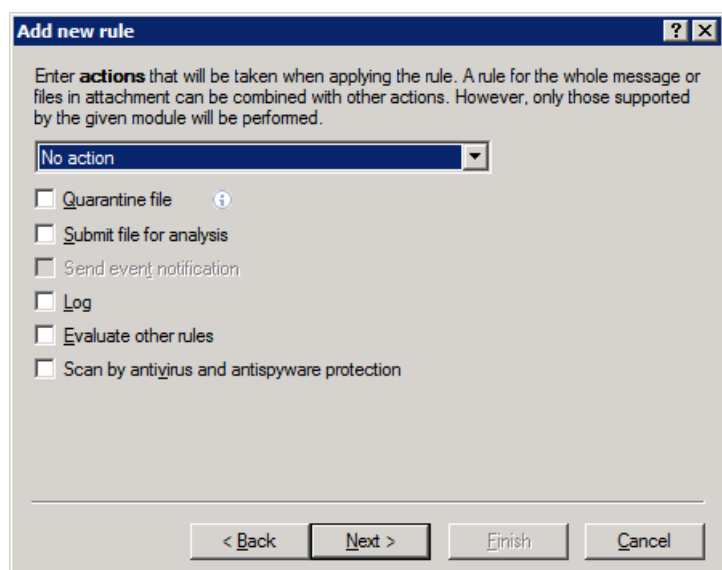


- **By attachment name** applies to a message with a specific attachment name
- **By attachment size** applies to a message with an attachment exceeding a defined size
- **By attachment type** applies to a message with an attachment of specified file type (actual file type is detected by its contents, regardless of file extension)

When specifying the conditions above (except the **By attachment size** condition), it is sufficient to fill in only part of a phrase as long as the **Match whole words** option is not selected. Values are not case-sensitive, unless the **Match case** option is selected. If you are using values other than alphanumeric characters, use parentheses and quotes. You can also create conditions using the logical operators AND, OR and NOT.

3.1.2.2 Actions taken when applying rules

This section allows you to select actions to take with messages and/or attachments matching conditions defined in rules. You can choose to take **No action** or to **Take action for uncleaned threat**. When action is being taken for uncleaned threat, particular part of the message is deleted (attachment or message body) depending on the criteria set.



- **No action** – no action will be taken with the message
- **Take action for uncleaned threat** - the message will be marked as if it contained an uncleaned threat (regardless of whether it contained the threat or not)

- **Quarantine file** - attached file(s) that meet the rules criteria will be put into file quarantine of ESET Security for Kerio
- **Submit file for analysis** - sends suspicious attachments to the ESET lab for analysis
- **Send event notification** - sends a notification to the administrator (based on settings in **Tools > Alerts and notifications**)
- **Log** - writes information about the applied rule to the program log
- **Evaluate other rules** - allows the evaluation of other rules, enabling the user to define multiple sets of conditions and multiple actions to take, given the conditions
- **Scan by antivirus and antispyware protection** - scans the message and its attachments for threats

NOTE: Messages to be scanned are sent by Kerio Connect in parts (not as a whole message). This may affect statistics and application of rules. Also, if a message body consists of multiple parts (plain, html, rtf), then each part is being scanned separately. Message body is named `avfile.tmp` during scanning.

NOTE: If a message contains attachment which does not have an extension, this file is then sent for scanning named as `avfile.tmp`. This needs to be considered when creating a rule with condition **By attachment name**.

3.1.3 Log files

Log files settings let you choose how the log file will be assembled. More detailed protocol can contain more information, but it may slow down server's performance.

If **Synchronized writing without using cache** is enabled, all the log entries will be immediately written in the log file without being stored in the log cache. By default, ESET Security for Kerio components running in Kerio Connect/Control store log messages in their internal cache and send them to the application log at periodic time intervals to preserve performance. In this case, however, the diagnostic entries in the log might not be in the proper order. We recommend keeping this setting turned off unless it is necessary for diagnostics. You can specify the type of information stored in the log files in the **Content** menu.

- **Log rule application** - when this option is enabled, ESET Security for Kerio writes the name of all activated rules into the log file.
- **Log performance** - logs information about the time interval of a performed task, size of the scanned object, transfer rate (kb/s) and performance rating.
- **Log diagnostic information** - logs diagnostic information needed for fine-tuning of the program to the protocol; this option is mostly for debugging and identifying problems. Having this option turned on is not recommended. To see diagnostic information provided by this function, you will have to set the Minimum logging verbosity to **Diagnostic records** in the **Tools > Log files > Minimum logging verbosity** setting.

3.1.4 Performance

In this section you can define a folder to store temporary files in to improve program performance. If no folder is specified, ESET Security for Kerio will create temporary files in the system's temporary folder.

NOTE: In order to reduce the potential I/O and fragmentation impact, we recommend placing the Temporary folder on a different hard drive than the one on which Kerio Connect/Control is installed. We strongly recommend that you avoid assigning the Temporary folder to removable media such as floppy disk, USB, DVD, etc.

NOTE: You can use system variables (e.g. `%SystemRoot%\TEMP`) when configuring Performance settings.

3.2 Antivirus and antispyware settings

You can enable antivirus and antispyware mail server protection by selecting the **Enable antivirus and antispyware server protection** option. Note that antivirus and antispyware protection is turned on automatically after every restart of the service/computer. ThreatSense engine parameter setup is accessible by clicking on the **Setup...** button.

3.2.1 Kerio Control/Connect

In this section, you can simply enable or disable **Kerio Control antivirus and antispyware protection** or **Kerio Connect antivirus and antispyware protection**. This is without registering/unregistering ESET Security for Kerio program's dll described [here](#). It means that the dll and configuration remains registered into Kerio Control/Connect, but only the protection is enabled or disabled. It is enabled by default.

Also, you can configure ThreatSense engine parameters by clicking on the **Setup...** button and then modifying the parameters.

3.2.2 Automatic exclusions

The developers of server applications and operating systems recommend excluding sets of critical working files and folders from antivirus scans for most of their products. Antivirus scans may have a negative influence on a server's performance, lead to conflicts and even prevent some applications from running on the server. Exclusions help minimize the risk of potential conflicts and increase the overall performance of the server when running antivirus software.

ESET Security for Kerio identifies critical server applications and server operating system files and automatically adds them to the list of Exclusions. Once added to the list, the server process/application can be enabled (by default) by checking the appropriate box or disabled by unchecking it, with the following result:

- 1) If an application/operating system exclusion remains enabled, any of its critical files and folders will be added to the list of files excluded from scanning (**Advanced setup > Computer protection > Antivirus and antispyware > Exclusions**). Every time the server is restarted, the system performs an automatic check of exclusions and restores any exclusions that may have been deleted from the list. This is the recommended setting, if you wish to make sure the recommended Automatic exclusions are always applied.
- 2) If the user disables an application/operating system exclusion, its critical files and folders remain on the list of files excluded from scanning (**Advanced setup > Computer protection > Antivirus and antispyware > Exclusions**). However, they will not be automatically checked and renewed on the **Exclusions** list every time the server is restarted (see point 1 above). We recommend this setting for advanced users, who wish to remove or modify some of the standard exclusions. If you wish to have removed the exclusions from the list without restarting the server, you will need to remove them manually from the list (**Advanced setup > Computer protection > Antivirus and antispyware > Exclusions**).

Any user-defined exclusions entered manually under **Advanced setup > Computer protection > Antivirus and antispyware > Exclusions** will not be affected by the settings described above.

The Automatic exclusions of server applications/operating systems are selected based on Microsoft's recommendations. For details, please see the following links:

<http://support.microsoft.com/kb/822158>

<http://support.microsoft.com/kb/245822>

<http://support.microsoft.com/kb/823166>

<http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx>

<http://technet.microsoft.com/en-us/library/bb332342.aspx>

3.3 FAQ

Q: Why is it that "File server protection" is shown in Setup section of the main GUI when I am using Kerio Control?

A: On a system with Kerio Control, ESET Security for Kerio displays **File server protection** in its main program window in **Setup** section. This is expected behaviour, and when enabled, it means the Kerio Control is being protected by ESET Security for Kerio.

4. ESET Security for Kerio - Server protection

While providing Kerio Connect/Control protection, ESET Security for Kerio has all of the necessary tools to ensure protection of the server itself (resident shield, web-access protection, email client protection).

4.1 Antivirus and antispyware protection

Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by first blocking it, and then cleaning, deleting or moving it to quarantine.

4.1.1 Real-time file system protection

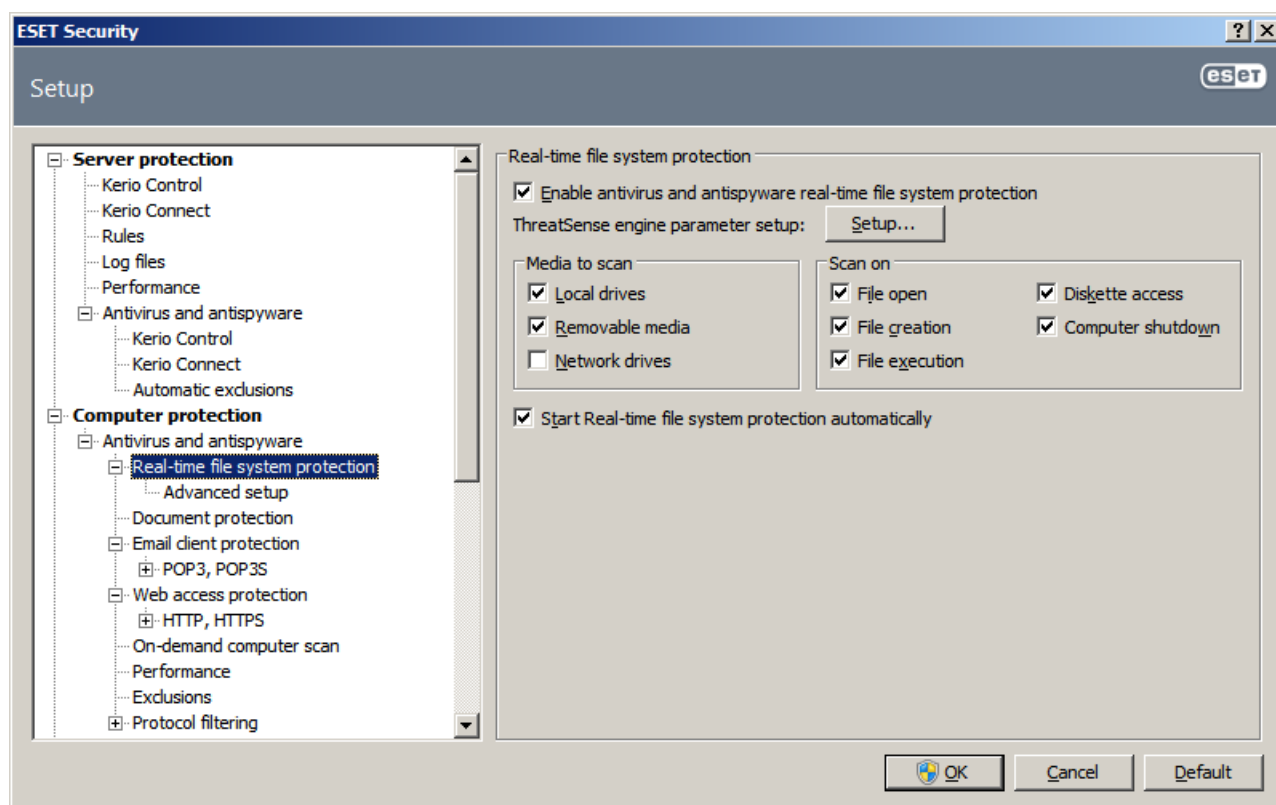
Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code at the moment they are opened, created or run on your computer. Real-time file system protection is launched at system startup.

4.1.1.1 Control setup

The Real-time file system protection checks all types of media, and control is triggered by various events. Using ThreatSense technology detection methods (as described in section [ThreatSense engine parameter setup](#)^[30]), 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.

To provide the minimum system footprint when using real-time protection, files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is configured using Smart optimization. If this is disabled, all files are scanned each time they are accessed. To modify this option, open the Advanced Setup window and click **Antivirus and antispyware > Realtime file system protection** from the Advanced Setup tree. Then click the **Setup...** button next to **ThreatSense engine parameter setup**, click **Other** and select or deselect the **Enable Smart optimization** option.

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), the real-time protection can be terminated by deselecting the **Start Real-time file system protection automatically** option.



4.1.1.1.1 Media to scan

By default, all types of media are scanned for potential threats.

Local drives – Controls all system hard drives

Removable media – Diskettes, USB storage devices, etc.

Network drives – Scans all mapped drives

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

4.1.1.1.2 Scan on (Event-triggered scanning)

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

The **Diskette access** option provides control of the diskette boot sector when this drive is accessed. The **Computer shutdown** option provides control of the hard disk boot sectors during computer shutdown. Although boot viruses are rare today, we recommend that you leave these options enabled, as there is still the possibility of infection by a boot virus from alternate sources.

4.1.1.1.3 Advanced scan options

More detailed setup options can be found under **Computer protection > Antivirus and antispyware > Real-time system protection > Advanced setup**.

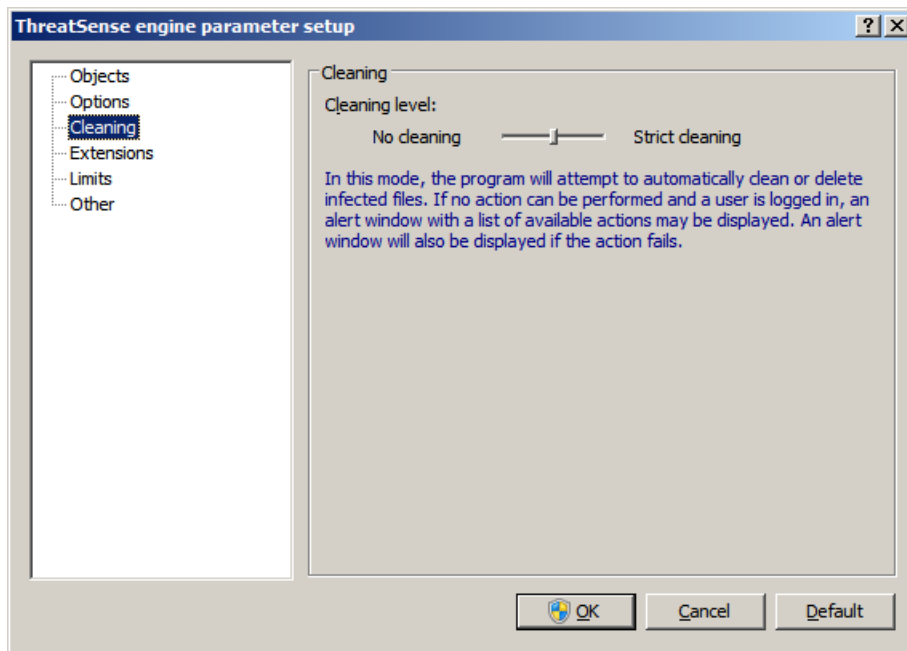
Additional ThreatSense parameters for newly created and modified files – The probability of infection in newly-created or modified files is comparatively higher than in existing files. That is why the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics are used, which greatly improves detection rates. In addition to newly-created files, scanning is also performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, deselect the Default archive scan settings option.

Additional ThreatSense.Net parameters for executed files – By default, advanced heuristics are not used when files are executed. However, in some cases you may want to enable this option (by checking the **Advanced heuristics on file execution** option). Note that advanced heuristics may slow the execution of some programs due to increased system requirements.

4.1.1.2 Cleaning levels

Real-time protection has three cleaning levels. To select a cleaning level, click the **Setup...** button in the **Real-time file system protection** section and then click the **Cleaning** branch.

- The first level, **No cleaning**, displays an alert window with available options for each infiltration found. You must choose an action for each infiltration individually. This level is designed for more advanced users who know which steps to take in the event of an infiltration.
- The default level automatically chooses and performs a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a message located in the bottom right corner of the screen. Automatic actions are not performed when the infiltration is located within an archive (which also contains clean files) or when infected objects do not have a predefined action.
- The third level, **Strict cleaning**, is the most “aggressive” – all infected objects are cleaned. As this level could potentially result in the loss of valid files, we recommend that it be used only in specific situations.



4.1.1.3 When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Therefore, please be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases. For example, if there is a conflict with a certain application or real-time scanner of another antivirus program.

After the installation of ESET Security for Kerio, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click the **Default** button located at the bottom-right of the **Real-time file system protection** window (**Advanced Setup > Antivirus and antispyware > Real-time file system protection**).

4.1.1.4 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a special harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file eicar.com is available for download at <http://www.eicar.org/download/eicar.com>

NOTE: Before performing a real-time protection check, it is necessary to disable the firewall. If the firewall is enabled, it will detect the file and prevent test files from downloading.

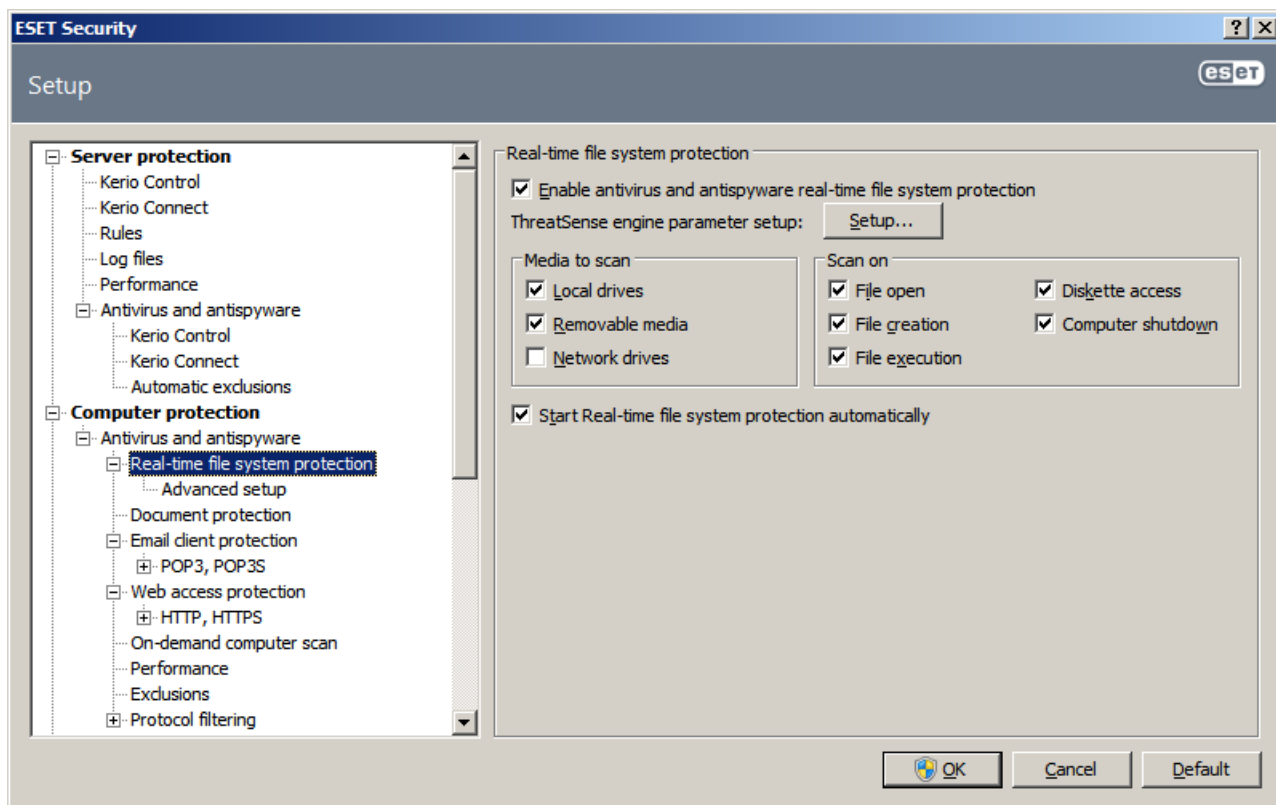
4.1.1.5 What to do if real-time protection does not work

In the next 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 was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup > Antivirus and antispyware** and click **Enable in the Real-time file system protection** section of the main program window.

If real-time protection is not initiated at system startup, it is probably due to the disabled option **Automatic real-time file system protection startup**. To enable this option, navigate to **Advanced Setup (F5)** and click **Real-time file system protection** in the **Advanced Setup** tree. In the **Advanced setup** section at the bottom of the window, make sure that the **Start Real-time file system protection automatically** checkbox is selected.



If 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 on your system.

Real-time protection does not start

If real-time protection is not initiated at system startup (and the **Start Real-time file system protection automatically** option is enabled), it may be due to conflicts with other programs. If this is the case, please consult ESET's Customer Care specialists.

4.1.2 Email client protection

Email protection provides control of email communication received through the POP3 protocol. Using the plug-in program for Microsoft Outlook, ESET Security for Kerio provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP).

When examining incoming messages, the program uses all advanced scanning methods provided by 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 protocol communications is independent of the email client used.

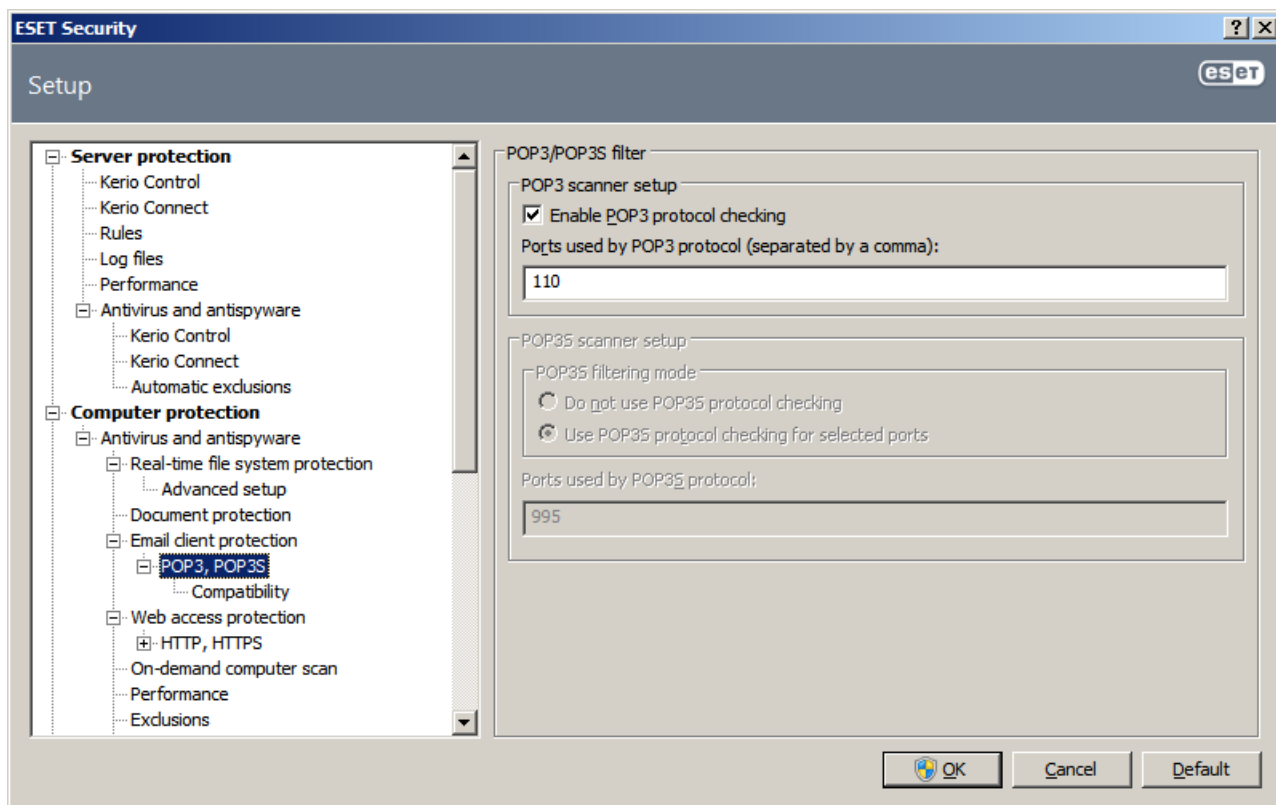
4.1.2.1 POP3 checking

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET Security for Kerio 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. For the module to work correctly, please make sure it is enabled – POP3 checking is performed automatically with no need for reconfiguration of the 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.

Encrypted communication is not controlled.

To be able to use the POP3/POP3S filtering you need to enable Protocol filtering first. If the POP3/POP3S options are grayed out, navigate to **Computer protection > Antivirus and antispyware > Protocol filtering** from within the advanced setup tree and check **Enable application protocol content filtering**. See the Protocol filtering section for more details on filtering and configuration.



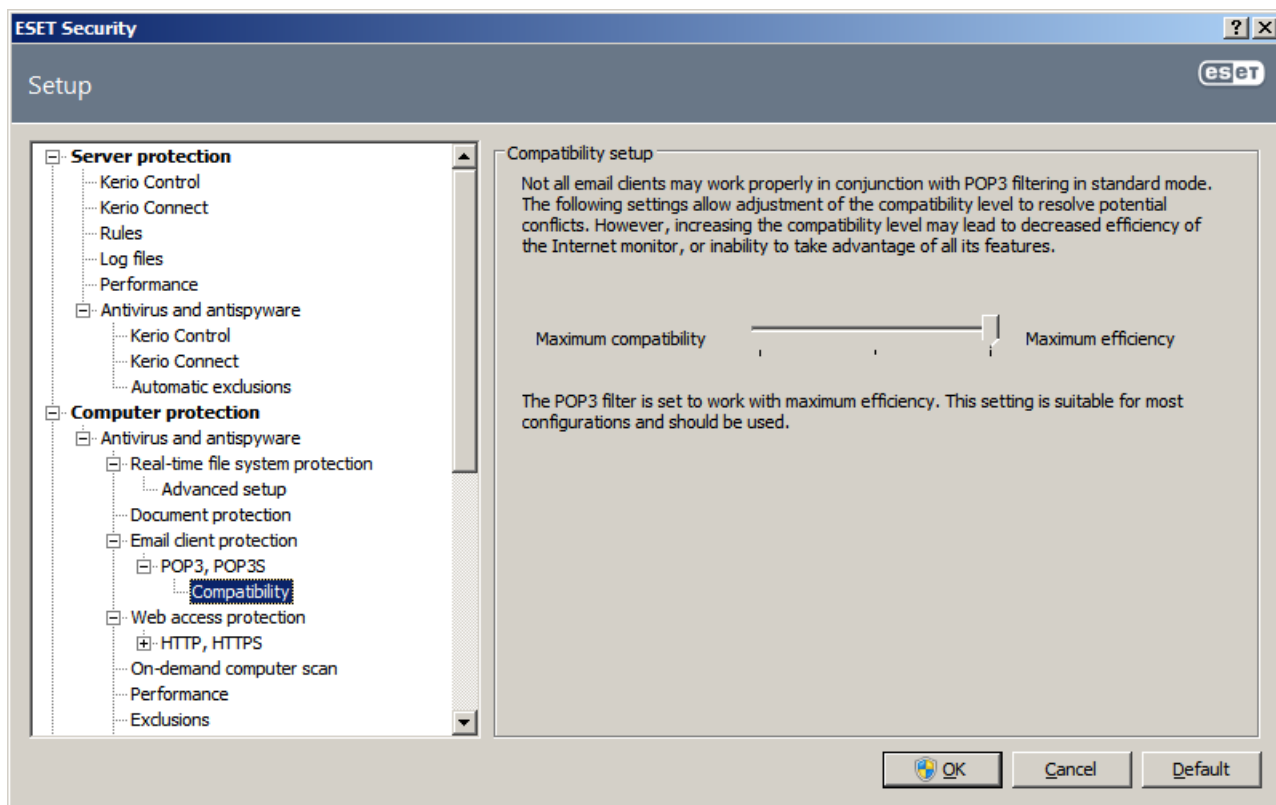
4.1.2.1.1 Compatibility

Certain email programs may experience problems with POP3 filtering (e.g., if receiving messages with a slow Internet connection, timeouts may occur due to checking). If this is the case, try modifying the way control is performed. Decreasing the control level may improve the speed of the cleaning process. To adjust the control level of POP3 filtering, from the Advanced Setup tree, navigate to **Antivirus and antispyware > Email protection > POP3, POP3s > Compatibility**.

If **Maximum efficiency** is enabled, infiltrations are removed from infected messages and information about the infiltration is inserted before the original email subject (the options **Delete** or **Clean** must be activated, or **Strict** or **Default** cleaning level must be enabled).

Medium compatibility modifies the way messages are received. Messages are gradually sent to the email client. After the message is transferred, it will be scanned for infiltrations. The risk of infection increases with this level of control. The level of cleaning and the handling of tag messages (notification alerts which are appended to the subject line and body of emails) is identical to the maximum efficiency setting.

With the **Maximum compatibility** level, you are warned by an alert window which reports the receipt of an infected message. No information about infected files is added to the subject line or to the email body of delivered messages and infiltrations are not automatically removed – you must delete infiltrations from the email client.

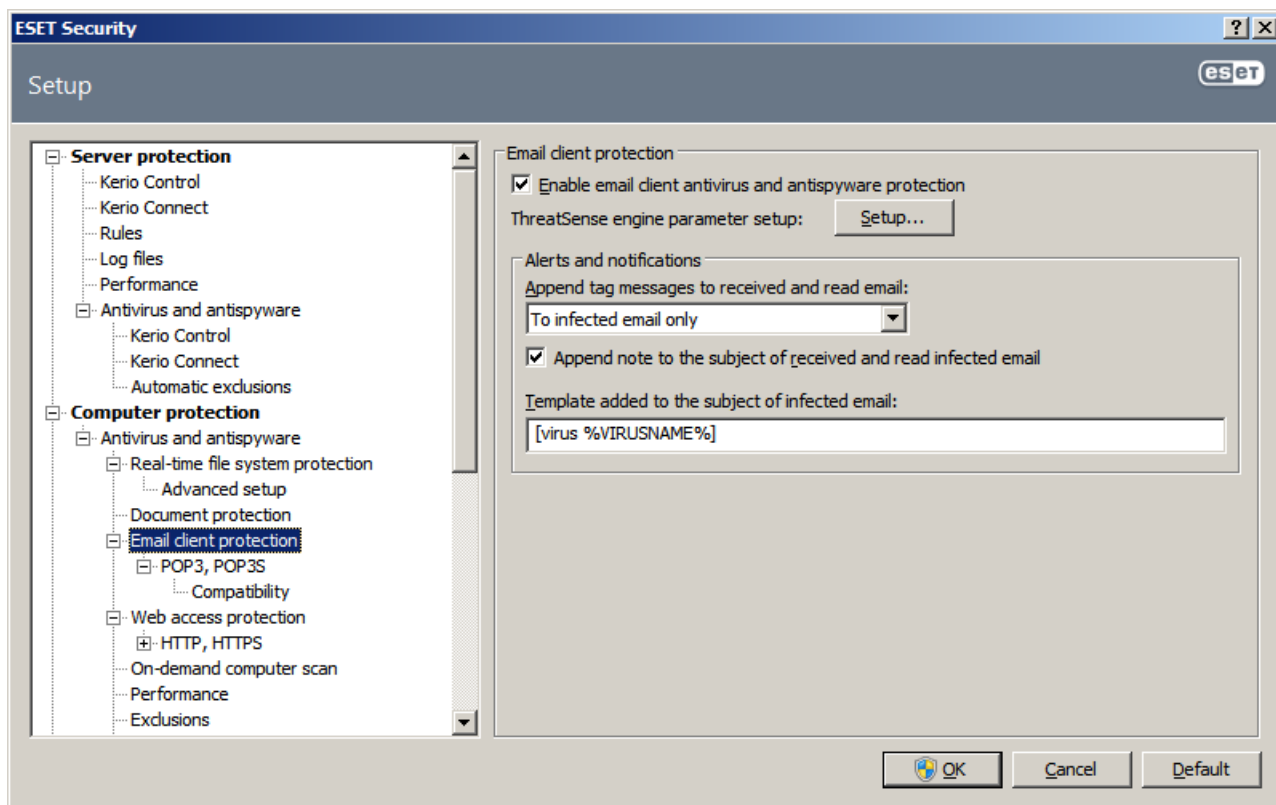


4.1.2.2 Integration with email clients

Integration of ESET Security for Kerio with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, this integration can be enabled in ESET Security for Kerio. If integration is activated, the ESET Security for Kerio toolbar is inserted directly into the email client, allowing for more efficient email protection. The integration settings are available through **Setup > Enter entire advanced setup tree... > Miscellaneous > Email client integration**. Email client integration allows you to activate integration with supported email clients. Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail and Mozilla Thunderbird.

Select the **Disable checking upon inbox content change** option if you are experiencing a system slowdown when working with your email client. Such a situation may take place when downloading email from Kerio Outlook Connector Store

Email protection is activated by clicking **Setup > Enter entire advanced setup tree... > Antivirus and antispyware > Email client protection** and selecting the **Enable email client antivirus and antispyware protection** option.



4.1.2.2.1 Appending tag messages to email body

Each email scanned by ESET Security for Kerio can be marked by appending a tag message to the subject or email body. This feature 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.

The options for this functionality are available through **Advanced setup > Antivirus and antispyware > Email client protection**. You can select to **Append tag messages to received and read mail**, as well as **Append tag messages to sent mail**. You also have the ability to decide whether tag messages are appended to all scanned email, to infected email only, or not at all.

ESET Security for Kerio also allows you to append messages to the original subject of infected messages. To enable appending to the subject, select both the **Append note to the subject of received and read infected email** and **Append note to the subject of sent infected email** options.

The content of notifications can be modified in the **Template added to the subject of infected email** field. The previously mentioned modifications can help automate the process of filtering infected email, as it allows you to filter email with a specific subject (if supported in your email client) to a separate folder.

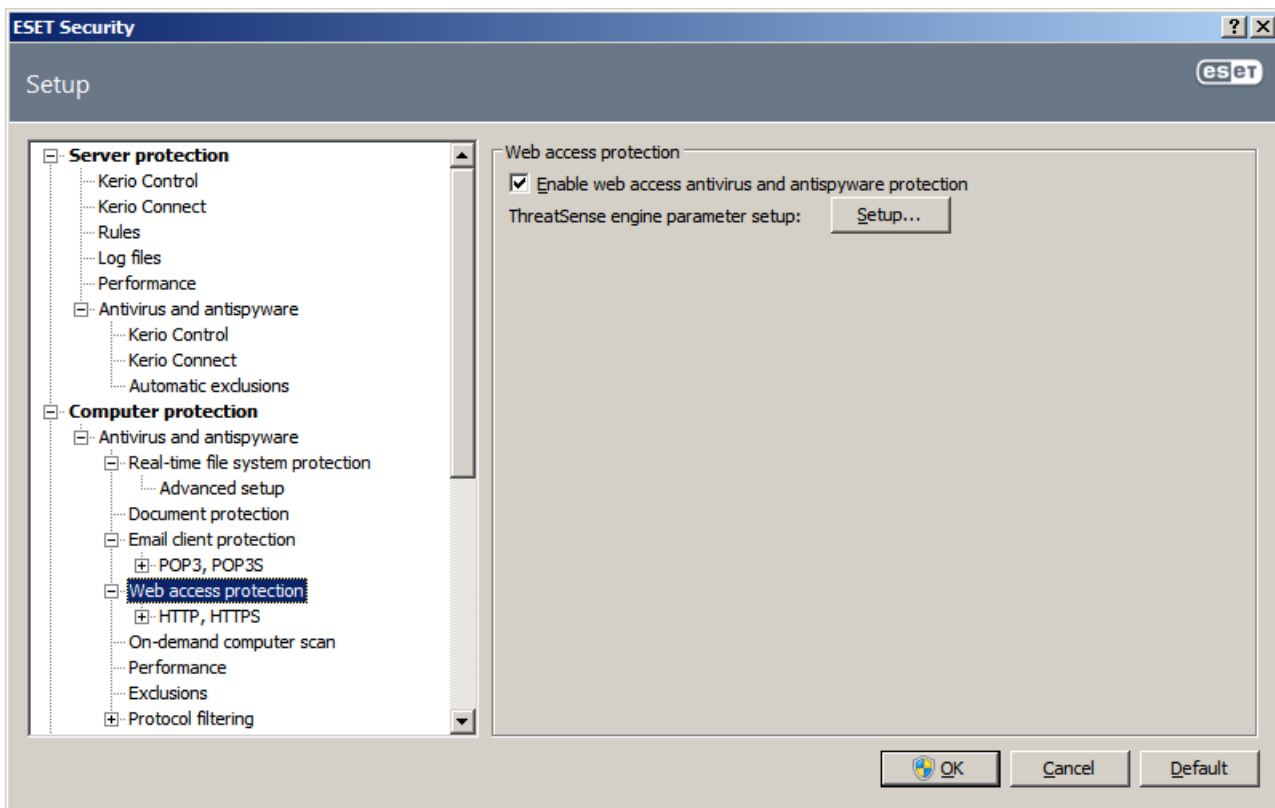
4.1.2.3 Removing infiltrations

If an infected email message is received, an alert window will display. The alert window shows the sender name, email and the name of the infiltration. In the lower part of the window the options **Clean**, **Delete** or **Leave** are available for the detected object. In almost all cases, we recommend that you select either **Clean** or **Delete**. In certain situations, if you wish to receive the infected file, select **Leave**.

If **Strict cleaning** is enabled, an information window with no options available for infected objects will displayed.

4.1.3 Web access protection

Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your Web access protection. We strongly recommend that the **Enable web access antivirus and antispysware protection** option is selected. This option is located in **Advanced Setup (F5) > Antivirus and antispysware > Web access protection**.

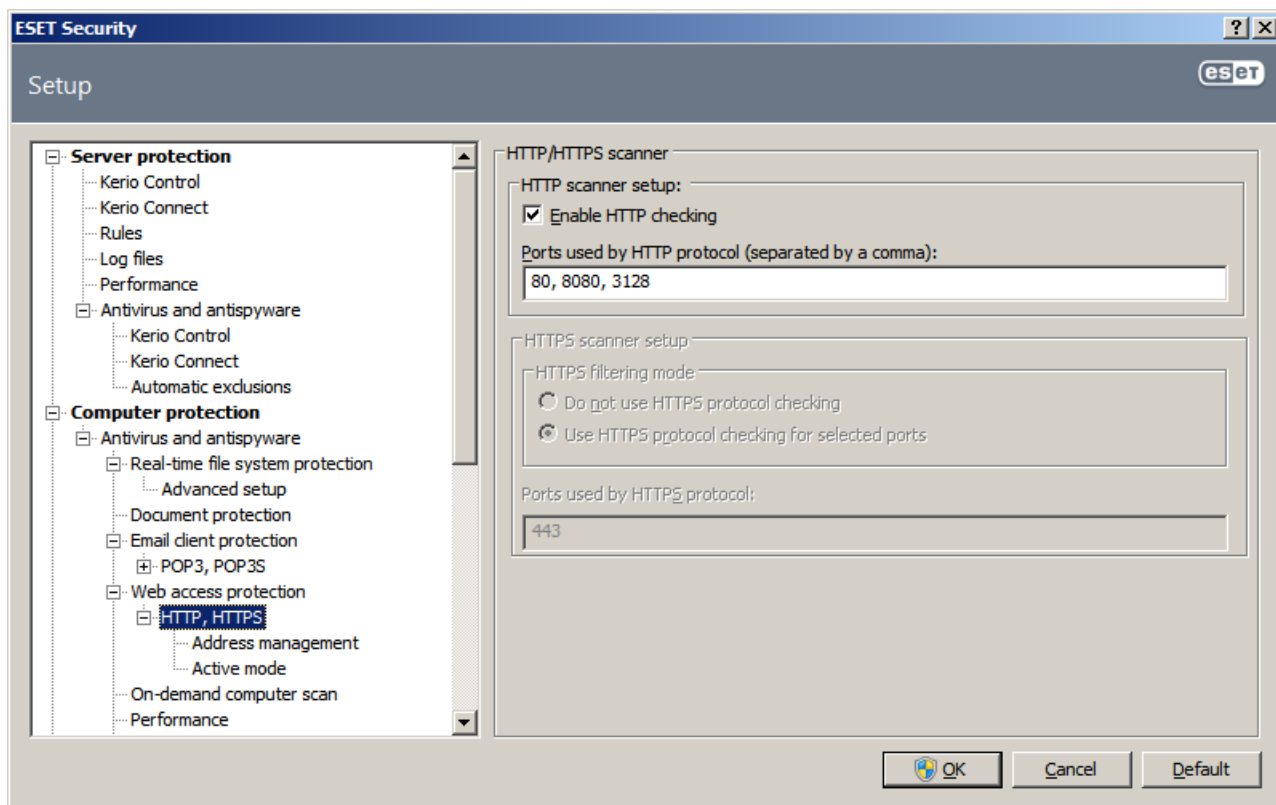


4.1.3.1 HTTP, HTTPS

Web access protection works by monitoring communication between Internet browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) rules. By default, ESET Security for Kerio is configured to use the standards of most Internet browsers. However, the HTTP scanner setup options can be modified in **Advanced Setup (F5) > Antivirus and antispysware > Web access protection > HTTP, HTTPS**. In the main HTTP filter window, you can select or deselect the **Enable HTTP checking** option. You can also define the port numbers used for HTTP communication. By default, the port numbers 80, 8080 and 3128 are predefined. HTTPS checking can be performed in the following modes:

Do not use HTTPS protocol checking – Encrypted communication will not be checked

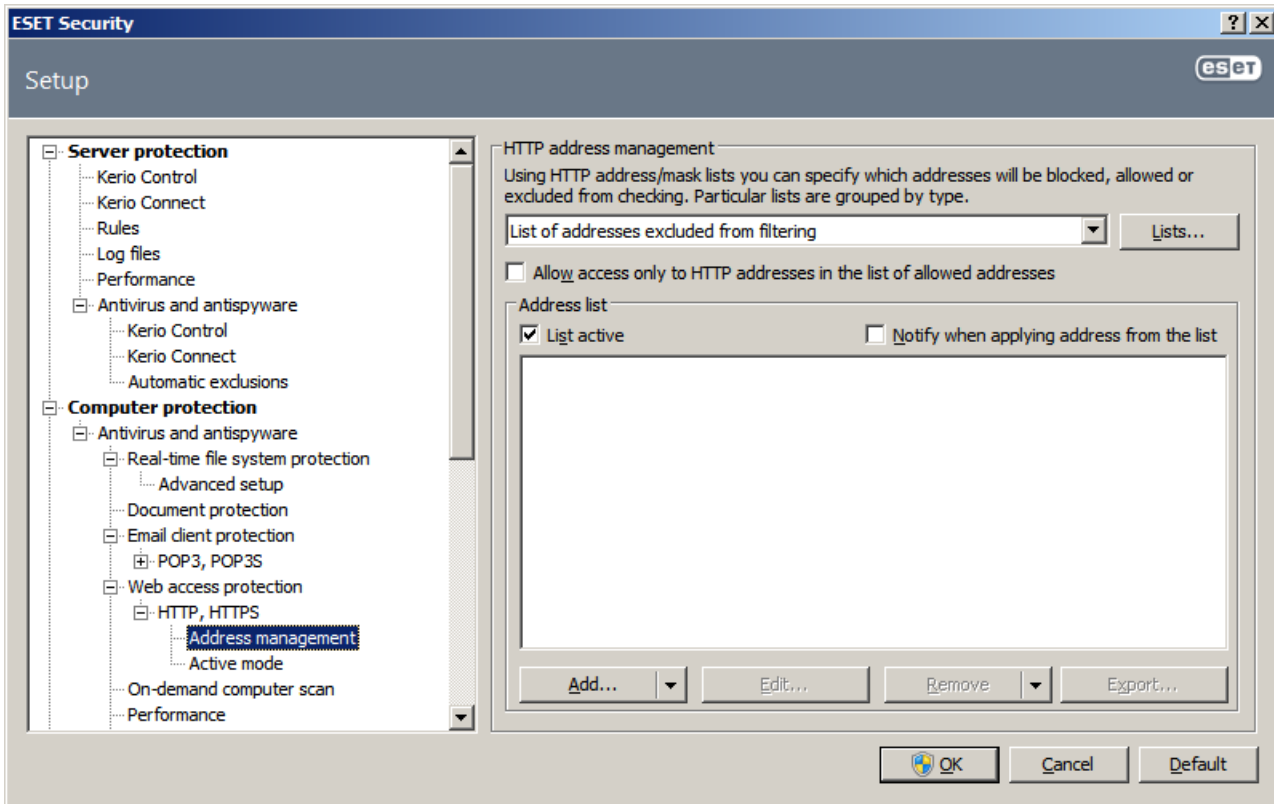
Use HTTPS protocol checking for selected ports – HTTPS checking only for ports defined in **Ports used by HTTPS protocol**



4.1.3.1.1 Address management

This section enables you to specify HTTP addresses to block, allow or exclude from checking. The buttons **Add...**, **Edit...**, **Remove** and **Export...** are used to manage the lists of addresses. 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. If you select the **Allow access only to HTTP addresses in the list of allowed addresses** option, only addresses present in the list of allowed addresses will be accessible, while all other HTTP addresses will be blocked.

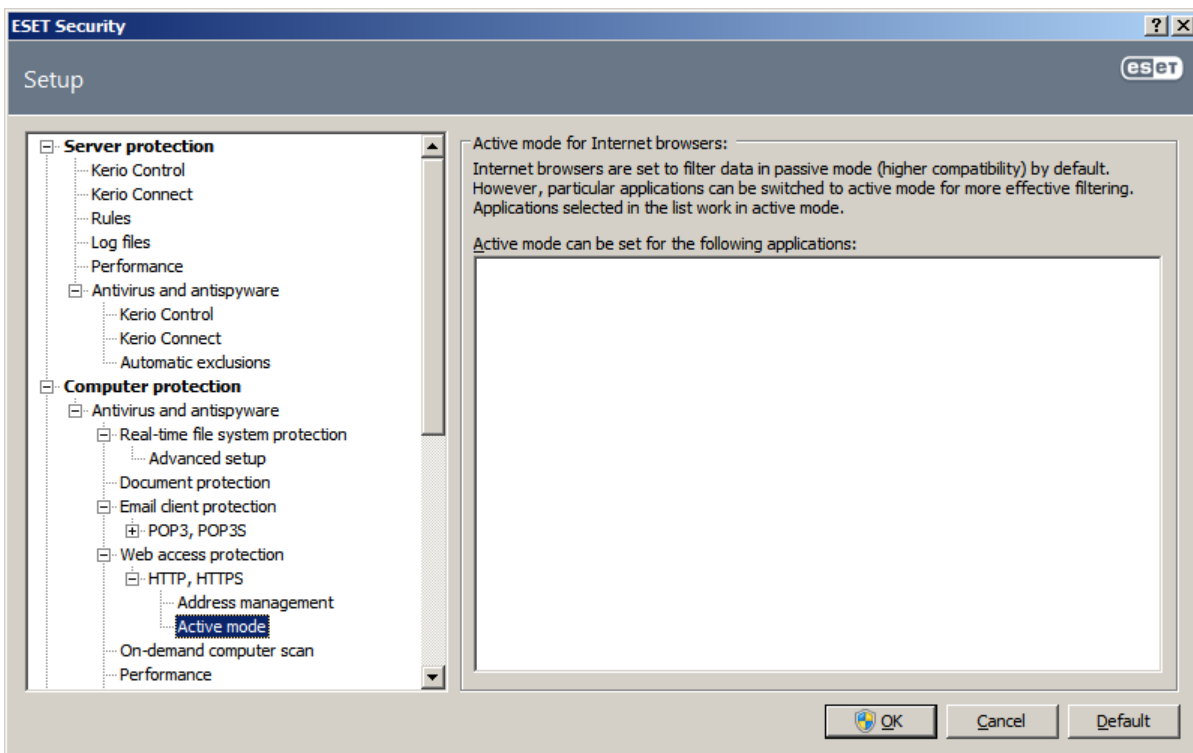
In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. To activate a list, select the **List active** option. If you wish to be notified when entering an address from the current list, select **Notify when applying address from the list** option.



4.1.3.1.2 Active mode

The list of applications marked as web browsers is accessible directly from the **Web browsers** submenu of the **HTTP, HTTPS** branch. This section also contains the **Active mode** submenu, which defines the checking mode for Internet browsers.

Active mode is useful because it examines transferred data as a whole. If it is not enabled, communication of applications is 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.



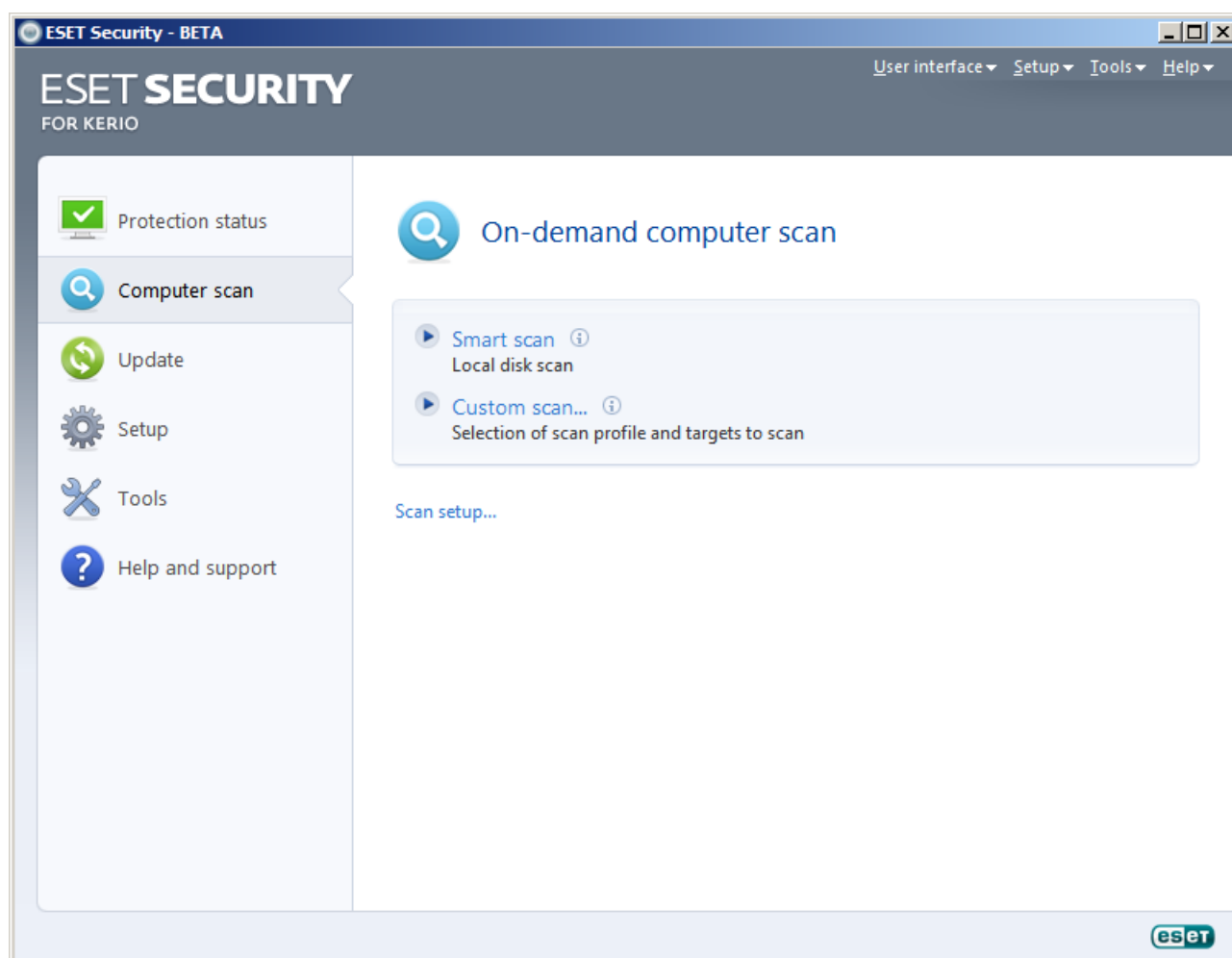
4.1.4 On-demand computer scan

If you suspect that your computer is infected (it behaves abnormally), run an On-demand computer scan to examine your computer for infiltrations. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. 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**.

4.1.4.1 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.



4.1.4.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantages are easy operation with no detailed scanning configuration. Smart scan checks all files on local drives 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 section [Cleaning](#)^[32].

4.1.4.1.2 Custom scan

Custom scan is an optimal solution if you wish to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. The configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.

To select scan targets, select **Computer scan > Custom scan** and select an option from the **Scan targets** drop-down menu or select specific 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 the **Scan without cleaning** option. Furthermore, you can choose from three cleaning levels by clicking **Setup... > Cleaning**.

4.1.4.2 Scan targets

The Scan targets drop-down menu allows you to select files, folders and devices (disks) to be scanned for viruses.

By profile settings – Selects targets set in the selected scan profile

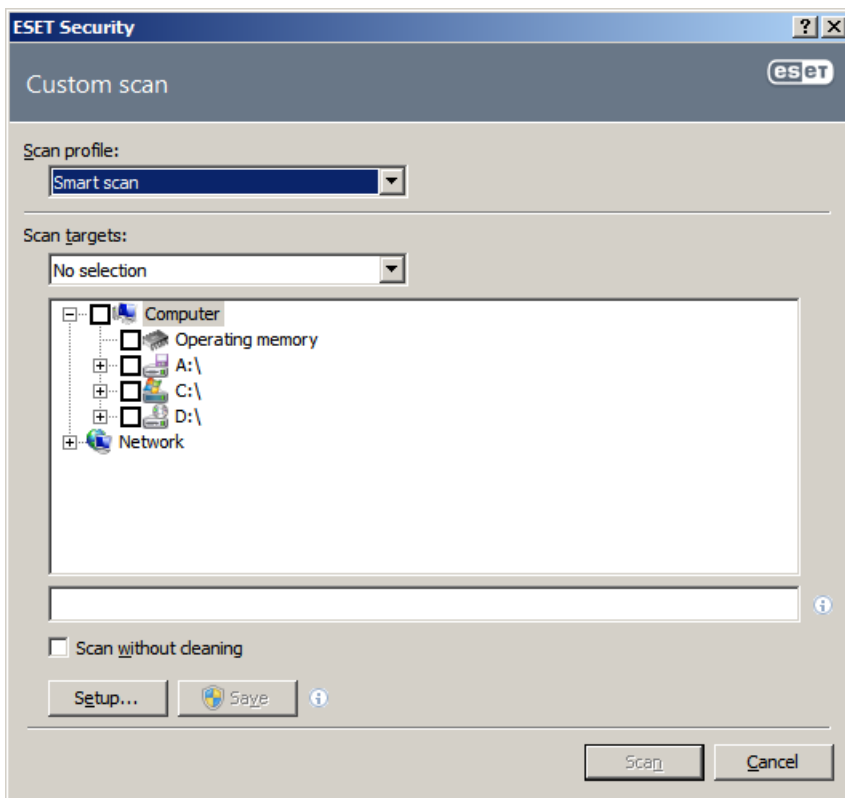
Removable media – Selects diskettes, USB storage devices, CD/DVD

Local drives – Selects all system hard drives

Network drives – Selects all mapped drives

No selection – Cancels all selections

A scan target can also be more precisely specified by entering the path to the folder or file(s) you wish to include in scanning. Select targets from the tree structure listing all devices available on the computer.

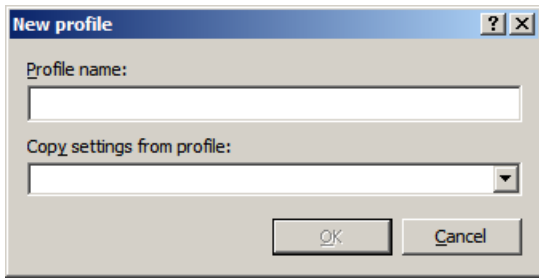


4.1.4.3 Scan profiles

Your preferred scan parameters 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, open the Advanced Setup window (F5) and click **On-demand computer scan > Profiles...** The **Configuration profiles** window has a drop-down menu of existing scan profiles as well as the option to create a new one. To help you create a scan profile to fit your needs, see section [ThreatSense engine parameters setup](#)^[30] 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 don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. From the **Configuration profiles** window, click the **Add...** button. Enter the name of your new profile in the **Profile name** field, and select **Smart scan** from the **Copy settings from profile:** drop-down menu. Then adjust the remaining parameters to meet your requirements.



4.1.4.4 Command Line

ESET Security for Kerio's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file.

The following parameters and switches can be used while running the On-demand scanner from the command line:

General options:

- | | |
|---------------------|-----------------------------------|
| – help | show help and quit |
| – version | show version information and quit |
| – base-dir = FOLDER | load modules from FOLDER |
| – quar-dir = FOLDER | quarantine FOLDER |
| – aind | show activity indicator |

Targets:

- | | |
|-----------------------------|--|
| – files | scan files (default) |
| – no-files | do not scan files |
| – boots | scan boot sectors (default) |
| – no-boots | do not scan boot sectorsk |
| – arch | scan archives (default) |
| – no-arch | do not scan archives |
| – max-archive-level = LEVEL | maximum archive nesting LEVEL |
| – scan-timeout = LIMIT | scan archives for LIMIT seconds at maximum. If the scanning time reaches this limit, the scanning of the archive is stopped and the scan will continue with the next file. |
| – max-arch-size=SIZE | scan only the first SIZE bytes in archives (default 0 = |

– mail	unlimited)
– no-mail	scan email files
– sfx	do not scan email files
– no-sfx	scan self-extracting archives
– rtp	do not scan self-extracting archives
– no-rtp	scan runtime packers
– exclude = FOLDER	do not scan runtime packers
– subdir	exclude FOLDER from scanning
– no-subdir	scan subfolders (default)
– max-subdir-level = LEVEL	do not scan subfolders
– symlink	maximum subfolder nesting LEVEL (default 0 = unlimited)
– no-symlink	follow symbolic links (default)
– ext-remove = EXTENSIONS	skip symbolic links
– ext-exclude = EXTENSIONS	exclude EXTENSIONS delimited by colon from scanning
Methods:	
– adware	scan for Adware/Spyware/Riskware
– no-adware	do not scan for Adware/Spyware/Riskware
– unsafe	scan for potentially unsafe applications
– no-unsafe	do not scan for potentially unsafe applications
– unwanted	scan for potentially unwanted applications
– no-unwanted	do not scan for potentially unwanted applications
– pattern	use signatures
– no-pattern	do not use signatures
– heur	enable heuristics
– no-heur	disable heuristics
– adv-heur	enable advanced heuristics
– no-adv-heur	disable advanced heuristics
Cleaning:	
– action = ACTION	perform ACTION on infected objects. Available actions: none, clean, prompt
– quarantine	copy infected files to Quarantine (supplements ACTION)
– no-quarantine	do not copy infected files to Quarantine
Logs:	
– log-file=FILE	log output to FILE
– log-rewrite	overwrite output file (default – append)

– log-all	log also clean files
– no-log-all	do not log clean files (default)

Possible exit codes of the scan:

0	– no threat found
1	– threat found but not cleaned
10	– some infected files remained
101	– archive error
102	– access error
103	– internal error

NOTE: Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

4.1.5 Performance

In this section, you can set the number of ThreatSense scan engines that will be used for virus scanning. More ThreatSense scan engines on multiprocessor machines can increase the scanning rate. Acceptable value is 1-20.

If there are no other restrictions, our recommendation is to increase the number of ThreatSense scan engines in the Advanced settings window (F5) under **Computer protection > Antivirus and antispyware > Performance**, according to this formula: *number of ThreatSense scan engines = (number of physical CPUs x 2) + 1*. Here is an example:

Let's say you have a server with 4 physical CPUs. For the best performance, according to formula above, you should have 9 scan engines.

NOTE: Changes made here will be applied only after restart.

4.1.6 Protocol filtering

Antivirus protection, for the POP3 and HTTP application protocols, is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. The control works automatically, regardless of the Internet browser or email client used. The following options are available for protocol filtering (if the **Enable application protocol content filtering** option is selected):

HTTP and POP3 ports - Limits scanning of communication to known HTTP and POP3 ports.

Applications marked as Internet browsers and email clients – Enable this option to only filter communication of applications marked as browsers (**Web access protection > HTTP, HTTPS > Web browsers**) and email clients (**Email client protection > POP3, POP3s > Email clients**).

Ports and applications marked as Internet browsers or email clients – Both ports and browsers are checked for malware.

NOTE: Starting with Windows Vista Service Pack 1 and Windows Server 2008, a new communication filtering method is used. As a result, the Protocol filtering section is not available.

4.1.6.1 SSL

ESET Security for Kerio enables you to check protocols encapsulated in SSL protocol. You can use various scanning modes for SSL protected communications using trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Always scan SSL protocol – Select this option to scan all SSL protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified about the fact and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked by you as trusted (it is added to the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

Ask about non-visited sites (exclusions can be set) - If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode enables you to create a list of SSL certificates that will

be excluded from scanning.

Do not scan SSL protocol - If selected, the program will not scan communications over SSL.

If the certificate cannot be verified using the Trusted Root Certification Authorities store (**protocol filtering > SSL > Certificates**):

Ask about certificate validity – Prompts you to select an action to take.

Block communication that uses the certificate – Terminates connection to the site that uses the certificate.

If the certificate is invalid or corrupt (**protocol filtering > SSL > Certificates**):

Ask about certificate validity – Prompts you to select an action to take.

Block communication that uses the certificate – Terminates connection to the site that uses the certificate.

4.1.6.1.1 Trusted certificates

In addition to the integrated Trusted Root Certification Authorities store where ESET Security for Kerio stores trusted certificates, you can create a custom list of trusted certificates that can be viewed in **Advanced Setup (F5) > Protocol filtering > SSL > Certificates > Trusted certificates**.

4.1.6.1.2 Excluded certificates

The Excluded certificates section contains certificates that are considered safe. The content of encrypted communications utilizing the certificates in the list will not be checked for threats. We recommend excluding only those web certificates that are guaranteed to be safe and the communication utilizing the certificates does not need to be checked.

4.1.7 ThreatSense engine parameters setup

ThreatSense is the name of the technology consisting of 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) which 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 eliminates 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.

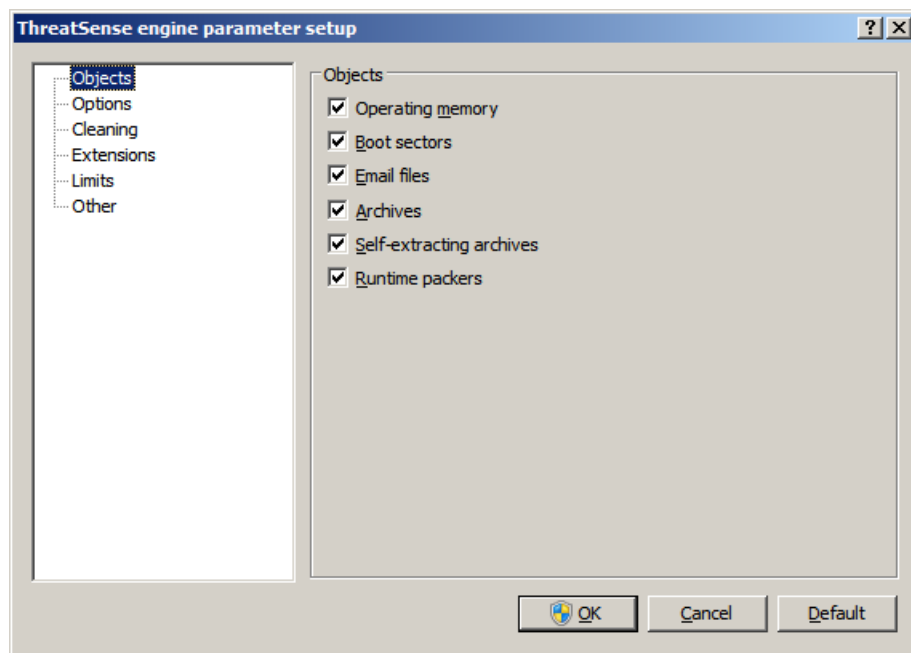
To enter the setup window, click the **Setup...** button located in any module's setup window which uses ThreatSense technology (see below). Different security scenarios could require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- [Real-time file system protection](#) ^[15]
- System startup file check
- [On-demand computer scan](#) ^[25]

The ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except On-demand computer scan.

4.1.7.1 Objects setup

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



Operating memory – Scans for threats that attack the operating memory of the system.

Boot sectors – Scans boot sectors for the presence of viruses in the master boot record.

Files – Provides scanning for all common file types (programs, pictures, audio, video files, database files, etc.).

Email files – Scans special files where email messages are contained.

Archives – Provides scanning for files compressed in archives (.rar, .zip, .arj, .tar, etc.).

Self-extracting archives – Scans files which are contained in self-extracting archive files, but typically presented with an .exe file extension

Runtime packers – Runtime packers (unlike standard archive types) decompress in memory, in addition to standard static packers (UPX, yoda, ASPack, FGS, etc.).

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.2 Options

In the **Options** section, you can select the methods to be used when scanning the system for infiltrations. The following options are available:

Signatures – Signatures can exactly and reliably detect and identify infiltrations by their name using virus signatures.

Heuristics – Heuristics use an algorithm that analyses 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).

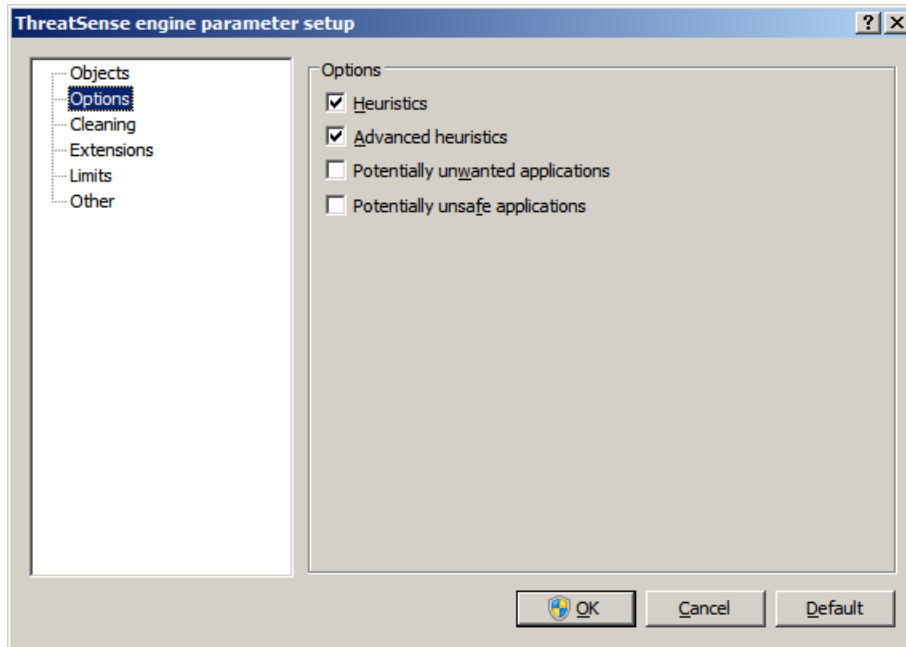
Advanced heuristics – Advanced heuristics comprise a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. Due to advanced heuristics, the detection intelligence of the program is significantly higher.

Adware/Spyware/Riskware – This category includes software which collects various sensitive information about users without their informed consent. This category also includes software which displays advertising material.

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 state before their installation). 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.

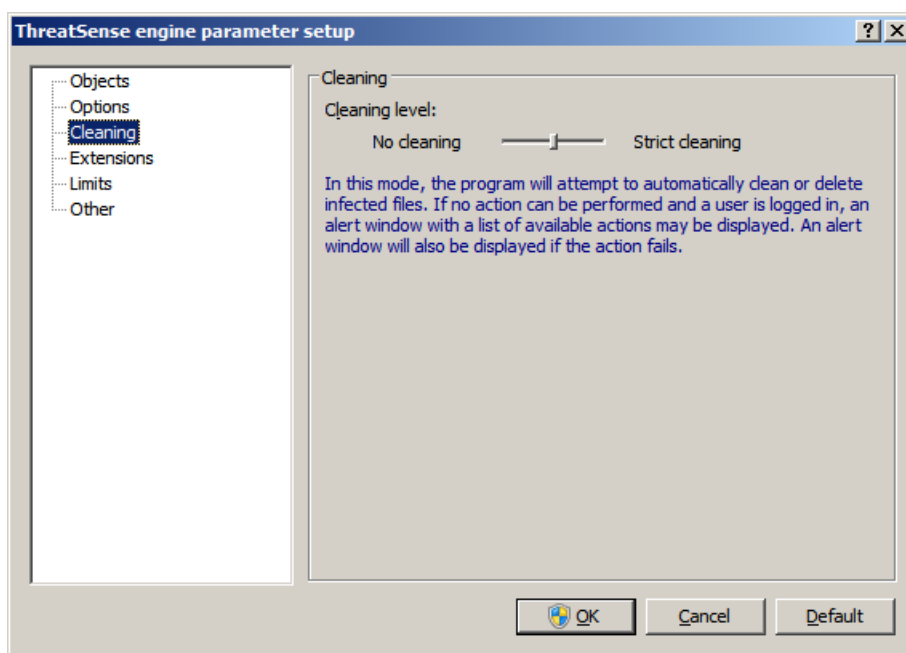
Potentially unsafe applications – Potentially unsafe applications is the classification used for commercial, legitimate software. It includes programs such as remote access tools, which is why this option is disabled by default.



NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.3 Cleaning

The cleaning settings determine the behavior of the scanner during the cleaning of 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.

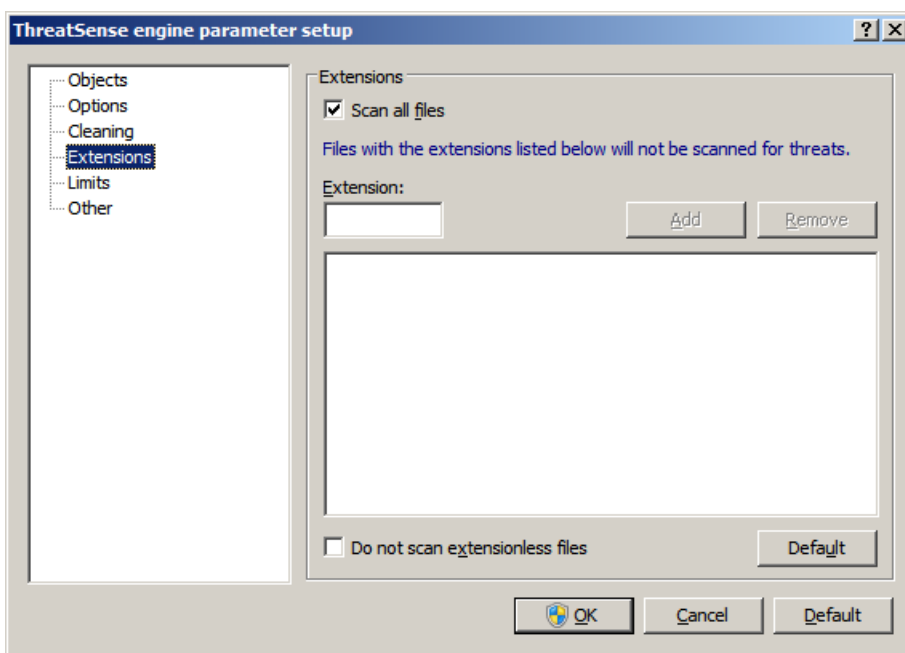
Strict cleaning – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean them, you will be offered an action to take in a warning window.

Warning: In the Default mode, the entire archive file is deleted only if all files in the archive are infected. If the archive also contains legitimate 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.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.4 Extensions

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



By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. If the **Scan all files** option is deselected, the list changes to show all currently scanned file extensions. Using the **Add** and **Remove** buttons, you can enable or prohibit scanning of desired extensions.

To enable scanning of files with no extension, select the **Scan extensionless files** option.

Excluding files from scanning is sometimes necessary if scanning certain file types prevents the program which is using the extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using Microsoft Exchange servers.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.5 Limits

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

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

Maximum scan time for object (sec.): – Defines the maximum time value 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, regardless of whether the scan has finished.

Archive 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 size of file in archive: – 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 this causes scanning an archive to be prematurely terminated, the archive will remain unchecked.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.6 Other

Scan alternate data streams (ADS) – Alternate data streams (ADS) used by the NTFS file system are file and folder associations which are invisible from ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.

Run background scans with low priority – Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects – If this option is selected, the log file will show all the scanned files, even those not infected.

Enable Smart optimization – Select this option so that files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update.

Preserve last access timestamp – Select this option to keep the original access time of scanned files instead of updating it (e.g., for use with data backup systems).

Scroll log – This option allows you to enable/disable log scrolling. If selected, information scrolls upwards within the display window.

Display notification about scan completion in a separate window – Opens a standalone window containing information about scan results.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.8 An infiltration is detected

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

If your computer is showing signs of malware infection, e.g., it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET Security for Kerio and click Computer scan
- Click **Smart scan** (for more information, see section [Smart scan](#) ^[25])
- 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 in ESET Security for Kerio, suppose that an infiltration is detected by the real-time file system monitor, which uses the Default cleaning level. It will attempt to clean or delete the file. If there is no predefined action to take for the real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **Leave** are available. Selecting **Leave** is not recommended, since the infected file(s) would be left untouched. The exception to this is 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 which has attached malicious code to the file. 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.



If an infected file is "locked" or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

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.

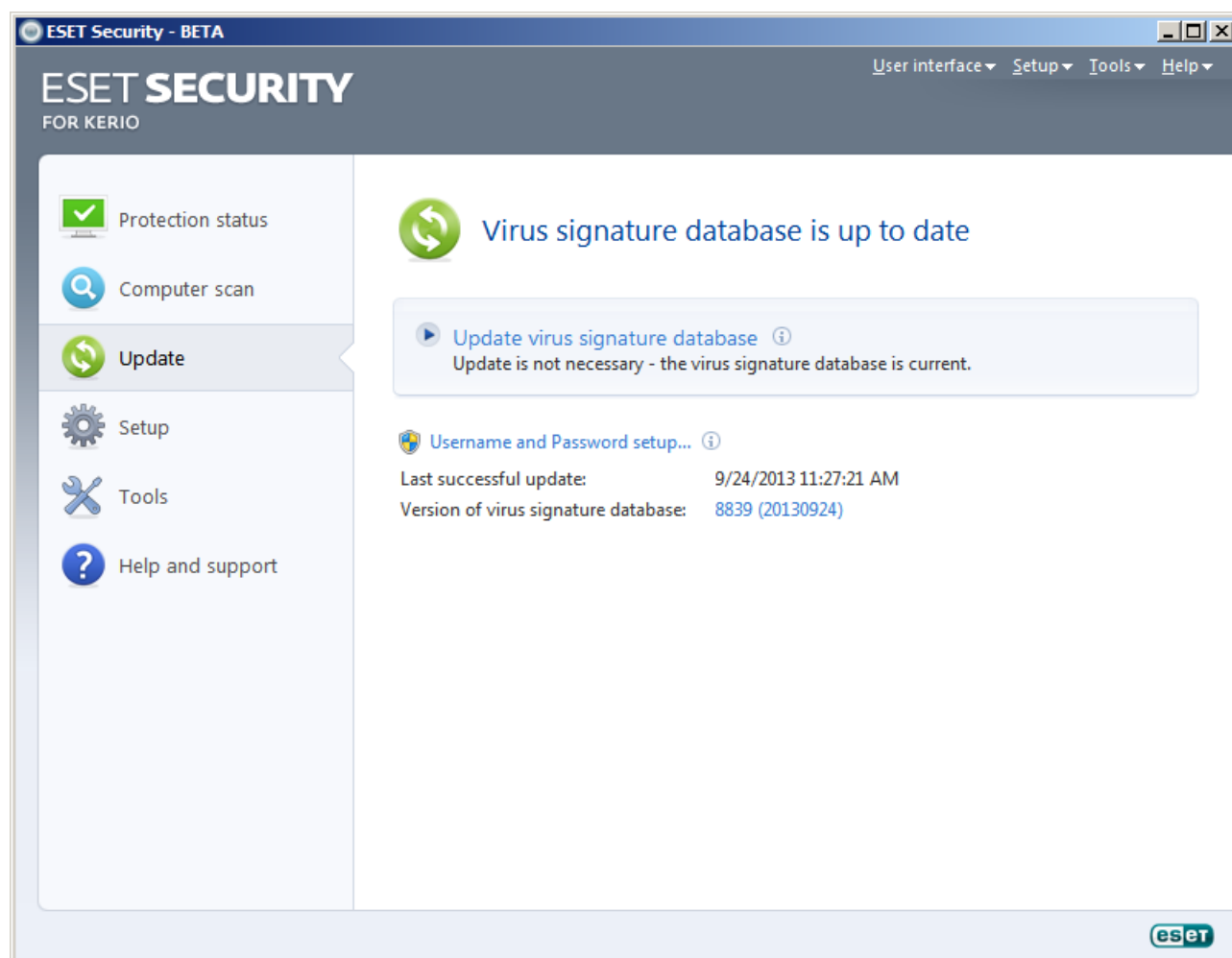
4.2 Updating the program

Regular updating of ESET Security for Kerio is the basic premise for obtaining the maximum level of security. The Update module ensures that the program is always up to date in two ways – by updating the virus signature database and by updating system components.

By clicking **Update** from the main menu, you can find the current update status, including the date and time of the last successful update and if an update is needed. The primary window also contains the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added within the given update.

In addition, the option to manually begin the update process – **Update virus signature database** – is available, as well as basic update setup options such as the username and password to access ESET's update servers.

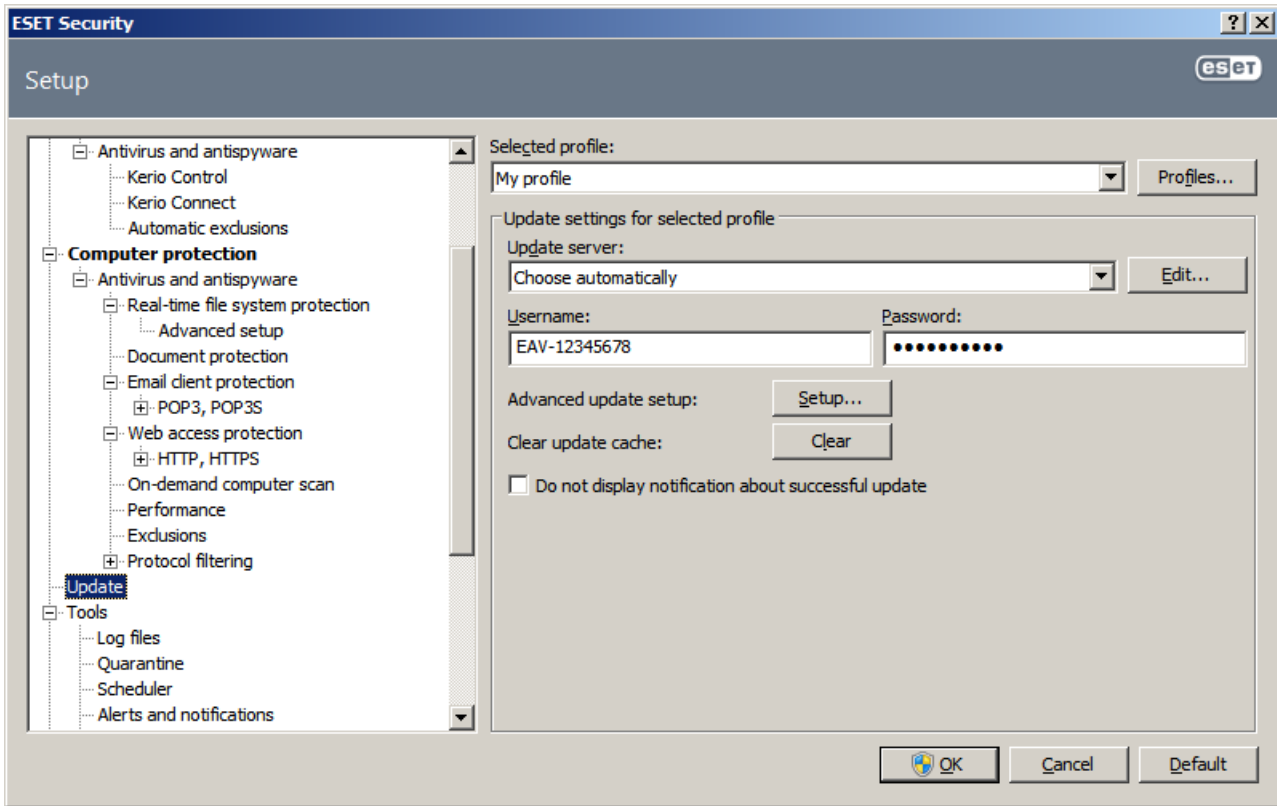
Use the **Product activation** link to open a registration form that will activate your ESET security product and send you an email with your authentication data (username and password).



NOTE: The username and password are provided by ESET after purchasing ESET Security for Kerio.

4.2.1 Update setup

The update setup section specifies update source information such as the update servers and authentication data for these servers. By default, the **Update server** drop-down menu is set to **Choose automatically** to ensure that update files will automatically download from the ESET server with the least network traffic. The update setup options are available from the Advanced Setup tree (F5 key), under **Update**.

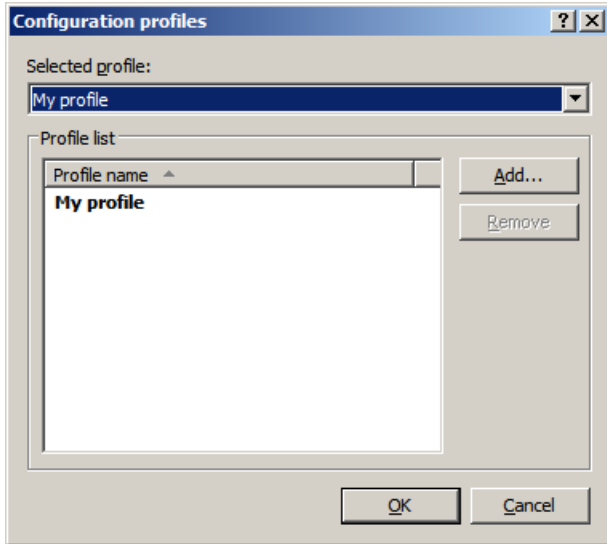


The list of available update servers is accessible via the **Update server** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button. Authentication for update servers is based on the **Username** and **Password** generated and sent to you after purchase.

4.2.1.1 Update profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users, who can create an alternative profile for Internet connection properties that regularly change.

The **Selected profile** drop-down menu displays the currently selected profile, set to **My profile** by default. To create a new profile, click the **Profiles...** button and then click the **Add...** button and enter your own **Profile name**. When creating a new profile, you can copy settings from an existing one by selecting it from the **Copy settings from profile** drop-down menu.



In the profile setup window, you can specify the update server from a list of available servers or add a new server. The list of existing update servers is accessible via the **Update server:** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button.

4.2.1.2 Advanced update setup

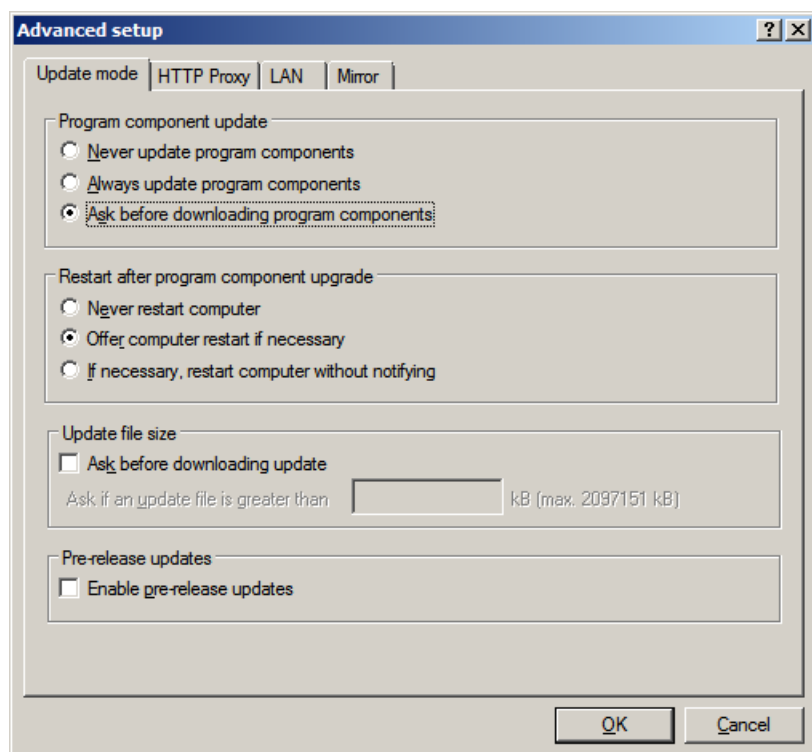
To view the Advanced update setup, click the **Setup...** button. Advanced update setup options include configuration of **Update mode**, **HTTP Proxy**, **LAN** and **Mirror**.

4.2.1.2.1 Update mode

The **Update mode** tab contains options related to the program component update.

In the **Program component update** section, three options are available:

- **Never update program components:** New program component updates will not be downloaded.
- **Always update program components:** New program component updates will occur automatically.
- **Ask before downloading program components:** The default option. You will be prompted to confirm or refuse program component updates when they are available.



After a program component update, it may be necessary to restart your computer to provide full functionality of all modules. The **Restart after program component upgrade** section allows you to select one of the following options:

- **Never restart computer**
- **Offer computer restart if necessary**
- **If necessary, restart computer without notifying**

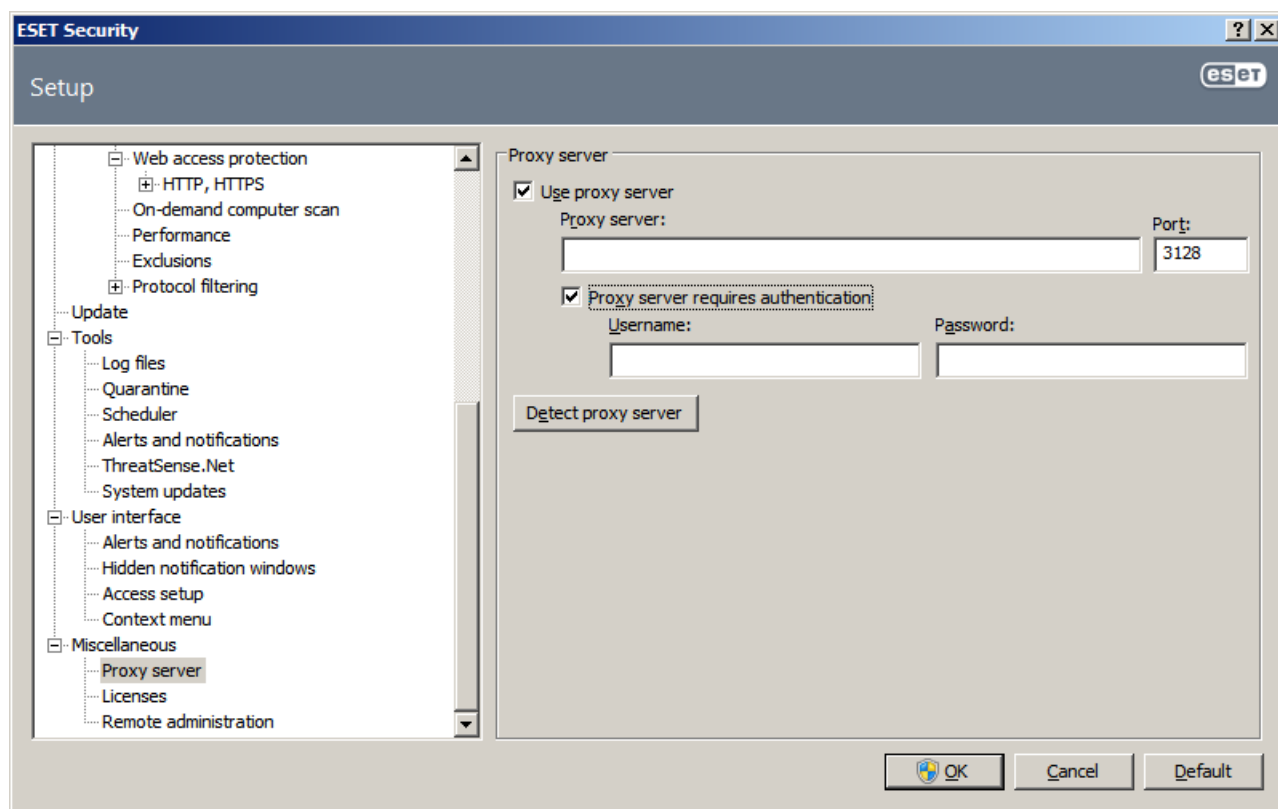
The default option is **Offer computer restart if necessary**. Selection of the most appropriate option depends on the workstation where the settings will be applied. Please be aware that there are differences between workstations and servers – e.g., restarting the server automatically after a program upgrade could cause serious damage.

4.2.1.2.2 Proxy server

In ESET Security for Kerio, proxy server setup is available in two different sections within the Advanced Setup tree.

First, proxy server settings can be configured under **Miscellaneous > Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Security for Kerio. Parameters here will be used by all modules requiring connection to the Internet.

To specify proxy server settings for this level, select the **Use proxy server** checkbox and then enter the address of the proxy server into the **Proxy server:** field, along with the **Port** number of the proxy server.



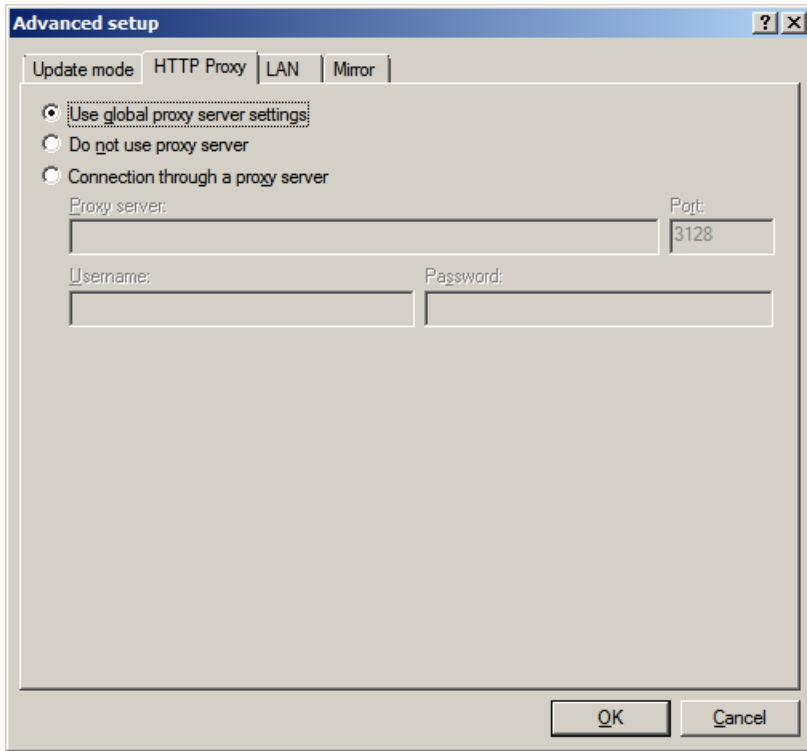
If communication with the proxy server requires authentication, select the **Proxy server requires authentication** checkbox and enter a valid **Username** and **Password** into the respective fields. Click the **Detect proxy server** button to automatically detect and insert proxy server settings. The parameters specified in Internet Explorer will be copied.

NOTE: This feature does not retrieve authentication data (username and password), it must be supplied by you.

Proxy server settings can also be established within Advanced update setup. This setting applies for the given update profile. You can access the proxy server setup options for a given update profile by clicking on the **HTTP Proxy** tab in **Advanced update setup**. You will have one of the three following options:

- **Use global proxy server settings**
- **Do not use proxy server**
- **Connection through a proxy server** (connection defined by the connection properties)

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified within the **Miscellaneous > Proxy server** branch of the Advanced Setup tree (as described at the top of this article).



Select the **Do not use proxy server** option to specify that no proxy server will be used to update ESET Security for Kerio.

The **Connection through a proxy server** option should be selected if a proxy server should be used to update ESET Security for Kerio and is different from the proxy server specified in the global settings (**Miscellaneous > Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port**, plus **Username** and **Password** for the proxy server, if required.

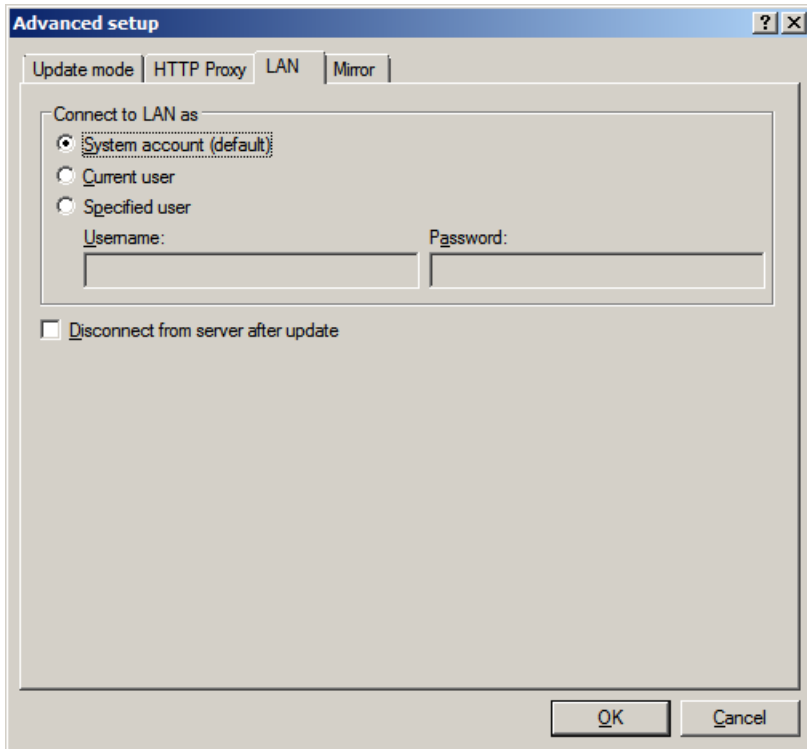
This option should also be selected if the proxy server settings were not set globally, but ESET Security for Kerio will connect to a proxy server for updates.

The default setting for the proxy server is **Use global proxy server settings**.

4.2.1.2.3 Connecting to the LAN

When updating from a local server with an NT-based operating system, authentication for each network connection is required by default. In most cases, a local system account does not have sufficient rights to access the Mirror folder (the Mirror folder contains copies of update files). If this is the case, enter the username and password in the update setup section, or specify an existing account under which the program will access the update server (Mirror).

To configure such an account, click the **LAN** tab. The **Connect to LAN as** section offers the **System account (default)**, **Current user**, and **Specified user** options.



Select the **System account (default)** option to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

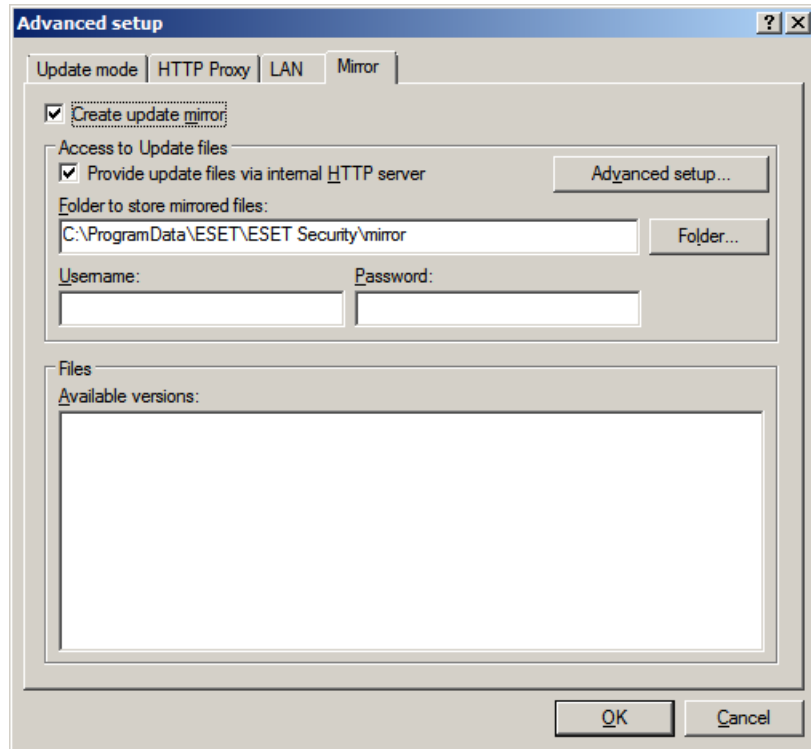
Select **Specified user** if you want the program to use a specific user account for authentication.

Warning: When either **Current user** or **Specified user** is selected, an error may occur when changing the identity of the program to the desired user. We recommend inserting the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: domain_name\user (if it is a workgroup, enter workgroup_name\name) and password. When updating from the HTTP version of the local server, no authentication is required.

4.2.1.2.4 Creating update copies - Mirror

ESET Security for Kerio allows you to create copies of update files which can be used to update other workstations located in the network. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local Mirror server are accessible (after adding a valid license key in the license manager, located in the ESET Security for Kerio Advanced Setup section) in the **Advanced update setup:** section. To access this section, press F5 and click **Update** in the Advanced Setup tree, then click the **Setup...** button next to **Advanced update setup:** and select the **Mirror** tab).



The first step in configuring the Mirror is to select the Create update mirror option. Selecting this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

The methods of Mirror activation are described in detail in section [Updating from the Mirror](#)^[44]. For now, note that there are two basic methods for accessing the Mirror – the folder with update files can be presented as a shared network folder or as an HTTP server.

The folder dedicated to storing update files for the Mirror is defined in the **Folder to store mirrored files** section. Click **Folder...** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be supplied in the **Username** and **Password** fields. The username and password should be entered in the format *Domain/ User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

When configuring the Mirror, you can also specify the language versions for which you want to download update copies. Language version setup is accessible in the section **Files - Available versions:**.

4.2.1.2.4.1 Updating from the Mirror

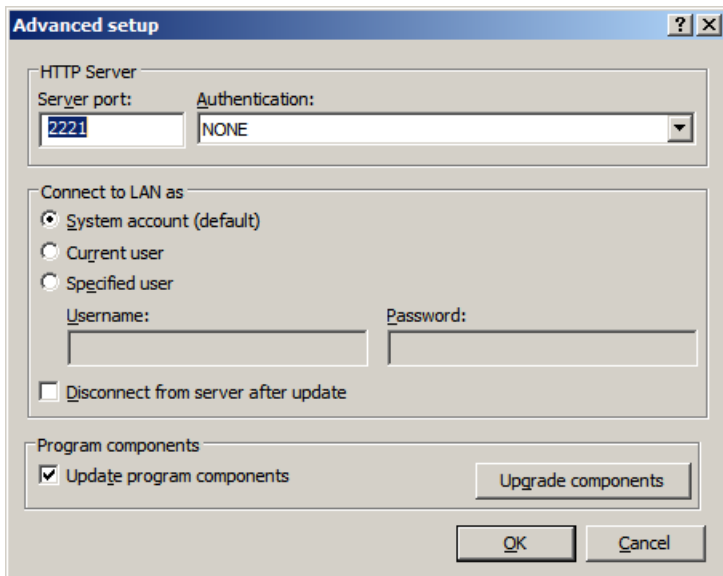
There are two basic methods of configuring the Mirror – the folder with update files can be presented as a shared network folder or as an HTTP server.

Accessing the Mirror using an internal HTTP server

This configuration is the default, specified in the predefined program configuration. In order to allow access to the Mirror using the HTTP server, navigate to **Advance update setup** (the **Mirror** tab) and select the **Create update mirror** option.

In the **Advanced setup** section of the **Mirror** tab you can specify the **Server Port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**. The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **NONE**, **Basic**, and **NTLM**. Select **Basic** to use the base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **NONE**, which grants access to the update files with no need for authentication.

Warning: If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Security for Kerio instance creating it.



After configuration of the Mirror is complete, go to the workstations and add a new update server in the format **http://IP_address_of_your_server:2221**. To do this, follow the steps below:

- Open ESET Security for Kerio **Advanced Setup** and click the **Update** branch.
- Click **Edit...** to the right of the **Update server** drop-down menu and add a new server using the following format: **http://IP_address_of_your_server:2221**.
- Select this newly-added server from the list of update servers.

Accessing the Mirror via system shares

First, a shared folder should be created on a local or a network device. When creating the folder for the Mirror, you must provide “write” access for the user who will save update files to the folder and “read” access for all users who will update ESET Security for Kerio from the Mirror folder.

Next, configure access to the Mirror in the **Advanced update setup** section (**Mirror** tab) by disabling the **Provide update files via internal HTTP server** option. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must specify authentication data to access the other computer. To specify authentication data, open ESET Security for Kerio Advanced Setup (F5) and click the **Update** branch. Click the **Setup...** button and then click the **LAN** tab. This setting is the same as for updating, as described in section [Connecting to LAN](#) ^[42].

After the Mirror configuration is complete, proceed to the workstations and set \\UNC\PATH as the update server. This operation can be completed using the following steps:

- Open ESET Security for Kerio Advanced Setup and click **Update**
- Click **Edit...** next to the Update server and add a new server using the \\UNC\PATH format.
- Select this newly-added server from the list of update servers

NOTE: For proper functioning, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

4.2.1.2.4.2 Troubleshooting Mirror update problems

In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data to the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or by a combination of the reasons above. Below is an overview of the most frequent problems which may occur during an update from the Mirror:

ESET Security for Kerio **reports an error connecting to Mirror server** – Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start** menu, click **Run**, insert the folder name and click **OK**. The contents of the folder should be displayed.

ESET Security for Kerio **requires a username and password** – Likely caused by incorrect authentication data (username and password) in the update section. The username and password are used to grant access to the update server, from which the program will update itself. Make sure that the authentication data is correct and entered in the correct format. For example, *Domain/Username*, or *Workgroup/ Username*, plus the corresponding Passwords. If the Mirror server is accessible to “Everyone”, please be aware that this does not mean that any user is granted access. “Everyone” does not mean any unauthorized user, it just means that the folder is accessible for all domain users. As a result, if the folder is accessible to “Everyone”, a domain username and password will still need to be entered in the update setup section.

ESET Security for Kerio **reports an error connecting to the Mirror server** – Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

4.2.2 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the primary window displayed after clicking Update from the main menu.

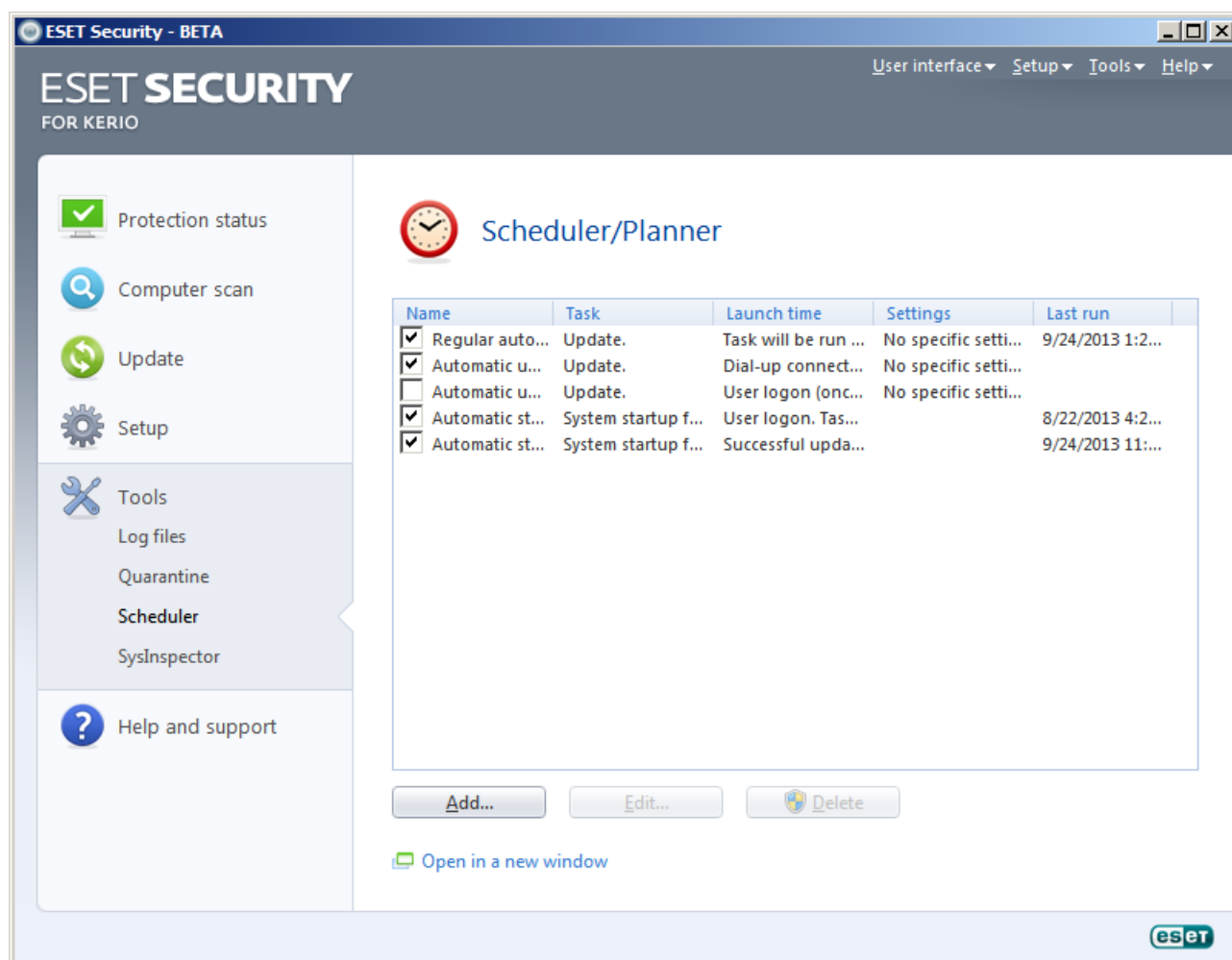
Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools > Scheduler**. By default, the following tasks are activated in ESET Security for Kerio:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each update task 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 section [Scheduler](#)^[46].

4.3 Scheduler

Scheduler is available if Advanced mode in ESET Security for Kerio is activated. **Scheduler** can be found in the ESET Security for Kerio main menu under **Tools**. Scheduler contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used.



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

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Automatic startup file check (after user logon)**
- **Automatic startup file check (after successful update of the virus signature database)**

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit...** or select the desired task you wish to modify and click the **Edit...** button.

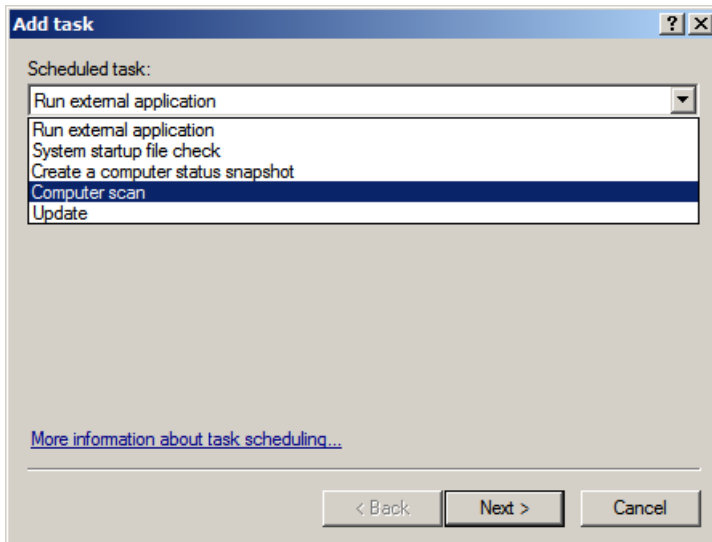
4.3.1 Purpose of scheduling tasks

Scheduler manages and launches scheduled tasks with predefined configuration 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.

4.3.2 Creating new tasks

To create a new task in Scheduler, click the **Add...** button or right-click and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run external application**
- **System startup file check**
- **Create a computer status snapshot**
- **On-demand computer scan**
- **Update**



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**. Click **Next** and enter the name of the task into the **Task name:** field. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered**. Based on the frequency selected, you will be prompted with different update parameters. Next, 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 task as soon as possible**
- **Run task immediately if the time since its last execution exceeds specified interval** (the interval can be defined using the Task interval scroll box)

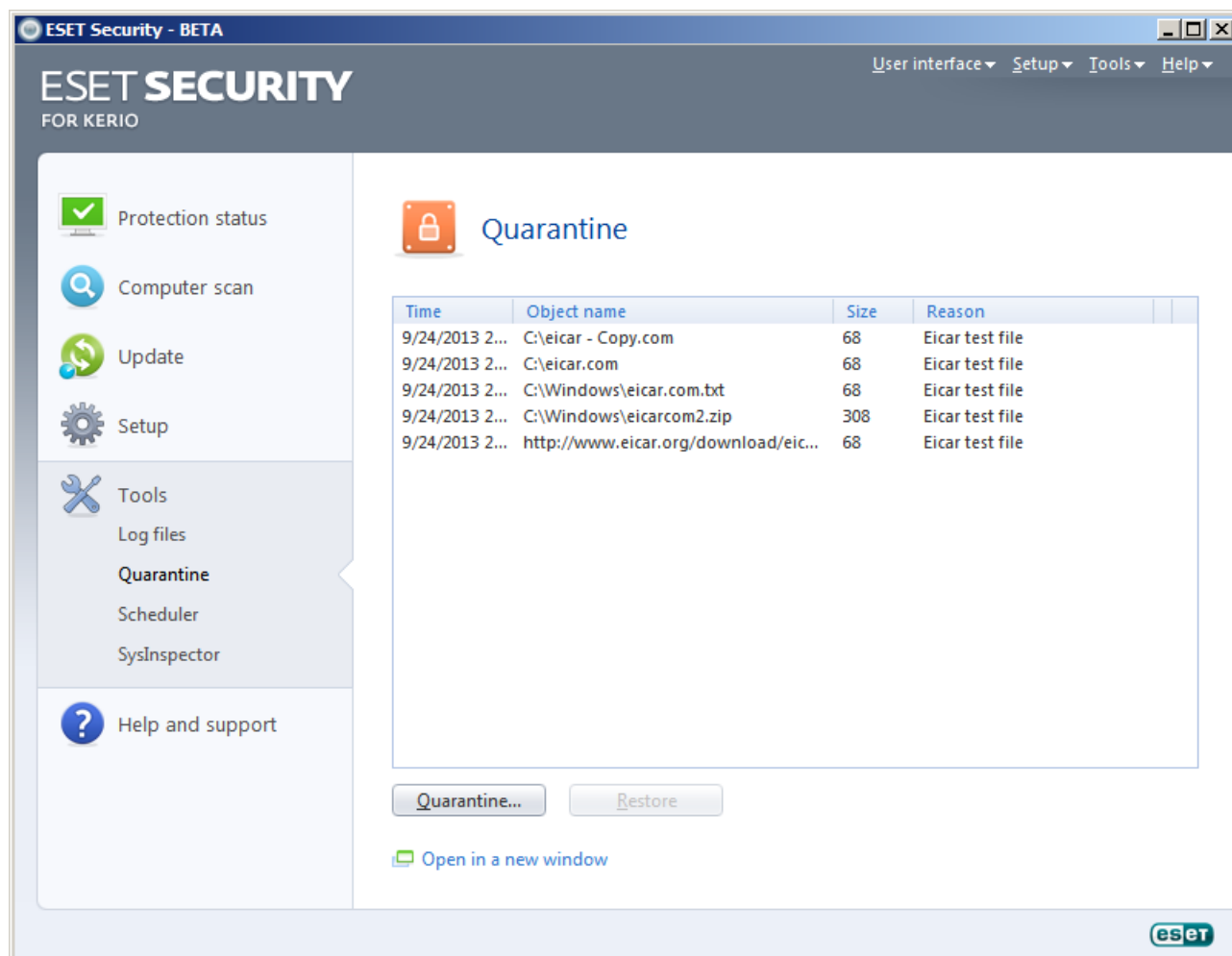
In the next step, a summary window with information about the current scheduled task is displayed; the option **Run task with specific parameters** should be automatically enabled. Click the **Finish** button.

A dialog window will appear, allowing you to select profiles to be used for the scheduled task. Here you can specify a primary and alternative profile, which is used in case the task cannot be completed using the primary profile. Confirm by clicking **OK** in the **Update profiles** window. The new scheduled task will be added to the list of currently scheduled tasks.

4.4 Quarantine

The main task of 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 Security for Kerio.

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 ESET's 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 (**added by user...**), and number of threats (e.g., if it is an archive containing multiple infiltrations).

4.4.1 Quarantining files

ESET Security for Kerio automatically quarantines deleted files (if you have not cancelled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking the **Quarantine...** button. If this is the case, the original file is not removed from its original location. The context menu can also be used for this purpose – right-click in the **Quarantine** window and select **Add...**

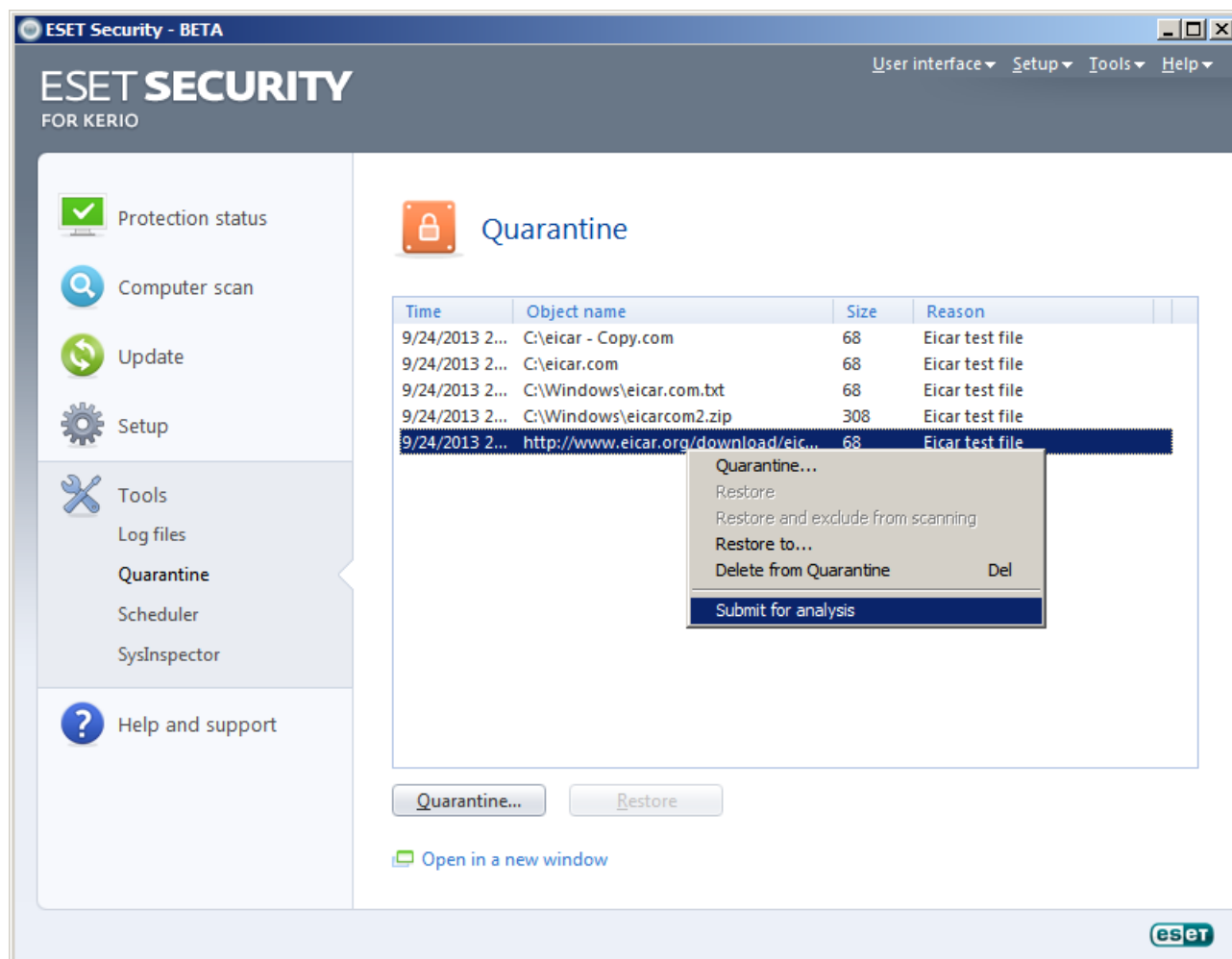
4.4.2 Restoring from Quarantine

Quarantined files can be restored to their original location. Use the **Restore** feature for this purpose. **Restore** is available from the context menu by right-clicking on the given file in the Quarantine window. The context menu also offers the **Restore to** option, which allows you to restore a file to a location other than the one from which it was deleted.

NOTE: If the program quarantined a harmless file by mistake, please exclude the file from scanning after restoring and send the file to ESET Customer Care.

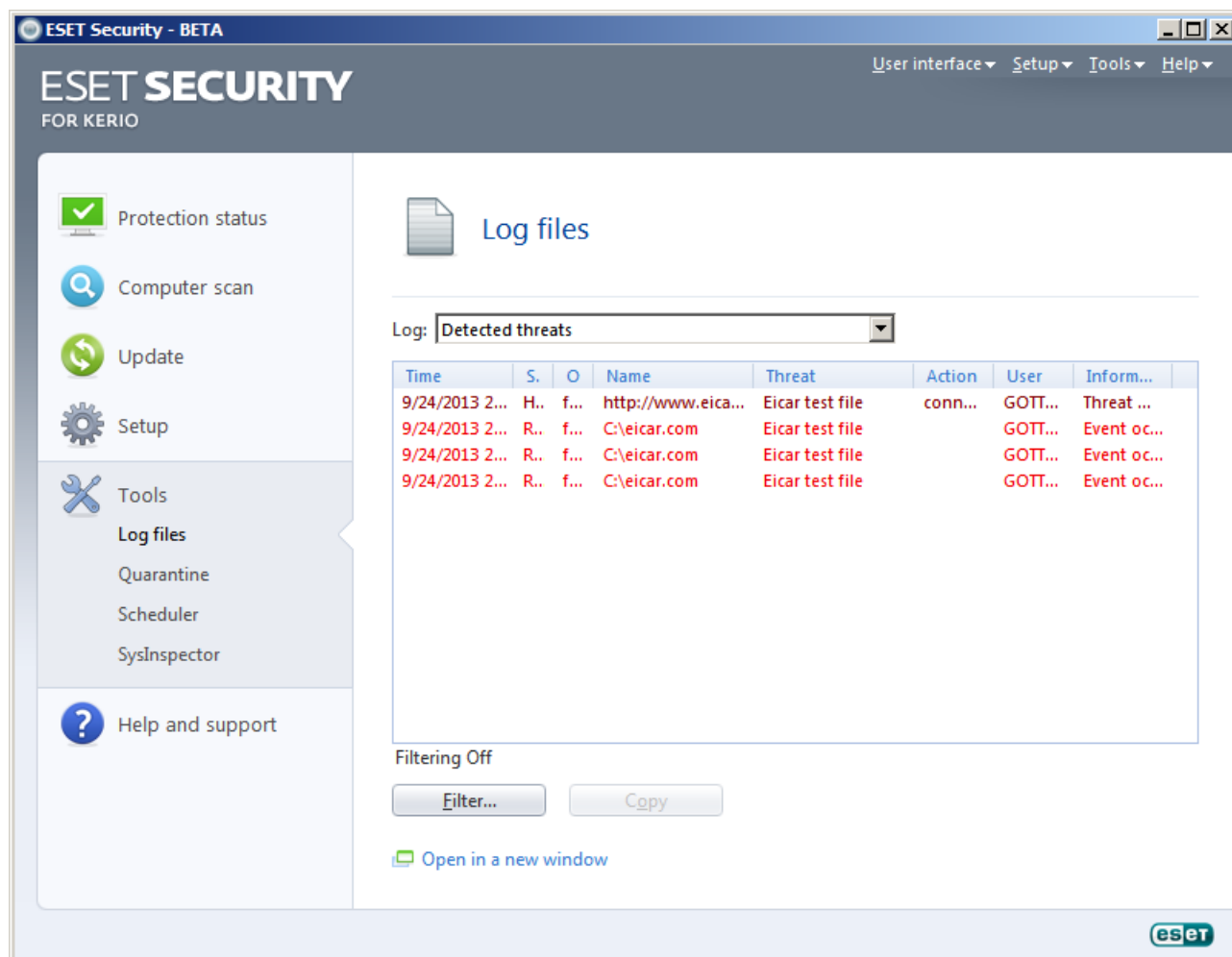
4.4.3 Submitting file from Quarantine

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 ESET's Threat Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.



4.5 Log files

The Log files contain information about all important program events that have occurred and provide 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 the current log verbosity settings. It is possible to view text messages and logs directly from the ESET Security for Kerio environment.



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

- **Detected threats** – Use this option to view all information about events related to detected infiltrations, except infiltrations detected by on-demand computer scan (these events are recorded in **On-demand computer scan** log).
- **Events** – This option is designed for system administrators and users to solve problems. All important actions performed by ESET Security for Kerio are recorded in the Event logs.
- **On-demand computer scan** – Results of all completed scans are displayed in this window. Double-click any entry to view details of the respective On-demand scan.

In each section, the displayed information can be directly copied to the clipboard by selecting the entry and clicking the **Copy** button. To select multiple entries, the CTRL and SHIFT keys can be used.

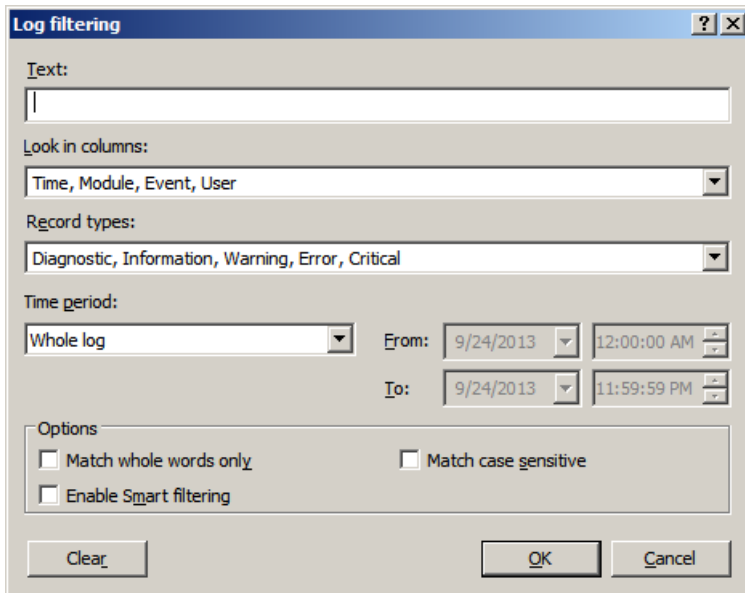
4.5.1 Log filtering

Log filtering is a useful feature that helps you find records in the log files, especially when there are too many records and it is difficult to find the particular information you need.

When using filtering, you can type in a string of **What** to filter, specify what **columns to look in**, select **Record types** and set a **Time period** to narrow down the number of records. By specifying certain filter options, only records that are relevant (according to those filter options) are shown in the **Log files** window for easy and quick access.

To open the **Log filtering** window, press **Filter...** button once in **Tools > Log files**, or use shortcut keys Ctrl + Shift + F.

NOTE: To search for a particular record, you can use the [Find in log](#) ⁵² functionality instead, or in conjunction with Log filtering.



By specifying certain filter options, only records that are relevant (according to those filter options) are shown in the Log files window. This will filter out / narrow down the records, thus making it easier for you to find what you are looking for. The more specific filter options you use, the narrower the result will be.

What: - Type in a string (word, or part of a word.) Only records that contain this string will be shown. The rest of the records will not be visible for better readability.

Look in columns: - Select what columns will be taken into account when filtering. You can check one or more columns to be used for filtering. By default, all columns are checked:

- **Time**
- **Module**
- **Event**
- **User**

Record types: - Lets you choose what type of records to show. You can choose one particular record type, multiple types at the same time, or have all of the record types shown (by default):

- **Diagnostic**
- **Information**
- **Warning**
- **Error**
- **Critical**

Time period: - Use this option to have records filtered by time period. You can choose one of the following:

- **Whole log** (default) - does not filter by time period as it shows whole log
- **Last day**
- **Last week**
- **Last month**
- **Interval** - by selecting interval, you can specify exact time period (date and time) to have shown only those records that happened within specified time period.

Apart from the filtering settings above, you also have several **Options**:

Match whole words only - Shows only records that match the string as a whole word in the **What** text box.

Match case sensitive - Shows only records that match the string with exact capitalization in the **What** text box.

Enable Smart filtering - Use this option to let ESET Security for Kerio perform filtering using its own methods.

Once you are finished with configuring filtering options, press the **OK** button to apply the filter. The **Log files** window will show only corresponding records according to the filter options.

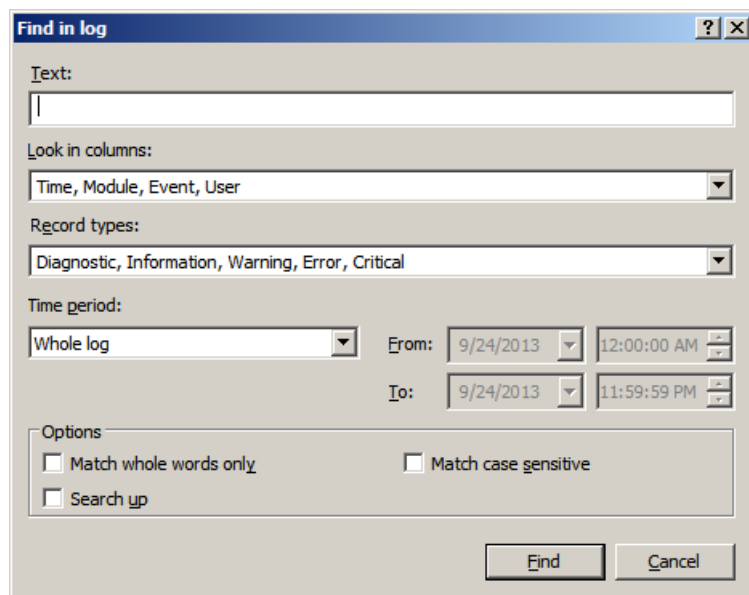
4.5.2 Find in log

In addition to [Log filtering](#)^[51], you can use search functionality within Log files, however you can also use it independently from log filtering. This is useful when you are looking for particular records in the logs. Like Log filtering, this search feature will help you find the information you are looking for, especially when there are too many records.

When using Find in log, you can type in a string of **What** to find, specify what **columns to look in**, select **Record types** and set a **Time period** to search only for records that happened within that time period. By specifying certain search options, only records that are relevant (according to those search options) will be searched in the Log files window.

In order to search in logs, open the **Find in Log** window by pressing Ctrl + f keys.

NOTE: You can use the Find in log feature in conjunction with [Log filtering](#)^[51]. You can first narrow down the number of records using Log filtering and then start searching only within filtered records.



What: - Type in a string (word, or part of a word). Only records that contain this string will be found. The rest of the records will be omitted.

Look in columns: - Select what columns will be taken into account when searching. You can check one or more columns to be used for searching. By default, all columns are checked:

- **Time**
- **Module**
- **Event**
- **User**

Record types: - Lets you choose what type of records to find. You can choose one particular record type, multiple types at the same time, or have all of the record types to be searched (by default):

- **Diagnostic**
- **Information**
- **Warning**
- **Error**
- **Critical**

Time period: - Use this option to find records only within particular time period. You can choose one of the following:

- **Whole log** (default) - does not search within time period, searches the whole log
- **Last day**
- **Last week**
- **Last month**
- **Interval** - by selecting interval, you can specify exact time period (date and time) to search only those record that happened within specified time period.

Apart from the find settings above, you also have several **Options**:

Match whole words only - Finds only records that match the string as a whole word in the **What** text box.

Match case sensitive - Finds only records that match the string with exact capitalization in the **What** text box.

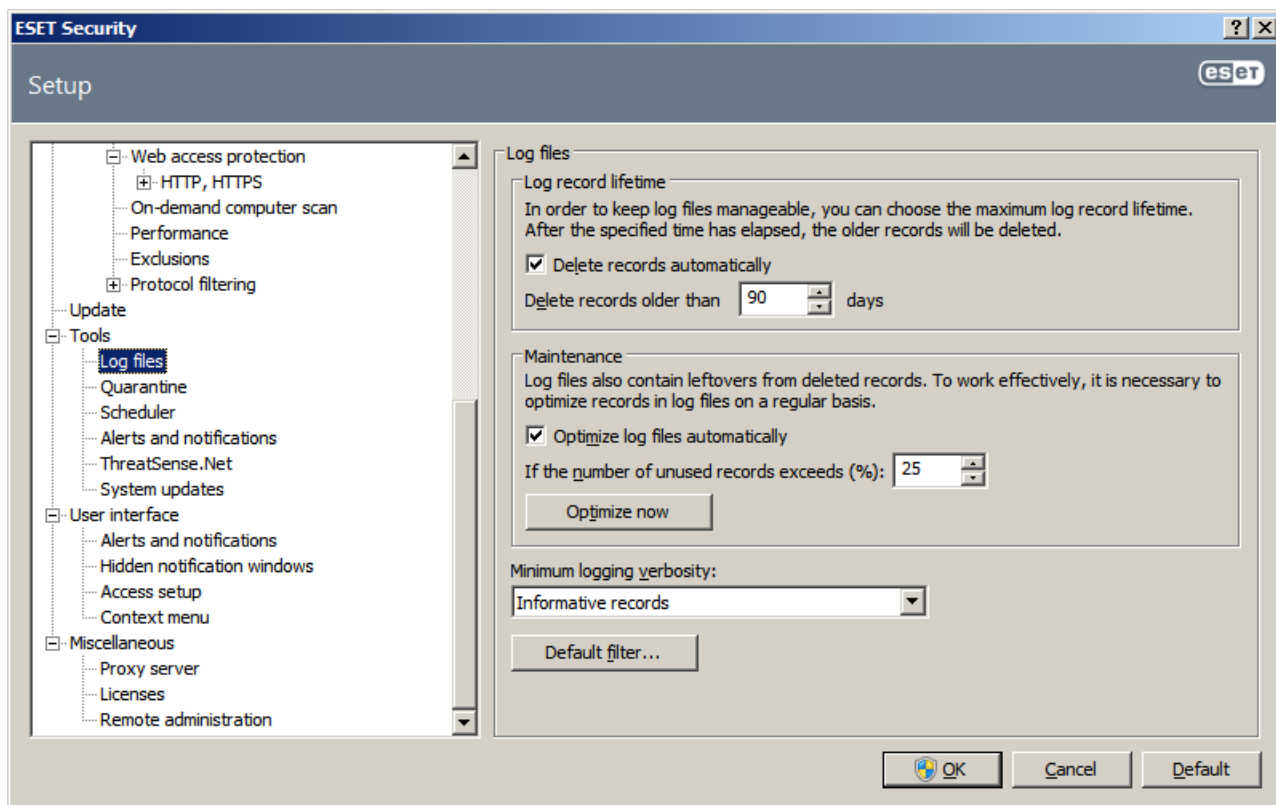
Search up - Searches from current position upwards.

Once you configured your search options, click the **Find** button to start searching. The search stops when it finds the first corresponding record. Click the **Find** button again to search further. The Log files are searched from top to bottom, starting from current position (record that is highlighted).

4.5.3 Log maintenance

The Logging configuration of ESET Security for Kerio is accessible from the main program window. Click **Setup > Enter entire advanced setup tree... > Tools > Log files**. You can specify the following options for log files:

- **Delete 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
- **Minimum logging verbosity:** Specifies the logging verbosity level. Available options:
 - **Diagnostic records** – Logs information needed for fine-tuning of the program and all records above
 - **Informative records** – Records informative messages including successful update messages plus all records above
 - **Warnings** – Records critical errors and warning messages
 - **Errors** – Only "Error downloading file" messages are recorded, plus critical errors
 - **Critical warnings** – Logs only critical errors (error starting Antivirus protection, etc...)



4.6 ESET SysInspector

4.6.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET's website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an .xml file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools > ESET SysInspector** (except ESET Remote Administrator).

Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

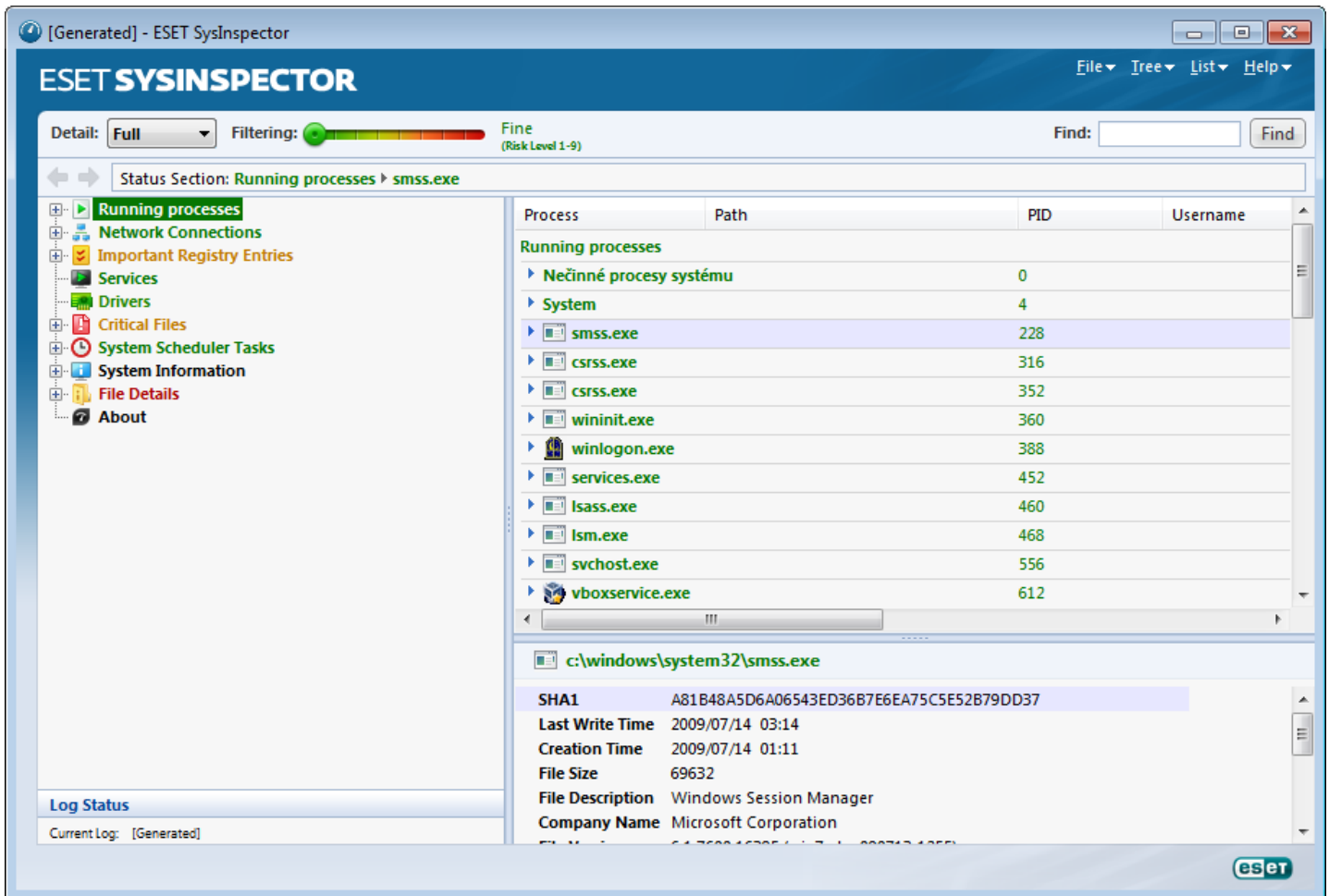
4.6.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website.

Please wait while the application inspects your system, which could take up to several minutes depending on your hardware and data to be gathered.

4.6.2 User Interface and application usage

For clarity the Main window is divided into four major sections – Program Controls located on the top of the Main window, the Navigation window on the left, the Description window on the right in the middle and the Details window on the right at the bottom of the Main window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



4.6.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

File

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

NOTE: You may open previously stored ESET SysInspector reports by simply dragging and dropping them into the Main window.

Tree

Enables you to expand or close all nodes and export selected sections to Service script.

List

Contains functions for easier navigation within the program and various other functions like finding information online.

Help

Contains information about the application and its functions.

Detail

This setting influences the information displayed in the Main window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

Item filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current Risk Level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose security risk. If you are not using a security solution from ESET, we recommend that you scan your system with [ESET Online Scanner](#) if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

NOTE: The Risk level of an item can be quickly determined by comparing the color of the item with the color on the Risk Level slider.

Search

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

Return



By clicking the back or forward arrow, you may return to previously displayed information in the Description window. You may use the backspace and space keys instead of clicking back and forward.

Status section

Displays the current node in Navigation window.

Important: Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

4.6.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or alternatively click  or  next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

Running processes

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

NOTE: An operating system comprises of several important kernel components running 24/7 that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with `\\?\`. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

Network connections

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

Important Registry Entries

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

Services

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

Drivers

A list of drivers installed in the system.

Critical files

The Description window displays content of critical files related to the Microsoft windows operating system.

System Scheduler Tasks

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

System information

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

File details

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

About

Information about version of ESET SysInspector and the list of program modules.

4.6.2.2.1 Keyboard shortcuts

Key shortcuts that can be used when working with the ESET SysInspector include:

File

Ctrl+O opens existing log
Ctrl+S saves created logs

Generate

Ctrl+G generates a standard computer status snapshot
Ctrl+H generates a computer status snapshot that may also log sensitive information

Item Filtering

1, O fine, risk level 1-9 items are displayed
2 fine, risk level 2-9 items are displayed
3 fine, risk level 3-9 items are displayed
4, U unknown, risk level 4-9 items are displayed
5 unknown, risk level 5-9 items are displayed

6	unknown, risk level 6-9 items are displayed
7, B	risky, risk level 7-9 items are displayed
8	risky, risk level 8-9 items are displayed
9	risky, risk level 9 items are displayed
-	decreases risk level
+	increases risk level
Ctrl+9	filtering mode, equal level or higher
Ctrl+0	filtering mode, equal level only

View

Ctrl+5	view by vendor, all vendors
Ctrl+6	view by vendor, only Microsoft
Ctrl+7	view by vendor, all other vendors
Ctrl+3	displays full detail
Ctrl+2	displays medium detail
Ctrl+1	basic display
BackSpace	moves one step back
Space	moves one step forward
Ctrl+W	expands tree
Ctrl+Q	collapses tree

Other controls

Ctrl+T	goes to the original location of item after selecting in search results
Ctrl+P	displays basic information about an item
Ctrl+A	displays full information about an item
Ctrl+C	copies the current item's tree
Ctrl+X	copies items
Ctrl+B	finds information about selected files on the Internet
Ctrl+L	opens the folder where the selected file is located
Ctrl+R	opens the corresponding entry in the registry editor
Ctrl+Z	copies a path to a file (if the item is related to a file)
Ctrl+F	switches to the search field
Ctrl+D	closes search results
Ctrl+E	run service script

Comparing

Ctrl+Alt+O	opens original / comparative log
Ctrl+Alt+R	cancels comparison
Ctrl+Alt+1	displays all items
Ctrl+Alt+2	displays only added items, log will show items present in current log
Ctrl+Alt+3	displays only removed items, log will show items present in previous log
Ctrl+Alt+4	displays only replaced items (files inclusive)
Ctrl+Alt+5	displays only differences between logs
Ctrl+Alt+C	displays comparison
Ctrl+Alt+N	displays current log
Ctrl+Alt+P	opens previous log

Miscellaneous

F1	view help
Alt+F4	close program
Alt+Shift+F4	close program without asking
Ctrl+I	log statistics

4.6.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting activity of malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Navigate to **File > Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, use **File > Open log**. In the main program window, ESET SysInspector always displays one log at a time.







The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, use the option **File > Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

NOTE: If you compare two log files, select **File > Save log** to save it as a ZIP file; both files are saved. If you open this file later, the contained logs are automatically compared.

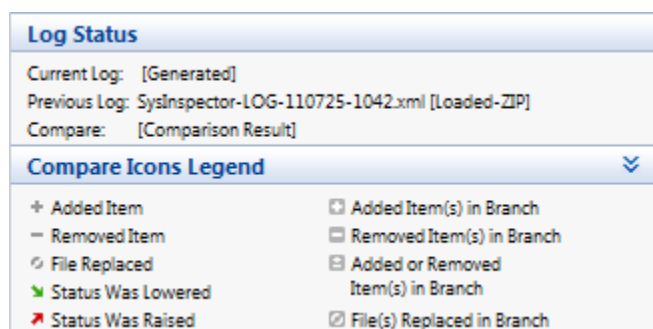
Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Items marked by a **-** can only be found in the active log and were not present in the opened comparative log. Items marked by a **+** were present only in the opened log and are missing in the active one.

Description of all symbols that can be displayed next to items:

- **+** new value, not present in the previous log
-  tree structure section contains new values
- **-** removed value, present in the previous log only
-  tree structure section contains removed values
-  value / file has been changed
-  tree structure section contains modified values / files
-  the risk level has decreased / it was higher in the previous log
-  the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



Any comparative log can be saved to a file and opened at a later time.

Example

Generate and save a log, recording original information about the system, to a file named *previous.xml*. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, navigate to **File > Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

```
SysInspector.exe current.xml previous.xml
```

4.6.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

/gen	generate a log directly from the command line without running the GUI
/privacy	generate a log excluding sensitive information
/zip	store the resulting log directly on the disk in a compressed file
/silent	suppress the display of the log generation progress bar
/help, /?	display information about the command line parameters

Examples

To load a specific log directly in the browser, use: `SysInspector.exe "c:\clientlog.xml"`

To generate a log to a current location, use: `SysInspector.exe /gen`

To generate a log to a specific folder, use: `SysInspector.exe /gen="c:\folder\"`

To generate a log to a specific file/location, use: `SysInspector.exe /gen="c:\folder\mynewlog.xml"`

To generate a log excluding sensitive information directly in a compressed file, use: `SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip`

To compare two logs, use: `SysInspector.exe "current.xml" "original.xml"`

NOTE: If the name of the file/folder contains a gap, then should be taken into inverted commas.

4.6.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

Example

If you have a suspicion that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

- Run ESET SysInspector to generate a new system snapshot.
- Select the first item in the section on the left (in the tree structure), press Ctrl and select the last item to mark all items.
- Right click the selected objects and select the **Export Selected Sections To Service Script** context menu option.
- The selected objects will be exported to a new log.
- This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
- Open ESET SysInspector, click **File > Run Service Script** and enter the path to your script.
- Click **OK** to run the script.

4.6.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either the **Export All Sections To Service Script** option or the **Export Selected Sections To Service Script** option.

NOTE: It is not possible to export the service script when two logs are being compared.

4.6.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

01) Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

02) Loaded modules

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khibehb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khibehb.dll was marked by a "+". When the script runs, it will recognize the processes using that specific module and end them.

03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
  HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to O-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]
```

The services marked and their dependant services will be stopped and uninstalled when the script is executed.

08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

09) Critical files

This section contains information about files that are critical to the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

4.6.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

4.6.5 FAQ

Does ESET SysInspector require Administrator privileges to run ?

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

Does ESET SysInspector create a log file ?

ESET SysInspector can create a log file of your computer's configuration. To save one, select **File > Save Log** from the main menu. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

How do I view the ESET SysInspector log file ?

To view a log file created by ESET SysInspector, run the program and select **File > Open Log** from the main menu. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

Is a specification available for the log file format? What about an SDK ?

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

How does ESET SysInspector evaluate the risk posed by a particular object ?

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from **1 - Fine (green)** to **9 - Risky (red)**. In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

Does a risk level of "6 - Unknown (red)" mean an object is dangerous ?

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

Why does ESET SysInspector connect to the Internet when run ?

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

What is Anti-Stealth technology ?

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time ?

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - %systemroot%\system32\catroot) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

Example:

Windows 2000 includes the HyperTerminal application located in C:\Program Files\Windows NT. The main application executable file is not digitally signed, but ESET SysInspector marks it as a file signed by Microsoft. The reason for this is a reference in C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat pointing to C:\Program Files\Windows NT\hypertrm.exe (the main executable of the HyperTerminal application) and sp4.cat is digitally signed by Microsoft.

4.7 ESET SysRescue

ESET SysRescue is a utility which enables you to create a bootable disk containing one of the ESET Security solutions - it can be ESET NOD32 Antivirus, ESET Smart Security or even some of the server-oriented products. The main advantage of ESET SysRescue is the fact that ESET Security solution runs independent of the host operating system, while it has a direct access to the disk and the entire file system. This makes it possible to remove infiltrations which normally could not be deleted, e.g., when the operating system is running, etc.

4.7.1 Minimum requirements

ESET SysRescue works in the Microsoft Windows Preinstallation Environment (Windows PE) version 2.x, which is based on Windows Vista.

Windows PE is a part of the free packages, Windows Automated Installation Kit (Windows AIK) or Windows Assessment and Deployment Kit (Windows ADK) and therefore Windows AIK or ADK must be installed before creating ESET SysRescue (<http://go.eset.eu/AIK>) or (<http://go.eset.eu/ADK>). Which one of these kits should be installed on your system depends on the operating system version you are running. Due to the support of the 32-bit version of Windows PE, it is necessary to use a 32-bit installation package of ESET Security solution when creating ESET SysRescue on 64-bit systems. ESET SysRescue supports Windows AIK 1.1 and higher as well as Windows ADK.

NOTE: Since Windows AIK is over 1 GB in size and Windows ADK is 1.3 GB in size, a high-speed internet connection is required for smooth download.

ESET SysRescue is available in ESET Security solutions version 4.0 and higher.

ESET SysRescue supports following operating systems:

- Windows Server 2003 Service Pack 1 with KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

Windows AIK supports:

- Windows Server 2003
- Windows Server 2008

Windows ADK supports:

- Windows Server 2012

4.7.2 How to create rescue CD

To launch the ESET SysRescue wizard, click **Start > Programs > ESET > ESET Security for Kerio > ESET SysRescue**.

First, the wizard checks for the presence of Windows AIK or Windows ADK and a suitable device for the boot media creation. If Windows AIK or Windows ADK is not installed on the computer (or it is either corrupt or installed incorrectly), the wizard will offer you the option to install it, or to enter the path to your Windows AIK folder (<http://go.eset.eu/AIK>) or Windows ADK (<http://go.eset.eu/ADK>).

NOTE: Since Windows AIK is over 1 GB in size and Windows ADK is 1.3 GB in size, a high-speed internet connection is required for smooth download.

In the [next step](#)⁶⁵, select the target media where ESET SysRescue will be located.

4.7.3 Target selection

In addition to CD/DVD/USB, you can choose to save ESET SysRescue in an ISO file. Later on, you can burn the ISO image on CD/DVD, or use it some other way (e.g. in the virtual environment such as VMware or VirtualBox).

If you select USB as the target medium, booting may not work on certain computers. Some BIOS versions may report problems with the BIOS - boot manager communication (e.g. on Windows Vista) and booting exits with the following error message:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attempting to read the boot configuration data
```

If you encounter this message, we recommend selecting CD instead of USB medium.

4.7.4 Settings

Before initiating ESET SysRescue creation, the install wizard displays compilation parameters in the last step of the ESET SysRescue wizard. These can be modified by clicking the **Change...** button. The available options include:

- [Folders](#)^[66]
- [ESET Antivirus](#)^[66]
- [Advanced](#)^[66]
- [Internet protocol](#)^[67]
- [Bootable USB device](#)^[67] (when the target USB device is selected)
- [Burning](#)^[67] (when the target CD/DVD drive is selected)

The **Create** button is inactive if no MSI installation package is specified, or if no ESET Security solution is installed on the computer. To select an installation package, click the **Change** button and go to the **ESET Antivirus** tab. Also, if you do not fill in username and password (**Change > ESET Antivirus**), the **Create** button is greyed out.

4.7.4.1 Folders

Temporary folder is a working directory for files required during ESET SysRescue compilation.

ISO folder is a folder, where the resulting ISO file is saved after the compilation is completed.

The list on this tab shows all local and mapped network drives together with the available free space. If some of the folders here are located on a drive with insufficient free space, we recommend that you select another drive with more free space available. Otherwise compilation may end prematurely due to insufficient free disk space.

External applications – Allows you to specify additional programs that will be run or installed after booting from a ESET SysRescue medium.

Include external applications – Allows you to add external programs to the ESET SysRescue compilation.

Selected folder – Folder in which programs to be added to the ESET SysRescue disk are located.

4.7.4.2 ESET Antivirus

For creating the ESET SysRescue CD, you can select two sources of ESET files to be used by the compiler.

ESS/EAV folder – Files already contained in the folder to which the ESET Security solution is installed on the computer.

MSI file – Files contained in the MSI installer are used.

Next, you can choose to update the location of (.nup) files. Normally, the default option **ESS/EAV folder/MSI file** should be set. In some cases, a custom **Update folder** can be chosen, e.g., to use an older or newer virus signature database version.

You can use one of the following two sources of username and password:

Installed ESS/EAV – Username and password will be copied from the currently installed ESET Security solution.

From user – Username and password entered in the corresponding text boxes will be used.

NOTE: ESET Security solution on the ESET SysRescue CD is updated either from the Internet or from the ESET Security solution installed on the computer on which the ESET SysRescue CD is run.

4.7.4.3 Advanced settings

The **Advanced** tab lets you optimize the ESET SysRescue CD according to the amount of memory on your computer. Select **576 MB and more** to write the content of the CD to the operating memory (RAM). If you select **less than 576 MB**, the recovery CD will be permanently accessed when WinPE will be running.

In the **External drivers** section, you can insert drivers for your specific hardware (usually network adapter). Although WinPE is based on Windows Vista SP1, which supports a large range of hardware, occasionally hardware is not recognized. This will required that you add a driver manually. There are two ways of introducing a driver into an ESET SysRescue compilation - manually (the **Add** button) and automatically (the **Aut. Search** button). In the case of manual inclusion, you need to select the path to the corresponding .inf file (applicable *.sys file must also be present in this folder). In the case of automatic introduction, the driver is found automatically in the operating

system of the given computer. We recommend using automatic inclusion only if ESET SysRescue is used on a computer that has the same network adapter as the computer on which the ESET SysRescue CD was created. During creation, the ESET SysRescue driver is introduced into the compilation so you do not need to look for it later.

4.7.4.4 Internet protocol

This section allows you to configure basic network information and set up predefined connections after ESET SysRescue.

Select **Automatic private IP address** to obtain the IP address automatically from DHCP (Dynamic Host Configuration Protocol) server.

Alternatively, this network connection can use a manually specified IP address (also known as a static IP address). Select **Custom** to configure the appropriate IP settings. If you select this option, you must specify an **IP address** and, for LAN and high-speed Internet connections, a **Subnet mask**. In **Preferred DNS server** and **Alternate DNS server**, type the primary and secondary DNS server addresses.

4.7.4.5 Bootable USB device

If you have selected a USB device as your target medium, you can select one of the available USB devices on the **Bootable USB device** tab (in case there are more USB devices).

Select the appropriate target **Device** where ESET SysRescue will be installed.

Warning: The selected USB device will be formatted during the creation of ESET SysRescue. All data on the device will be deleted.

If you choose the **Quick format** option, formatting removes all the files from the partition, but does not scan the disk for bad sectors. Use this option if your USB device has been formatted previously and you are sure that it is not damaged.

4.7.4.6 Burn

If you have selected CD/DVD as your target medium, you can specify additional burning parameters on the **Burn** tab.

Delete ISO file – Check this option to delete the temporary ISO file after the ESET SysRescue CD is created.

Deletion enabled – Enables you to select fast erasing and complete erasing.

Burning device – Select the drive to be used for burning.

Warning: This is the default option. If a rewritable CD/DVD is used, all the data on the CD/DVD will be erased.

The Medium section contains information about the medium in your CD/DVD device.

Burning speed – Select the desired speed from the drop-down menu. The capabilities of your burning device and the type of CD/DVD used should be considered when selecting the burning speed.

4.7.5 Working with ESET SysRescue

For the rescue CD/DVD/USB to work effectively, you must start your computer from the ESET SysRescue boot media. Boot priority can be modified in the BIOS. Alternatively, you can use the boot menu during computer startup – usually using one of the F9 - F12 keys depending on the version of your motherboard/BIOS.

After booting up from the boot media, ESET Security solution will start. Since ESET SysRescue is used only in specific situations, some protection modules and program features present in the standard version of ESET Security solution are not needed; their list is narrowed down to **Computer scan**, **Update**, and some sections in **Setup**. The ability to update the virus signature database is the most important feature of ESET SysRescue, we recommend that you update the program prior starting a Computer scan.

4.7.5.1 Using ESET SysRescue

Suppose that computers in the network have been infected by a virus which modifies executable (.exe) files. ESET Security solution is capable of cleaning all infected files except for *explorer.exe*, which cannot be cleaned, even in Safe mode. This is because *explorer.exe*, as one of the essential Windows processes, is launched in Safe mode as well. ESET Security solution would not be able to perform any action with the file and it would remain infected.

In this type of scenario, you could use ESET SysRescue to solve the problem. ESET SysRescue does not require any component of the host operating system, and is therefore capable of processing (cleaning, deleting) any file on the disk.

4.8 User interface options

The user interface configuration options in ESET Security for Kerio allow you to adjust the working environment to fit your needs. These configuration options are accessible from the **User interface** branch of the ESET Security for Kerio Advanced Setup tree.

In the **User interface elements** section, the **Advanced mode** option gives users the ability to toggle to Advanced mode. Advanced mode displays more detailed settings and additional controls for ESET Security for Kerio.

The **Graphical user interface** option should be disabled if the graphical elements slow the performance of your computer or cause other problems. The graphical interface may also need to be turned off for visually impaired users, as it may conflict with special applications that are used for reading text displayed on the screen.

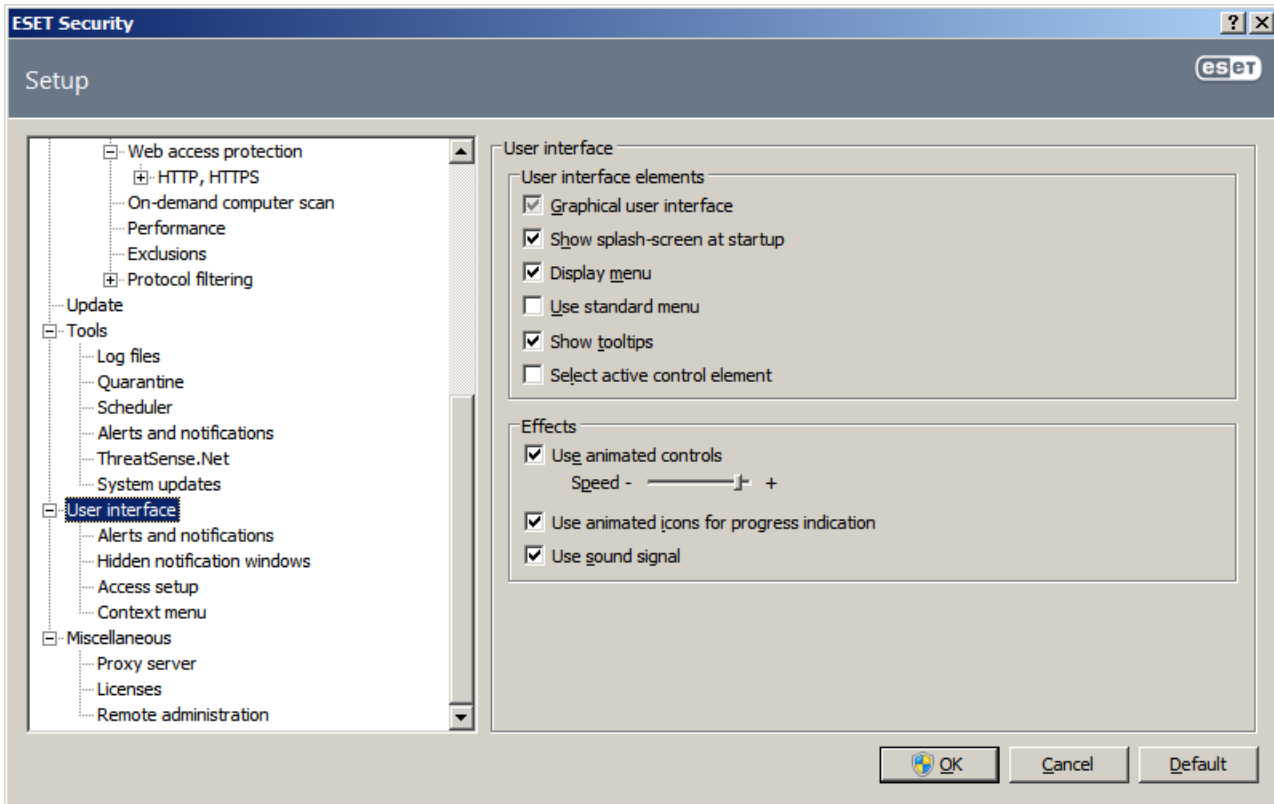
If you wish to disable the ESET Security for Kerio splash-screen, uncheck the **Show splash-screen at startup** option.

At the top of the ESET Security for Kerio main program window is a Standard menu which can be activated or disabled based on the **Use standard menu** option.

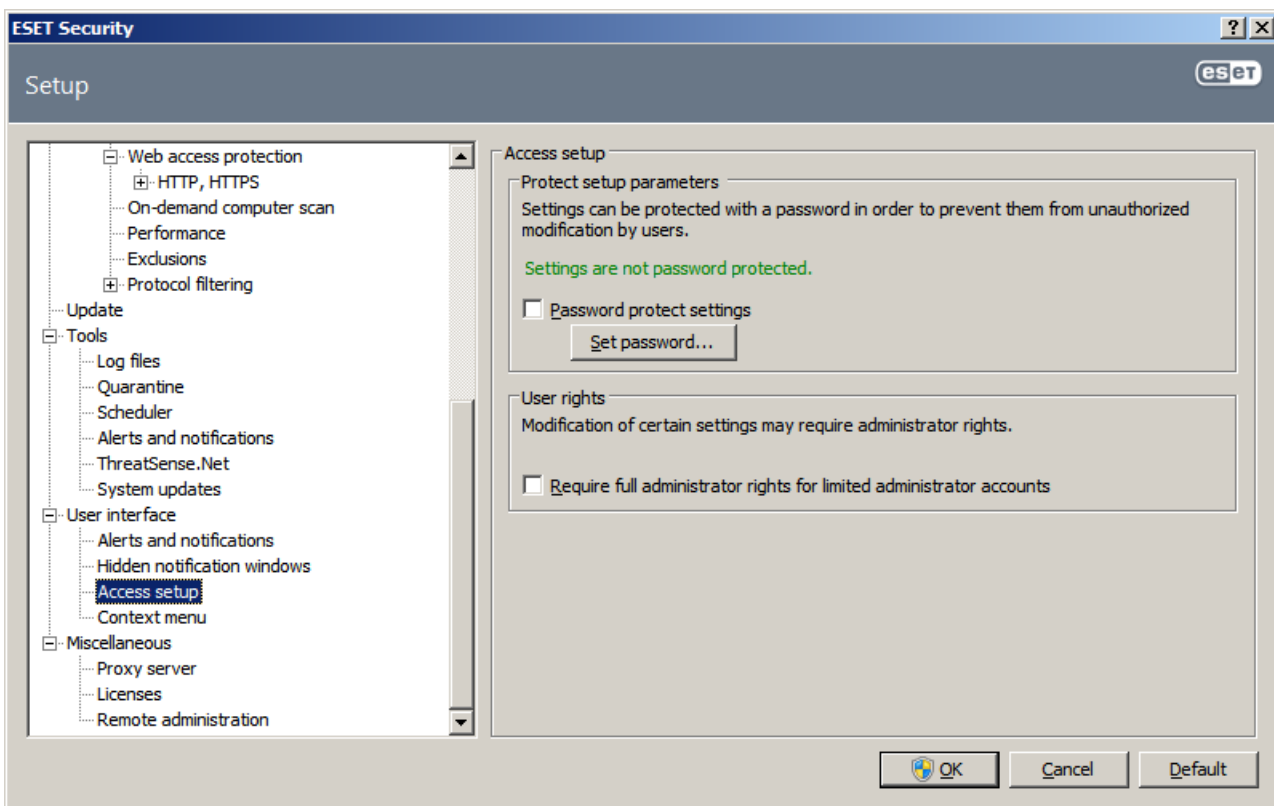
If the **Show tooltips** option is enabled, a short description will be displayed if the cursor is placed over an option. The **Select active control element** option will cause the system to highlight any element which is currently under the active area of the mouse cursor. The highlighted element will be activated after a mouse click.

To decrease or increase the speed of animated effects, select the **Use animated controls** option and move the **Speed** slider bar to the left or right.

To enable the use of animated icons to display the progress of various operations, select the **Use animated icons for progress indication** option. If you want the program to sound a warning if an important event takes place, select the **Use sound signal** option.



The **User interface** features also include the option to password-protect the ESET Security for Kerio setup parameters. This option is located in the **Settings protection** submenu under **User interface**. In order to provide maximum security for your system, it is essential that the program be correctly configured. Unauthorized modifications could result in the loss of important data. To set a password to protect the setup parameter, click **Set password...**



4.8.1 Alerts and notifications

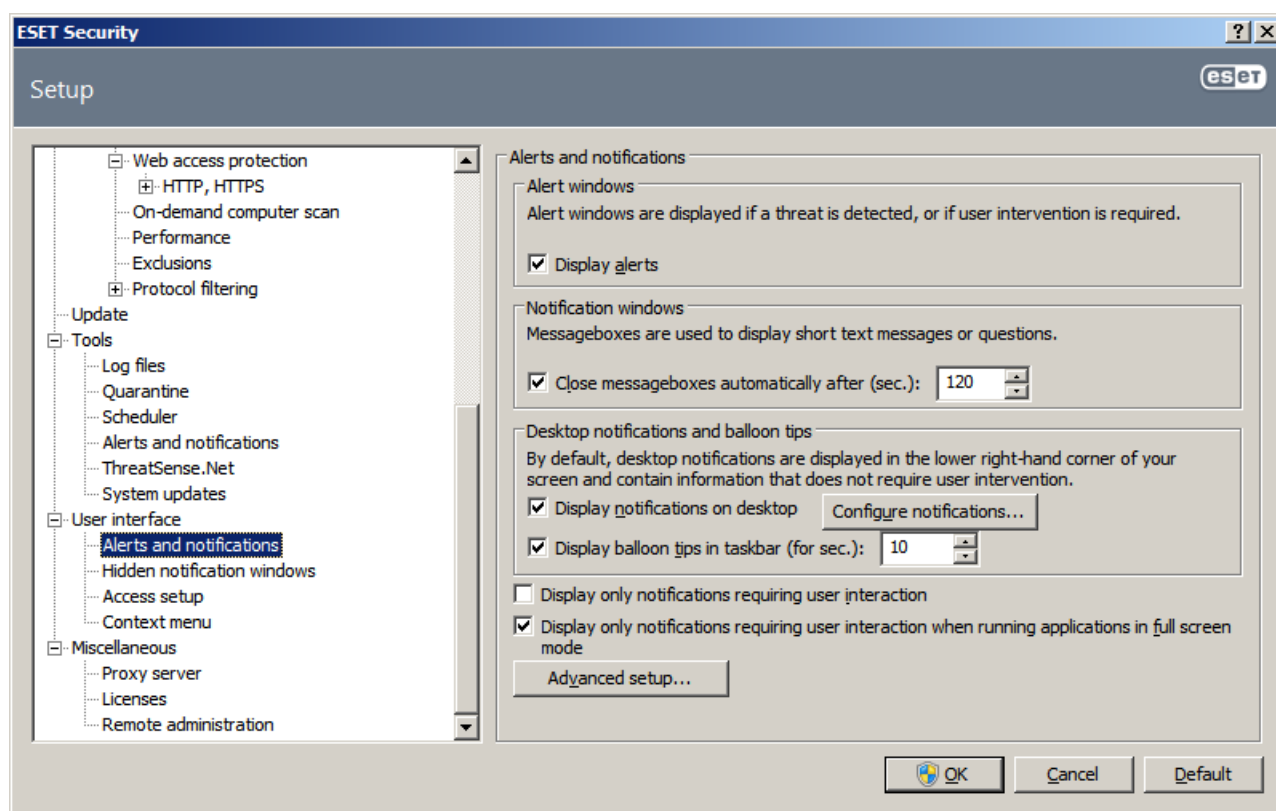
The **Alerts and notifications setup** section under **User interface** allows you to configure how threat alerts and system notifications are handled in ESET Security for Kerio.

The first item is **Display alerts**. Disabling this option will cancel all alert windows and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left to its default setting (enabled).

To close pop-up windows automatically after a certain period of time, select the option **Close messageboxes automatically after (sec.)**. If they are not closed manually, alert windows are automatically closed after the specified time period has expired.

Notifications on the Desktop and balloon tips are informative only, and do not require or offer user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate displaying Desktop notifications, select the **Display notifications on desktop** option. More detailed options – notification display time and window transparency can be modified by clicking the **Configure notifications...** button.

To preview the behavior of notifications, click the **Preview** button. To configure the duration of the balloon tips display time, see the option **Display balloon tips in taskbar (for sec.)**.



Click **Advanced setup...** to enter additional **Alerts and notification** setup options that include the **Display only notifications requiring user's interaction**. This option allows you to turn on/off displaying of alerts and notifications that require no user interaction. Select **Display only notifications requiring user's interaction when running applications in full screen mode** to suppress all noninteractive notifications. From the **Minimum verbosity of events to display** drop-down menu you can select the starting severity level of alerts and notification to be displayed.

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of the user:** field allows you to define who will receive important notifications from ESET Security for Kerio. Normally this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

4.8.2 Disable GUI on Terminal Server

This chapter describes how to disable GUI of ESET Security for Kerio running on Windows Terminal Server for user sessions.

Normally, ESET Security for Kerio GUI starts up every time a remote user logs onto the server and creates a terminal session. This is usually undesirable on Terminal Servers. If you want to turn off the GUI for terminal sessions follow these steps:

1. Run *regedit.exe*
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Right-click on Value *egui* and select *Modify...*
4. Add a */terminal* switch to the end of an existing string

Here is an example of how the Value data of *egui* should be:

```
"C:\Program Files\ESET\ESET Security\egui.exe" /hide /waitservice /terminal
```

If you want to revert this setting and enable automatic startup of the ESET Security for Kerio GUI, remove the */terminal* switch. To get to the *egui* registry Value, repeat steps 1. to 3.

4.9 eShell

eShell (short for ESET Shell) is a command line interface for ESET Security for Kerio. It is an alternative to the graphical user interface (GUI). eShell has all the features and options that the GUI normally gives you. eShell lets you configure and administer the whole program without the use of the GUI.

Apart from all the functions and features that are available in the GUI, it also provides you with the option of using automation by running scripts in order to configure, modify configuration or perform an action. Also, eShell can be useful for those who prefer using the command line over the GUI.

This section explains how to navigate and use eShell as well as lists all the commands with the description of what particular command is used for and what it does.

There are two modes in which eShell can be run:

- Interactive mode - this is useful when you want to work with eShell (not just execute single command) for tasks such as changing configuration, viewing logs, etc. You can also use interactive mode if you are not familiar with the all the commands yet. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a particular context.
- Single command / Batch mode - you can use this mode if you only need to execute a command without entering the interactive mode of eShell. This can be done from the Windows Command Prompt by typing in `eshell` with appropriate parameters. For example:

```
eshell set av document status enabled
```

NOTE: In order to run eShell commands from Windows Command Prompt or to run batch files, you need to have this function enabled first (command `set general access batch always` needs to be executed in interactive mode). For further information about the `set batch` command click [here](#)⁷⁵.

To enter interactive mode in eShell, you can use one of the following two methods:

- Via Windows Start menu: **Start > All Programs > ESET > ESET File Security > ESET shell**
- From Windows Command Prompt by typing in `eshell` and pressing the Enter key

When you run eShell in interactive mode for the first time, a first run screen will display.

```

ESET Shell
ESET Shell 1.1 (4.5.16004.0 BETA)
Copyright (c) 1992-2013 ESET, spol. s r. o. All rights reserved.
-----
First run
To display this information again enter:
    guide      /?      -help

Syntax:
    [<operation>] [<command path>] <command> [<arguments>]

For example, to activate document protection enter:
    set      av document      status      enabled

Operation
The command may or may not support some of the operations. Operations change
the meaning of the command. For example get av status returns the status of
antivirus protection, while set av status enabled enables antivirus protection.
An example of a command with no operation is exit.

Following operations are available:
get      set      select      add      remove      clear      start
stop     pause     resume     restore     send      import     export

For the meaning of the operation in relation to the specific command, see help.
-- More -- (ENTER - Line, SPACE - Page, X - End)

```

It shows you some basic examples how to use eShell with Syntax, Prefix, Command path, Abbreviated forms, Aliases, etc. This is basically a quick guide to eShell.

NOTE: If you want to display the first run screen in future, type in `guide` command.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

4.9.1 Usage

Syntax

Commands must be formatted in the correct syntax to function and can be composed of a prefix, context, arguments, options, etc. This is the general syntax used throughout the eShell:

```
[<prefix>] [<command path>] <command> [<arguments>]
```

Example (this activates document protection):

```
SET AV DOCUMENT STATUS ENABLED
```

SET - a prefix

AV DOCUMENT - path to a particular command, a context where this command belong

STATUS - the command itself

ENABLED - an argument for the command

Using `HELP` or `?` with a command will display the syntax for that particular command. For example, `CLEANLEVEL HELP` will show you the syntax for `CLEANLEVEL` command:

SYNTAX:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

You may notice that `[get]` is in brackets. It designates that the prefix `get` is default for the `cleanlevel` command. This means that when you execute `cleanlevel` without specifying any prefix, it will actually use the default prefix (in this case `get cleanlevel`). Using commands without a prefix saves time when typing. Usually `get` is the default prefix for most commands, but you need to be sure what the default prefix is for particular command and that it is exactly what you want to execute.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Prefix / Operation

A prefix is an operation. The `GET` prefix will give you information about how a certain feature of ESET Security for Kerio is configured or show you the status (such as `GET AV STATUS` will show you current protection status). The `SET` prefix will configure functionality or change its status (`SET AV STATUS ENABLED` will activate protection).

These are the prefixes that eShell lets you use. A command may or may not support any of the prefixes:

- GET - returns current setting/status
- SET - sets value/status
- SELECT - selects an item
- ADD - adds an item
- REMOVE - removes an item
- CLEAR - removes all items/files
- START - starts an action
- STOP - stops an action
- PAUSE - pauses an action
- RESUME - resumes an action
- RESTORE - restores default settings/object/file
- SEND - sends an object/file
- IMPORT - imports from a file
- EXPORT - exports to a file

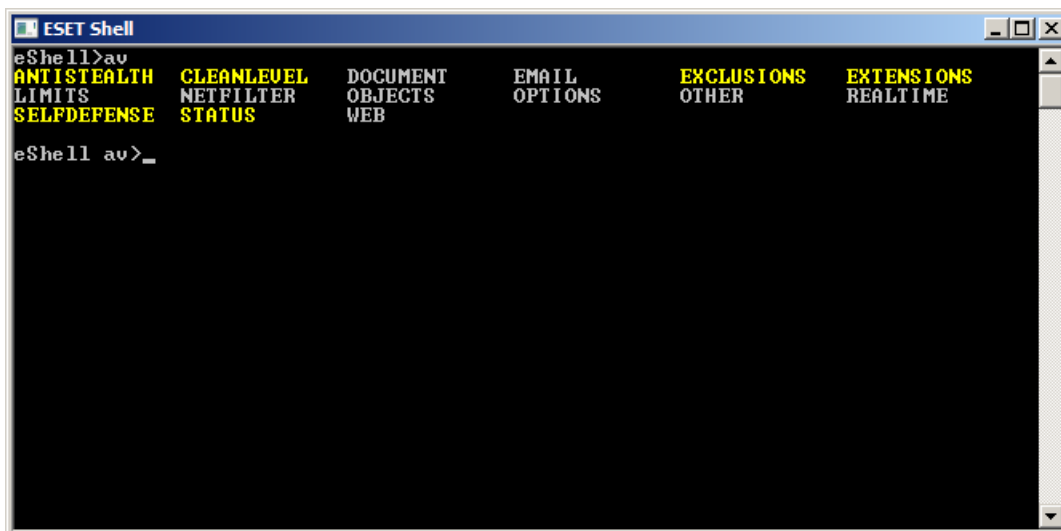
Prefixes such as `GET` and `SET` are used with many commands, but some commands (such as `EXIT`) do not use a prefix.

Command path / Context

Commands are placed in contexts which form a tree structure. The top level of the tree is root. When you run eShell, you are at the root level:

```
eShell>
```

You can either execute a command from here, or enter the context name to navigate within the tree. For example, when you enter `TOOLS` context, it will list all commands and sub-contexts that are available from here.



Yellow items are commands you can execute and grey items are sub-contexts you can enter. A sub-context contains further commands.

If you need to return back to a higher level, use `..` (two dots). For example, say you are here:

```
eShell av options>
```

type `..` and it will get you up one level, to:

```
eShell av>
```

If you want to get back to root from `eShell av options>` (which is two levels lower from root), simply type `.. ..` (two dots and two dots separated by space). By doing so, you will get two levels up, which is root in this case. You can use this no matter how deep within the context tree you are. Use the appropriate number of `..` as you need to get to the desired level.

The path is relative to the current context. If the command is contained in the current context, do not enter a path. For example, to execute `GET AV STATUS` enter:

- `GET AV STATUS` - if you are in the root context (command line shows `eShell>`)
- `GET STATUS` - if you are in the context `AV` (command line shows `eShell av>`)
- `.. GET STATUS` - if you are in the context `AV OPTIONS` (command line shows `eShell av options>`)

Argument

An argument an action which is performed for a particular command. For example, command `CLEANLEVEL` can be used with following arguments:

```
none - Do not clean
normal - Standard cleaning
strict - Strict cleaning
```

Another example are the arguments `ENABLED` or `DISABLED`, which are used to enable or disable a certain feature or functionality.

Abbreviated form / Shortened commands

eShell allows you to shorten contexts, commands and arguments (provided the argument is a switch or an alternative option). It is not possible to shorten a prefix or argument that are concrete values such as a number, name or path.

Examples of the short form:

```
set status enabled => set stat en
add av exclusions C:\path\file.ext => add av exc C:\path\file.ext
```

In a case where two commands or contexts start with same letters (such as `ABOUT` and `AV`, and you enter `A` as shortened command), eShell will not be able to decide which command of these two you want to run. An error message will display and list commands starting with "A" which you can choose from:

```
eShell>a
The following command is not unique: a
```

The following commands are available in this context:

```
ABOUT - Shows information about program
AV - Changes to context av
```

By adding one or more letters (e.g. `AB` instead of just `A`) eShell will execute `ABOUT` command since it is unique now.

NOTE: When you want to be sure that a command executes the way you need, we recommend that you do not abbreviate commands, arguments, etc. and use the full form. This way it will execute exactly as you need and prevent unwanted mistakes. This is especially true for batch files / scripts.

Aliases

An alias is an alternative name which can be used to execute a command (provided that the command has an alias assigned). There are few default aliases:

```
(global) help - ?
(global) close - exit
(global) quit - exit
(global) bye - exit
warnlog - tools log events
virlog - tools log detections
```

"(global)" means that the command can be used anywhere regardless of current context. One command can have multiple aliases assigned, for example command `EXIT` has alias `CLOSE`, `QUIT` and `BYE`. When you want to exit eShell, you can use the `EXIT` command itself or any of its aliases. Alias `VIRLOG` is an alias for command `DETECTIONS` which is located in `TOOLS LOG` context. This way the detections command is available from `ROOT` context, making it easier to access (you don't have to enter `TOOLS` and then `LOG` context and run it directly from `ROOT`).

eShell allows you to define your own aliases.

Protected commands

Some commands are protected and can only be executed after entering a password.

Guide

When you run the `GUIDE` command, it will display a "first run" screen explaining how to use eShell. This command is available from the `ROOT` context (eShell>).

Help

When the `HELP` command is used alone, it will list all available commands with prefixes as well as sub-contexts within the current context. It will also give you a short description to each command / sub-context. When you use `HELP` as an argument with a particular command (e.g. `CLEANLEVEL HELP`), it will give you details for that command. It

will display SYNTAX, OPERATIONS, ARGUMENTS and ALIASES for the command with a short description for each.

Command history

eShell keeps history of previously executed commands. This applies only to the current eShell interactive session. Once you exit eShell, the command history will be dropped. Use the Up and Down arrow keys on your keyboard to navigate through the history. Once you find the command you were looking for, you can execute it again, or modify it without having to type in the entire command from the beginning.

CLS / Clear screen

The `CLS` command can be used to clear screen. It works the same way as it does with Windows Command Prompt or similar command line interfaces.

EXIT / CLOSE / QUIT / BYE

To close or exit eShell, you can use any of these commands (`EXIT`, `CLOSE`, `QUIT` OR `BYE`).

4.9.2 Commands

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Commands contained within **ROOT** context:

ABOUT

Lists information about the program. It shows name of the product installed, version number, installed components (including version number of each component) and basic information about the server and the operating system that ESET Security for Kerio is running on.

CONTEXT PATH:

```
root
```

BATCH

Starts eShell batch mode. This is very useful when running batch files / scripts and we recommend using it with batch files. Put `START BATCH` as the first command in the batch file or script to enable batch mode. When you enable this function, no interactive input is prompted (e.g. entering a password) and missing arguments are replaced by defaults. This ensures that the batch file will not stop in the middle because eShell is expecting the user to do something. This way the batch file should execute without stopping (unless there is an error or the commands within the batch file are incorrect).

CONTEXT PATH:

```
root
```

SYNTAX:

```
[start] batch
```

OPERATIONS:

```
start - Starts eShell in batch mode
```

CONTEXT PATH:

```
root
```

EXAMPLES:

```
start batch - Starts eShell batch mode
```

GUIDE

Displays first run screen.

CONTEXT PATH:

```
root
```

PASSWORD

Normally, to execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands such as those that disable antivirus protection and those that may affect ESET Security for Kerio functionality. You will be prompted for password every time you execute such command. You can define this password in order to avoid entering password every time. It will be remembered by eShell and automatically be used when a password-protected command is executed. This means that you do not have to enter the password every time.

NOTE: Defined password works only for the current eShell interactive session. Once you exit eShell, this defined password will be dropped. When you start eShell again, the password needs to be defined again.

This defined password is also very useful when running batch files / scripts. Here is an example of a such batch file:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

This concatenated command above starts a batch mode, defines password which will be used and disables protection.

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERATIONS:

`get` - Show password

`set` - Set or clear password

`restore` - Clear password

ARGUMENTS:

`plain` - Switch to enter password as parameter

`password` - Password

EXAMPLES:

`set password plain <yourpassword>` - Sets a password which will be used for password-protected commands

`restore password` - Clears password

EXAMPLES:

`get password` - Use this to see whether the password is configured or not (this is only shows only stars "*", does not list the password itself), when no stars are visible, it means that there is no password set

`set password plain <yourpassword>` - Use this to set defined password

`restore password` - This command clears defined password

STATUS

Shows information about the current protection status of ESET Security for Kerio (similar to GUI).

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERATIONS:

`get` - Show antivirus protection status

`set` - Disable/Enable antivirus protection

`restore` - Restores default settings

ARGUMENTS:

`disabled` - Disable antivirus protection

`enabled` - Enable antivirus protection

EXAMPLES:

`get status` - Shows current protection status

`set status disabled` - Disables protection

`restore status` - Restores protection to default setting (Enabled)

VIRLOG

This is an alias of the `DETECTIONS` command. It is useful when you need to view information about detected infiltrations.

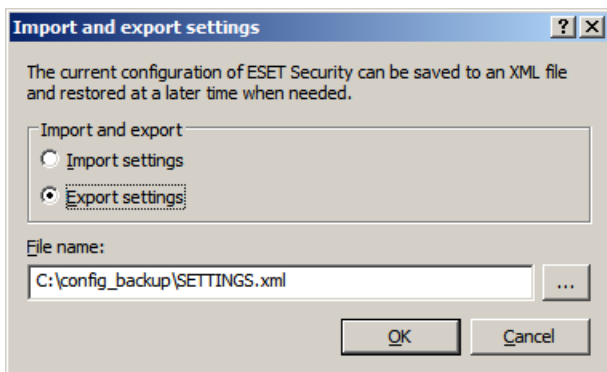
WARNLOG

This is an alias of the `EVENTS` command. It is useful when you need to view information about various events.

4.10 Import and export settings

Importing and exporting configurations of ESET Security for Kerio is available under **Setup** by clicking on **Import and export settings**.

Both import and export use the `.xml` file type. Import and export are useful if you need to backup the current configuration of ESET Security for Kerio to be able to use it later. The export settings option is also convenient for users who wish to use their preferred configuration of ESET Security for Kerio on multiple systems - they can easily import an `.xml` file to transfer the desired settings.



4.11 ThreatSense.Net

The ThreatSense.Net Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional ThreatSense.Net 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 to as many of our customers as possible and use them as our Threat Scouts. There are two options:

1. You can decide not to enable the ThreatSense.Net Early Warning System. You will not lose any functionality in the software, and you will still receive the best protection that we offer.
2. You can configure the ThreatSense.Net Early Warning System to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

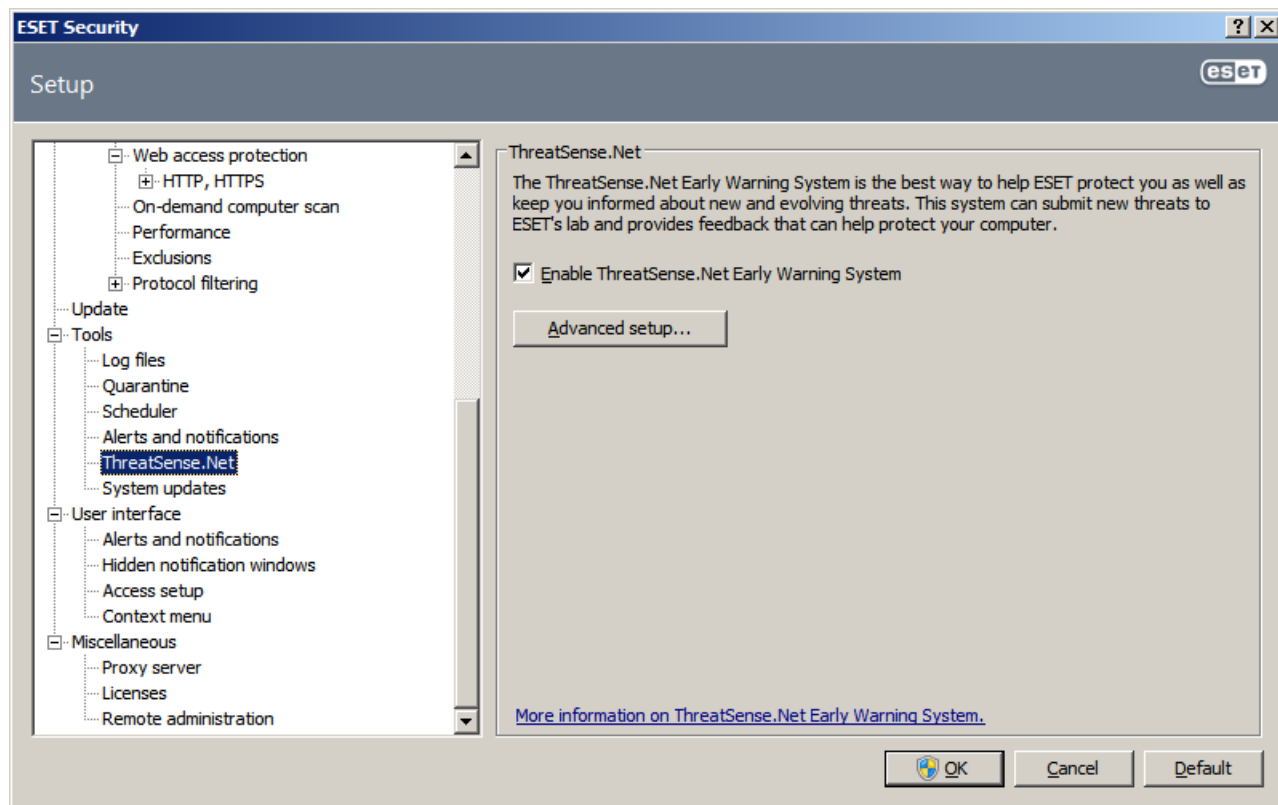
The ThreatSense.Net Early Warning System will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared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

information about your computer's operating system.

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

By default, ESET Security for Kerio is configured to ask before submitting suspicious files for detailed analysis to ESET's Threat Lab. Files with certain extensions such as .doc or .xls are always excluded. You can also add other extensions if there are particular files that you or your organization wants to avoid sending.

The ThreatSense.Net setup is accessible from the Advanced Setup tree, under **Tools > ThreatSense.Net**. Select the **Enable ThreatSense Early Warning System** option to activate and then click the **Advanced setup...** button.

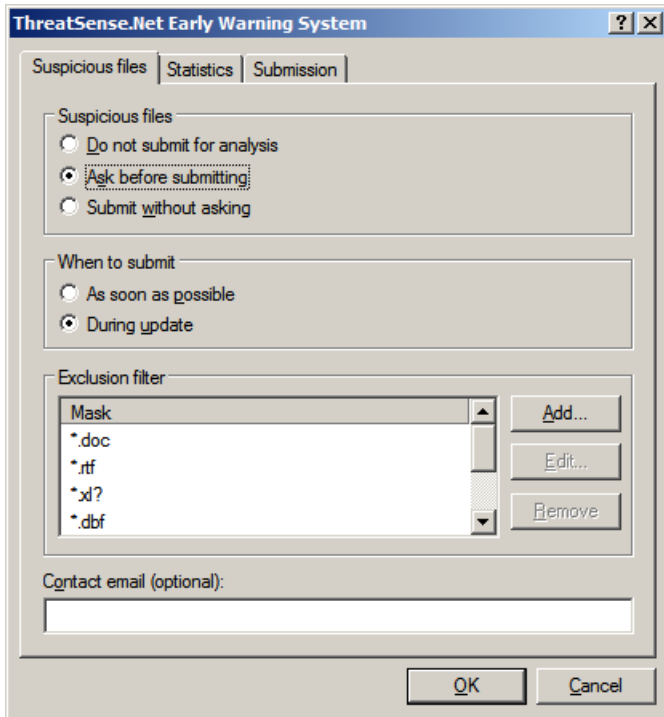


4.11.1 Suspicious files

The **Suspicious files** tab allows you to configure the manner in which threats are submitted to ESET's Threat Lab for analysis.

If you find a suspicious file, you can submit it for analysis to our ThreatLabs. If it is a malicious application, its detection will be added to the next virus signature update.

File submission can be set to occur automatically, or select the **Ask before submitting** option if you wish to know which files have been sent for analysis and confirm the submission.



If you do not want any files to be submitted, select the **Do not submit for analysis** option. Selecting not to submit files for analysis does not affect submission of statistical information which is configured in its own setup (see section [Statistics](#) ^[80]).

When to submit – By default, the **As soon as possible** option is selected for suspicious files to be sent to ESET's Threat Lab. This is recommended if a permanent Internet connection is available and suspicious files can be delivered without delay. Select the **During** update option for suspicious files to be uploaded to ThreatSense.Net during the next update.

Exclusion filter – The Exclusion filter allows you to exclude certain files/folders 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, etc.). You can add to the list of excluded files if desired.

Contact email – Your **Contact email [optional]** can be sent with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

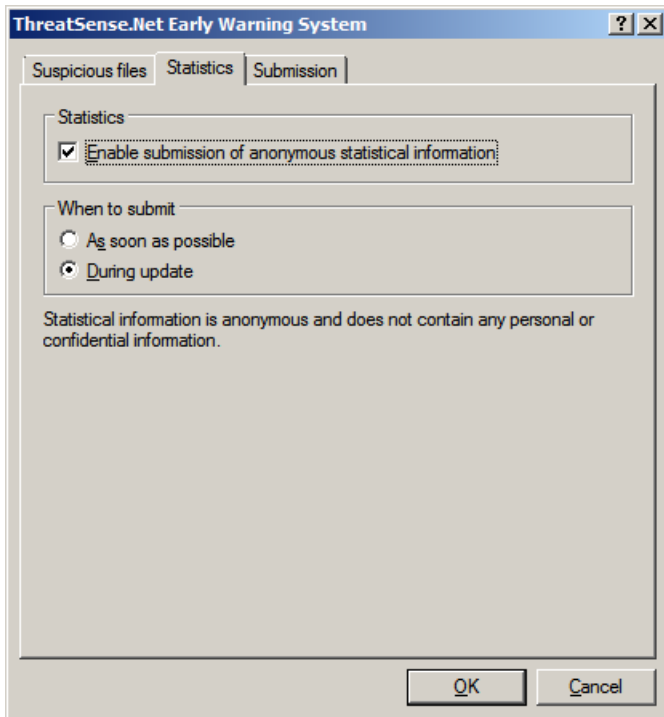
4.11.2 Statistics

The ThreatSense.Net Early Warning System collects anonymous information about your computer related to newly detected threats. This information may include 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. The statistics are typically delivered to ESET's servers once or twice a day.

Below is an example of a statistical package submitted:

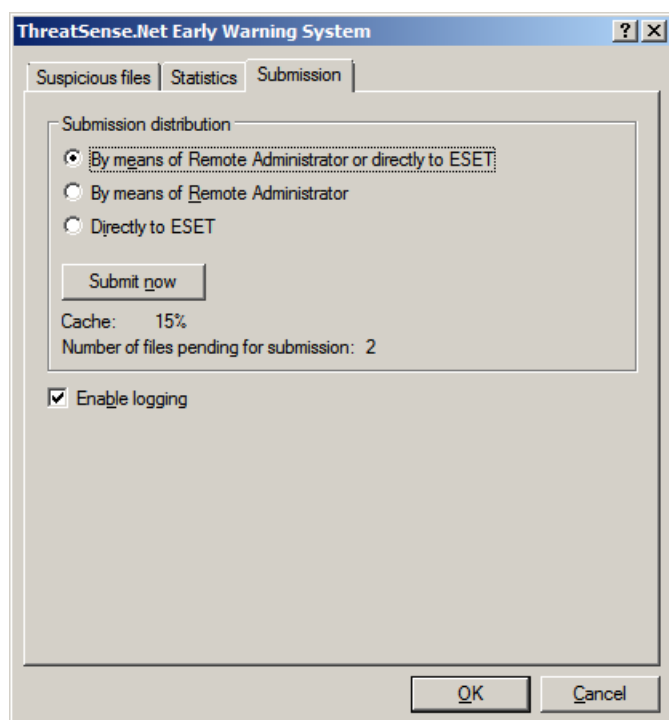
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

When to submit – You can define when the statistical information will be submitted. If you choose to submit **As soon as possible** statistical information will be sent immediately after it is created. This setting is suitable if a permanent Internet connection is available. If the **During update** option is selected, statistical information will be submitted collectively during the next update.



4.11.3 Submission

You can select how files and statistical information will be submitted to ESET. Select the **By means of Remote Administrator or directly to ESET** option for files and statistics to be submitted by any available means. Select the **By means of Remote Administrator** option to submit files and statistics to the remote administration server, which will ensure their subsequent submission to ESET's Threat Lab. If the option **Directly to ESET** is selected, all suspicious files and statistical information are sent to ESET's virus lab directly from the program.



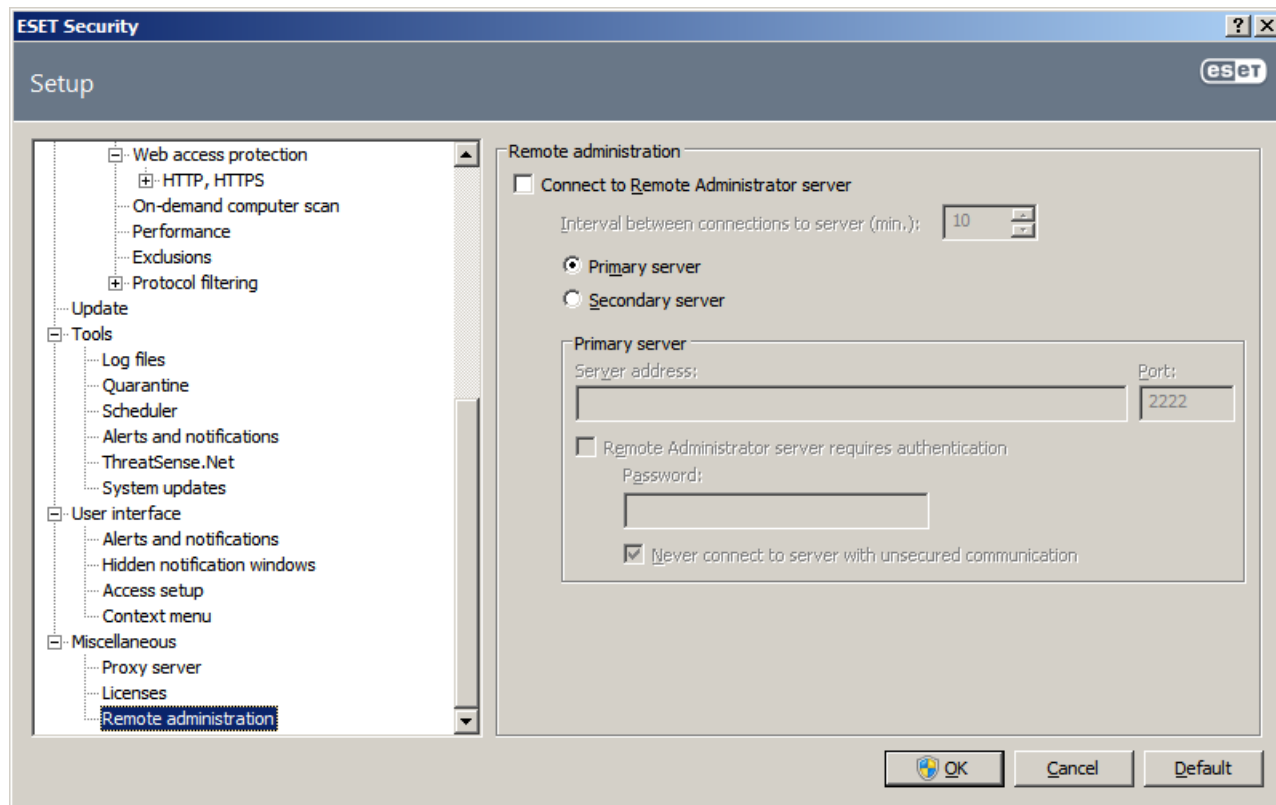
When there are files pending submission, the **Submit now** button will be active. Click this button to immediately submit files and statistical information.

Select the **Enable logging** option to create a log to record file and statistical information submissions.

4.12 Remote administration

ESET Remote Administrator (ERA) is a powerful tool to manage security policy and to obtain an overview of the overall security within a network. It is especially useful when applied to larger networks. ERA not only increases the security level, but also provides ease-of-use in the administration of ESET Security for Kerio on client workstations.

Remote administration setup options are available from the main ESET Security for Kerio program window. Click **Setup > Enter the entire advanced setup tree... > Miscellaneous > Remote administration**.



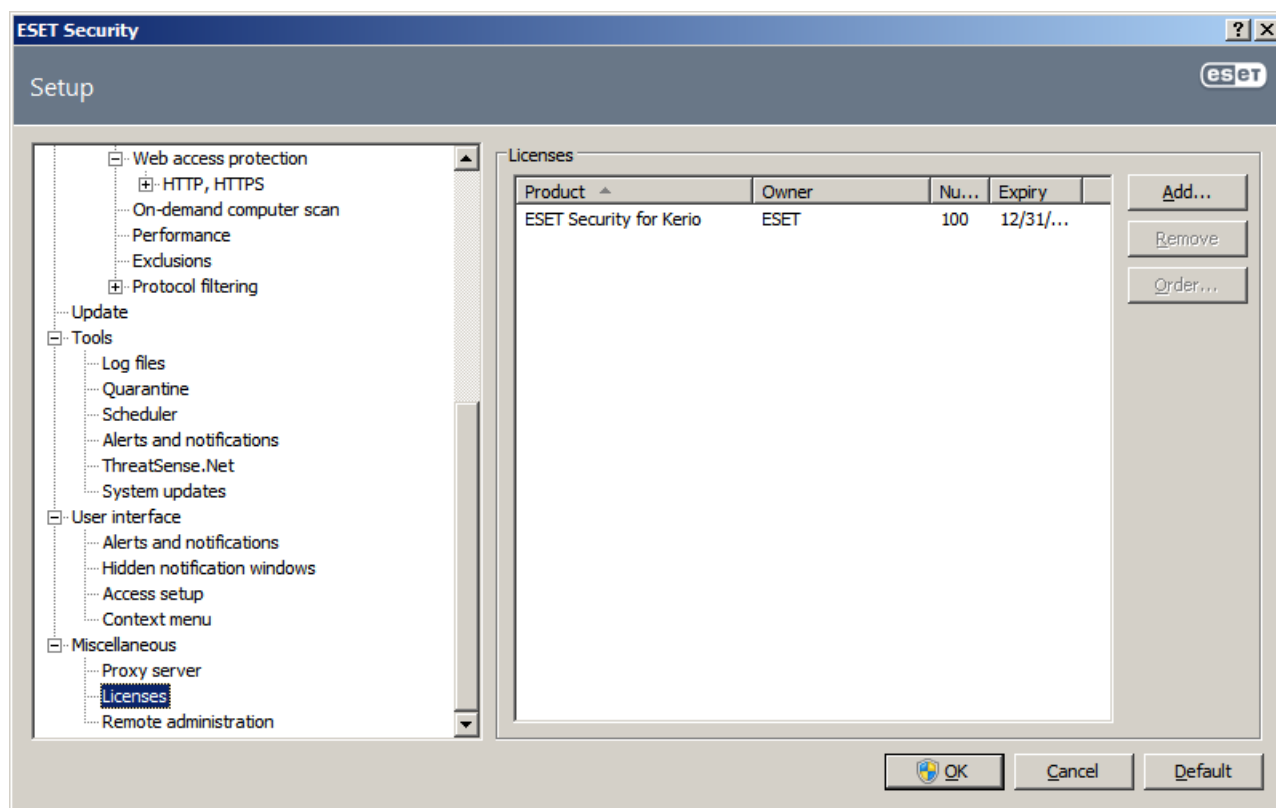
Activate remote administration by selecting the **Connect to Remote Administration server** option. You can then access the other options described below:

- **Interval between connections to server (min.):** This designates the frequency that ESET Security for Kerio will connect to the ERA Server. If it is set to 0, information will be submitted every 5 seconds.
- **Server address:** Network address of the server where the ERA Server is installed.
- **Port:** This field contains a predefined server port used for connection. We recommend that you leave the default port setting of 2222
- **Remote Administrator server requires authentication:** Allows you to enter a password to connect to the ERA Server, if required.

Click **OK** to confirm changes and apply the settings. ESET Security for Kerio will use these settings to connect to the ERA Server.

4.13 Licenses

The **Licenses** branch allows you to manage the license keys for ESET Security for Kerio and other ESET products such as ESET Mail Security, etc. After purchase, license keys are delivered along with your username and password. To **Add/Remove** a license key, click the corresponding button in the license manager window. The license manager is accessible from the Advanced Setup tree under **Miscellaneous > Licenses**.



The license key is a text file containing information about the purchased product: the owner, number of licenses, and the expiration date.

The license manager window allows you to upload and view the content of a license key using the **Add...** button – the information contained is displayed in the manager. To delete license files from the list, click **Remove**.

If a license key has expired and you are interested in purchasing a renewal, click the **Order...** button – you will be redirected to our online store.

5. Glossary

5.1 Types of infiltration

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

5.1.1 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 mainly attack executable files 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 by him/herself.

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. On the other hand, 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 – i.e., to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

5.1.2 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 or even minutes of their release. 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 you delete the infected files because they likely contain malicious code.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

5.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past – today, there is no longer a need for them 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 was 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 with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

Examples of well-known trojans are: NetBus, Trojandownloader, Small.ZL, Slapper

5.1.4 Rootkits

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

There are two levels of detection to prevent rootkits:

- 1) When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
- 2) When they are hidden from the usual testing. ESET Security for Kerio users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

5.1.5 Adware

Adware is a short 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 their creators to cover development costs of their (usually useful) applications.

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

If you decide to use a freeware product, please 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 means that adware may often 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 to delete it, since there is a high probability that it contains malicious code.

5.1.6 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. Spylfalcon 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, it is advisable to delete it, since there is a high probability that it contains malicious code.

5.1.7 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 Security for Kerio provides the option to detect such threats.

“Potentially unsafe applications” is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and [keyloggers](#)^[84] (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

5.1.8 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 state 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
- Application communicates with remote servers

5.2 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, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases – with more complicated aliases, the probability of tracking is lower
- Don't 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 – e.g., one for business, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

5.2.1 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's 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.

5.2.2 Hoaxes

A hoax is misinformation which 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.

5.2.3 Phishing

The term phishing defines a criminal activity which uses techniques of 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 masquerading as 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.

5.2.4 Recognizing spam scams

Generally, there are a few indicators which 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

5.2.4.1 Rules

In the context of Antispam solutions and email clients, rules are tools for manipulating email functions. They consist of two logical parts:

- 1) Condition (e.g., an incoming message from a certain address)
- 2) Action (e.g., deletion of the message, moving it to a specified folder)

The number and combination of rules varies with the Antispam solution. These rules serve as measures against spam (unsolicited email). Typical examples:

- Condition: An incoming email message contains some of the words typically seen in spam messages 2. Action: Delete the message
- Condition: An incoming email message contains an attachment with an .exe extension 2. Action: Delete the attachment and deliver the message to the mailbox
- Condition: An incoming email message arrives from your employer 2. Action: Move the message to the "Work" folder

We recommend that you use a combination of rules in Antispam programs in order to facilitate administration and to more effectively filter spam.

5.2.4.2 Bayesian filter

Bayesian spam filtering is an effective form of email filtering used by almost all Antispam products. It is able to identify unsolicited email with high accuracy and can work on a per-user basis.

The functionality is based on the following principle: The learning process takes place in the first phase. The user manually marks a sufficient number of messages as legitimate messages or as spam (normally 200/200). The filter analyzes both categories and learns, for example, that spam usually contains the words "rolex" or "viagra", and legitimate messages are sent by family members or from addresses in the user's contact list. Provided that a sufficient number of messages are processed, the Bayesian filter is able to assign a specific "spam index" to each message in order to determine whether it is spam or not.

The main advantage of a Bayesian filter is its flexibility. For example, if a user is a biologist, all incoming emails concerning biology or relative fields of study will generally receive a lower probability index. If a message includes words that would normally qualify it as unsolicited, but it is sent by someone from the user's contact list, it will be marked as legitimate, because senders from a contact list decrease overall spam probability.

5.2.4.3 Whitelist

In general, a whitelist is a list of items or persons who are accepted, or have been granted permission. The term "email whitelist" defines a list of contacts from whom the user wishes to receive messages. Such whitelists are based on keywords searched for in email addresses, domain names, or IP addresses.

If a whitelist works in "exclusivity mode", then messages from any other address, domain, or IP address will not be received. If a whitelist is not exclusive, such messages will not be deleted, but filtered in some other way.

A whitelist is based on the opposite principle to that of a [blacklist](#)^[88]. Whitelists are relatively easy to maintain, more so than blacklists. We recommend that you use both the Whitelist and Blacklist to filter spam more effectively.

5.2.4.4 Blacklist

Generally, a blacklist is a list of unaccepted or forbidden items or persons. In the virtual world, it is a technique enabling acceptance of messages from all users not present on such a list.

There are two types of blacklist. Those created by users within their Antispam application, and a professional, regularly updated blacklists which are created by specialized institutions and can be found on the Internet.

It is essential to use blacklists to successfully block spam, but they are difficult to maintain, since new items to be blocked appear every day. We recommended you use both a [whitelist](#)^[88] and a blacklist to most effectively filter spam.

5.2.4.5 Server-side control

Server-side control is a technique for identifying mass spam based on the number of received messages and the reactions of users. Each message leaves a unique digital “footprint” based on the content of the message. The unique ID number tells nothing about the content of the email. Two identical messages will have identical footprints, while different messages will have different footprints.

If a message is marked as spam, its footprint is sent to the server. If the server receives more identical footprints (corresponding to a certain spam message), the footprint is stored in the spam footprints database. When scanning incoming messages, the program sends the footprints of the messages to the server. The server returns information on which footprints correspond to messages already marked by users as spam.