Contents

1. Introduction .................................................. 6
  1.1 Overview.................................................. 6
  1.2 Help pages............................................... 7

2. User Interface ................................................ 10
  2.1 Safe mode.................................................. 10

3. Installation .................................................... 11
  3.1 Requirements.............................................. 11
  3.2 Typical installation....................................... 11
  3.3 Custom installation....................................... 12
  3.4 Upgrading to a newer version......................... 13
  3.5 Post-installation configuration....................... 14

4. IBM Lotus Domino server protection ............... 16
  4.1 IBM Lotus Domino........................................ 16
  4.1.1 Protected processes.................................. 16
  4.1.2 Quarantine settings................................... 16
  4.2 On-demand database scan.............................. 17
  4.3 Rules........................................................ 17
  4.4 Log files.................................................. 17
  4.5 Performance.............................................. 18
  4.6 Antivirus and antispyware settings................. 18
  4.6.1 IBM Lotus Domino.................................... 18
  4.6.1.1 Mail................................................ 18
  4.6.1.2 Database............................................ 19
  4.6.2 Actions................................................ 20
  4.6.3 Alerts and notifications............................. 20
  4.6.4 Automatic exclusions............................... 20
  4.7 Antispam protection.................................... 21
  4.7.1 IBM Lotus Domino antispam protection......... 21
  4.7.2 Antispam engine....................................... 22
  4.7.2.1 Antispam engine parameter setup.............. 22
  4.7.2.1.1 Analysis.......................................... 22
  4.7.2.1.1.1 Samples......................................... 22
  4.7.2.1.1.1.1 List of cache memory files................ 23
  4.7.2.1.2 Training........................................... 23
  4.7.2.1.3 Rules.............................................. 24
  4.7.2.1.3.1 Rule weight.................................... 24
  4.7.2.1.3.2 List of downloaded rule files.............. 24
  4.7.2.1.3.3 Category weight.............................. 25
  4.7.2.1.3.4 Custom rules list............................ 25
  4.7.2.1.4 Filtering.......................................... 25
  4.7.2.1.4.1 Allowed senders.............................. 25
  4.7.2.1.4.2 Blocked senders.............................. 25
  4.7.2.1.4.3 Allowed IP addresses....................... 25
  4.7.2.1.4.4 Ignored IP addresses....................... 26
  4.7.2.1.4.5 Blocked IP addresses....................... 26
  4.7.2.1.4.6 Allowed domains............................ 26
  4.7.2.1.4.7 Ignored domains............................ 26
  4.7.2.1.4.8 Blocked domains............................. 26
  4.7.2.1.4.9 Spoofed senders.............................. 26
  4.7.2.1.5 Verification.................................... 26
  4.7.2.1.5.1 RBL (Realtime Blackhole List)............ 26
  4.7.2.1.5.1.1 List of RBL servers....................... 27
  4.7.2.1.5.1.2 LBL (Last Blackhole List)................ 27
  4.7.2.1.5.1.3 List of LBL servers....................... 27
  4.7.2.1.5.2 List of skipped IP addresses............... 27
  4.7.2.1.5.3 DNSBL (DNS Block List)..................... 27
  4.7.2.1.5.3.1 List of DNSBL servers.................... 27
  4.7.2.1.6 DNS............................................... 27
  4.7.2.1.7 Score............................................. 28
  4.7.2.1.8 Spamblai......................................... 28
  4.7.2.1.8.1 Spamblai addresses.......................... 28
  4.7.2.1.8.2 Addresses regarded as nonexistent........ 29
  4.7.2.1.9 Communication.................................. 29
  4.7.2.1.10 Performance.................................... 29
  4.7.2.1.11 Regional settings............................. 29
  4.7.2.1.11.1 List of home languages.................... 29
  4.7.2.1.11.2 List of home countries................... 31
  4.7.2.1.11.3 List of blocked countries................ 34
  4.7.2.1.11.4 List of blocked charsets.................. 35
  4.7.2.1.12 Log files........................................ 35
  4.7.2.1.13 Statistics....................................... 35
  4.7.2.1.14 Options.......................................... 35
  4.7.3 Alerts and notifications............................ 35

5. Computer protection ..................................... 36
  5.1 Program menu............................................ 36
  5.2 Protection status........................................ 36
  5.2.1 Watch activity........................................ 37
  5.2.2 Statistics............................................... 37
  5.3 Database scan............................................ 38
  5.3.1 On-demand database scan.......................... 38
  5.4 Computer scan............................................ 38
  5.4.1 Computer scan - Window........................... 39
  5.4.2 Scan targets.......................................... 39
  5.4.2.1 Scan SetUp.......................................... 39
  5.4.2.1.1 Scan completed successfully.................. 40
  5.4.2.1.2 Scan set up....................................... 40
  5.4.3.1 Select scan targets............................... 40
  5.4.4 Command line.......................................... 40
  5.5 Updating the program.................................. 42
  5.5.1 Update.................................................. 43
  5.5.1.1 Username and password setup.................... 43
  5.5.1.2 Operating system updates........................ 43
  5.5.1.2.1 Update information............................. 43
  5.5.1.2.2 Operating system update - settings............ 43
  5.5.2 Update setup.......................................... 44
  5.5.2.1 Update mode........................................ 44
  5.5.2.2 HTTP Proxy.......................................... 45
  5.5.2.3 LAN connection setup............................. 45
  5.5.2.4 Mirror............................................... 45
  5.5.2.4.1 Advanced setup.................................. 46
  5.6 Setup..................................................... 46
  5.6.1 Antivirus and antispyware protection............... 47
  5.6.1.1 Antivirus and antispyware protection setup..... 47
  5.6.1.2 Real-time file system protection................. 47
  5.6.1.2.1 Control setup.................................... 48
  5.6.1.2.1.1 Media to scan.................................. 48
  5.6.1.2.1.2 Scan on (Event-triggered scanning)........ 48
  5.6.1.2.1.3 Advanced scan options....................... 48
  5.6.1.2.1.1.1 Removable media block setup................ 49
  5.6.1.2.2 Cleaning levels.................................. 49
  5.6.1.2.3 When to modify real-time protection configuration... 49
  5.6.1.2.4 Checking real-time protection................ 49
8.2 Email ................................................................. 191
  8.2.1 Advertisements ........................................ 191
  8.2.2 Hoaxes ..................................................... 192
  8.2.3 Phishing ..................................................... 192
  8.3 Recognizing spam scams ................................ 192
    8.3.1 Rules ..................................................... 193
    8.3.2 Bayesian filter ........................................ 193
    8.3.3 Whitelist ................................................ 193
    8.3.4 Blacklist ................................................ 193
    8.3.5 Server-side control .................................. 194

7. Help and support .............................................. 187
  7.1 About ESET Mail Security ................................. 187
  7.2 Troubleshooting ............................................. 187
  7.3 Selection of data to submit ................................ 187
  7.4 Confirmation and submitted data ........................ 188
  7.5 Finish .......................................................... 188
  7.6 Support wait ................................................... 188

8. Glossary .......................................................... 189
  8.1 Types of infiltration ......................................... 189
    8.1.1 Viruses ................................................... 189
    8.1.2 Worms .................................................... 189
    8.1.3 Trojan horses ........................................... 189
    8.1.4 Rootkits ................................................... 190
    8.1.5 Adware ..................................................... 190
    8.1.6 Spyware ................................................... 190
    8.1.7 Potentially unsafe applications ..................... 191
    8.1.8 Potentially unwanted applications ................ 191
1. Introduction

ESET Mail Security for IBM Lotus Domino is an integrated solution to protect the databases and user mailboxes in the IBM Lotus Domino environment from various types of malware (for more information about threats see the chapter on Types of infiltration). ESET Mail Security provides three types of protection: Antivirus, Antispam and the application of user-defined rules.

**NOTE**: While providing IBM Lotus Domino protection, ESET Mail Security also has tools to protect the server machine itself.

1.1 Overview

This picture represents the basic schema for how the protection in ESET Mail Security for IBM Lotus Domino works.

**1. Mail Action**
- **SMTP**: Action taken on messages received through the SMTP protocol. See the chapter Message filtering (SMTP level) for more details. The messages are scanned using the Greylisting technique, the antivirus and antispam module and user-defined rules.

**2. Database Action**

All actions regarding the database (read/write). See the chapter Database scan for more information. When the files are written into the database or retrieved from the database (read), they are scanned again by the antivirus module and user-defined rules.
1.2 Help pages

Dear valued customer, we are glad to welcome you among the users of ESET Mail Security. We believe that the information within the help pages will make the work you do with your computer more comfortable and secure.

We prepared a guide to help you setup and customize the basic settings of ESET Mail Security.

Help topics are divided into several chapters and sub-chapters to allow for a better orientation. You can find related information by simply browsing the help pages structure.

To learn more about any window in the program, simply press F1. The help page related to the window you are currently viewing will be displayed.

The program allows you to search for a topic within the help pages by keywords or by typing words or phrases to be searched for in the content of Help pages. The difference between these two methods is that a keyword may be logically related to help pages which do not contain that particular keyword in the text. Searching by words and phrases will search the content of all pages and display only those containing the searched word or phrase in the actual text.

1.3 Types of protection

ESET Mail Security uses three types of protection:

1. Antivirus protection
2. Antispam protection
3. User-defined rules

1.3.1 Antivirus protection

Antivirus protection is one of the basic functions of the ESET Mail Security product. 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 blocking it and then cleaning, deleting or moving it to the quarantine for infected files from the IBM Lotus Domino server.

1.3.2 Antispam protection

Antispam protection integrates several technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Rules, Manual whitelisting/blacklisting, etc.) to achieve maximum detection of email threats. The antispam scanning engine's output is the spam probability value of the given email message expressed as a percentage (0 to 100).

Another component of the antispam protection module is the Greylisting technique (disabled by default). The technique relies on the RFC 821 specification, which states that since SMTP is considered an unreliable transport, every message transfer agent (MTA) should repeatedly attempt to deliver an email after encountering a temporary delivery failure. A substantial part of spam consists of one-time deliveries (using specialized tools) to a bulk list of email addresses generated automatically. A server employing Greylisting calculates a control value (hash) for the envelope sender address, the envelope recipient address and the IP address of the sending MTA. If the server cannot find the control value for the triplet within its own database, it refuses to accept the message, returning a temporary failure code (temporary failure, for example, 451). A legitimate server will attempt a redelivery of the message after a variable time period. The triplet's control value will be stored in the database of verified connections on the second attempt, allowing any email with relevant characteristics to be delivered from then on.
1.3.3 User-defined rules

You can use the ESET Mail Security user interface to create individual rules that may be combined to create new rules. If one rule uses multiple conditions, the conditions will be linked using the logical operator AND. Consequently, the rule will be executed only if all conditions are fulfilled. If multiple rules are created, the logical operator OR will be applied, and the program will run the first rule where the conditions are met. See the chapter Rules for more information.

Note: ESET Mail Security supports two types of antivirus protection: Antivirus protection of the IBM Lotus Domino server, which checks the notes in the Domino server databases and the System real-time protection, that checks the Microsoft windows operating system itself.

1.4 Methods used

Communication between the IBM Lotus Domino server and ESET Mail Security is secured by a plug-in (LMON.dll) that is loaded on the server startup as a part of the IBM Lotus Domino Extension manager. If this plug-in is loaded it is a part of every important process running on the server.

Note: The server configuration is stored in the notes.ini file on the server. In this file, all plug-ins loaded on startup are shown in the EXTMGR_ADDINS row. The ESET Mail Security plug-in loaded on the startup is notified about every important event, for example: a new connection, a new message in a mailbox, when a file in a database is accessed and so on. During the installation, the files LMON.dll and LmonLang.dll are copied into the Domino Server directory (The file LmonLang.dll is only present in localized versions of the product).

1.4.1 Message filtering (SMTP level)

When a message arrives through the SMTP, the following actions are taken in the scanning sequence:

1. The message is scanned using the Greylisting technique (if enabled). For more information, see the chapter antispam protection.
2. The message is then scanned by the user-defined rules. See the chapter rules for more information on how they work.
3. The message is scanned by the antispam module.
4. The message is scanned by the antivirus module.

If the message is infected or recognized as a spam, the appropriate action is taken. If the message is clean, it will be received by the client.

1.4.2 Message filtering (NRPC level)

NRPC stands for Notes remote procedure call. This protocol is used for internal communication on the IBM Lotus Domino server.

When a message arrives through the NRPC, the following actions are taken in the scanning sequence:

1. The message is put in a dead state for the scan.
2. The message is then scanned by the user-defined rules. See the chapter rules for more information on how they work.
3. The message is scanned by the antivirus module.
4. The message is forwarded to the client.

If the message is infected or recognized as a spam, the appropriate action is taken. If the message is clean, it will be received by the client.

Note: IBM Lotus Domino statistics can be influenced by the messages being scanned (put on hold).
1.4.3 Database scan

ESET Mail Security protects the shared server databases when writing/reading notes on the IBM Lotus Domino server. When a note is opened or saved by the user, it is scanned again, by the antivirus module and for User-defined rules. First, the user-defined rules are applied, and then the antivirus module.
2. User Interface

ESET Mail Security’s graphical user interface (GUI) was 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 that 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 three main sections: Server protection, Computer protection and Tools. The Server protection section contains items concerning ESET Mail Security settings specific to IBM Lotus Domino server protection and Automatic exclusions specific to the server's operating system and system files. The Computer protection section contains the configurable items for the protection of the server itself. For more information about the user interface settings, see the User interface options chapter. For more information and configuration settings for tools, please go to the Tools chapter.

2.1 Safe mode

If the graphical interface of ESET Mail Security is launched in safe mode, a dialog window reporting that the application is to be run in safe mode is displayed. Since in safe mode the operation of all programs is limited, it is not possible to open the graphical interface of ESET Mail Security as in the standard mode.

The displayed window will let you run a computer scan. If you wish to check your computer for malicious code, select the option Yes. Doing so will launch scanning in a separate window using the same parameters as the default computer scan profile after the installation of ESET Mail Security.

Select the option No to close the dialog window; ESET Mail Security will perform no action.
3. Installation

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 Mail Security on a freshly installed and configured operating system, if possible. However, if you need to install it on an existing system, make sure that there are no other security solutions installed. If this is the case, uninstall all other security solutions, restart the server and install ESET Mail Security afterwards.

**NOTE:** If you currently have ESET NOD32 Antivirus for IBM Lotus Domino version 2.7 running on your system, you need to uninstall it prior to installing ESET Mail Security. Upgrade is not supported. For detailed instructions, please read this [KB Article](#).

3.1 Requirements

Hardware requirements depend on the operating system version and the version of IBM Lotus Domino being used. We recommend reading IBM Lotus Domino product documentation for more detailed information on hardware requirements.

**Supported Operating Systems:**
- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012

Supported IBM Lotus Domino versions: Version 6.5.4 and higher.

3.2 Typical Installation

**Typical installation** mode quickly installs ESET Mail Security 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. After ESET Mail Security has been installed on your system, you can modify the options and configuration settings at any time.

1. You will be notified that it is necessary to manually stop the IBM Lotus Domino server before installation. Failure to stop the IBM Lotus Domino server can result in incorrect installation.

2. Enter the **Update parameters** you received after purchasing ESET Mail Security, or select **Set update parameters later**. Update parameters are used to receive the latest updates that ensure maximum protection.

3. Upload your license(s) to the **License Manager**. You can also upload multiple licenses and merge them. These are used for the clients communicating with the server. After you upload the license you will see the following information about the selected license: Name of the **Owner**, **Number of licenses** and the **Expiration** date.

4. Select whether you want to **Enable ThreatSense.Net Early Warning System** on your computer. 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 through the ThreatSense.Net Early Warning System.

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

6. Confirm the installation by clicking **Install**.
3.3 Custom Installation

Custom installation is suitable for administrators who want to configure ESET Mail Security during the installation process.

1. You will be notified that it is necessary to manually stop the IBM Lotus Domino server before the installation. Please make sure that the server is stopped, otherwise the product may install correctly.

2. Select the installation folder for ESET Mail Security.

3. Enter the Update parameters you received after purchasing ESET Mail Security, or select Set update parameters later. Update parameters are used to receive the latest updates and ensure maximum protection.

4. Upload your license(s) to the License Manager. You can also upload multiple licenses and merge them. These are used for the clients communicating with the server. After you upload the license, you will see the following information about the selected license: Name of the Owner, Number of licenses and the Expiration date.

5. Configure your proxy server settings (if applicable). 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. Once your proxy server details are entered, click Apply and confirm the selection. If you would like to have the proxy server configured automatically, use 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.

6. 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 Never update program components. Select Ask before downloading program components to display a confirmation window before downloading program components. To download program component upgrades automatically, select Always update program components.

**NOTE:** After a program component update, a restart is usually required. We recommend selecting Never restart computer. The latest component updates will come into effect after the next server restart (whether it is scheduled, manual or otherwise). You can select 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.

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

8. The next two installation steps, ThreatSense.Net Early Warning System and Detection of potentially unwanted applications are the same as the Typical Installation mode steps 3 and 4.

9. Select whether you want to Enable Greylisting on the IBM Lotus Domino mail server. Greylisting is a method that protects users against spam by temporarily rejecting messages from unidentified sources. If the source is legitimate, the message will be delivered (after a period of time).

10. The final step in Custom installation mode is to confirm the installation by clicking Install.

**Note:** During installation, the following files are copied into the IBM Lotus Domino folder:

- **LMON.dll** - Communication with the ESET Security product.
- **LmonLang.dll** - Localization for different languages.
- **LMON_SCANNER.exe** - On Demand database scan.
- **EsetQuarantine.ntf** - Template for the ESET Quarantine.

Also, following changes are made in the server configuration:

- **LMON** is added to the EXTMGR_ADDINS.
- **LMON_SCANNER** is added to the ServerTasks configuration.
3.4 Upgrading to a newer version

Newer versions of ESET Mail Security are issued to bring improvements or fix issues that cannot be resolved by automatic program module updates. Upgrading to a newer version can be done in one of several ways:

1. Automatically upgrade by means of a program component update (PCU)
   Since program component updates are distributed to all users and may have an impact on certain system configurations, they are issued after a long period of testing to ensure a smooth upgrade process on all possible system configurations. If you need to upgrade to a newer version immediately after it has been released, use one of the following methods.

2. Manually upgrade by downloading and installing a new version over the previous installation
   At the beginning of the installation, you can choose to preserve current program settings by selecting the Use current settings check box.

3.5 Post-Installation configuration

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

**System exclusions** - There are files excluded from the real time file system protection by default. These exclusions help prevent conflicts with the system files and certain applications and ensure smooth system performance. These exclusions are predefined by the Automatic exclusions functionality of ESET Mail Security. By default, the server operating system and core applications are excluded. Check the excluded files and be careful when changing these settings.

**Antispam protection setup**

This section describes the settings, methods and techniques you can use to protect your network from spam. We recommend reading the following instructions carefully before choosing the most suitable combination of settings for your network.

**Spam management**

To ensure a high level of Antispam protection you must set actions to be performed on messages already marked as SPAM.

There are three options available:

1. **Deleting spam** - The criteria for a message to be marked as SPAM by ESET Mail Security are set reasonably high, decreasing the chances of deleting legitimate email. The more specific the Antispam settings, the less likely it is that legitimate email will be deleted. Advantages of this method include very low consumption of system resources and less administration. The drawback of this method is that if a legitimate email is deleted, it cannot be restored locally.

2. **Quarantine** - This option excludes the risk of deleting legitimate email. Messages can be restored and resent to the original recipients immediately. The drawbacks of this method are higher consumption of system resources and additional time required for email quarantine maintenance. For further details regarding Quarantine and different methods, see the chapter on Quarantine settings.

3. **Forwarding spam** - Spam will be forwarded along to its recipient. Information about this SPAM will be added to the message header and actions will be taken accordingly.

**Spam filtering**

**Antispam Engine** - See the Antispam engine chapter for additional information and Antispam settings.

We recommend defining a list of blocked and allowed IP addresses before running the server:

1. Open the Advanced setup tree and go to Antispam protection. Select Enable antispam protection.

2. Go to the Antispam engine section.

3. Click Set... and define allowed, ignored and blocked IP addresses.

**Greylisting** - Greylisting is a method protecting users from spam using the following technique: Transport agent sends a "temporarily reject" SMTP return value (default is 451/4.7.1) for any email from a sender it does not recognize. A legitimate server will attempt to redeliver the message. Spammers typically do not attempt to redeliver messages, because they go through thousands of email addresses at a time and typically cannot spend extra time on resending. Greylisting must be thoroughly configured, or else unwanted operational flaws (e.g., delays in legitimate message deliveries etc.) may occur. These negative effects recede continuously as this method fills the internal whitelist with trusted connections. If you are not familiar with this method, or if you consider its negative side-effect unacceptable, we recommend that you disable the method in the Advanced settings menu under Antispam protection > IBM Lotus Domino > Enable Greylisting. We recommend disabling greylisting if you intend to test the product's basic functionalities and do not want to configure the advanced features of the program.

**NOTE**: Greylisting is an additional layer of antispam protection and does not have any effect on the spam evaluation capabilities of the antispam module.
Antivirus protection setup

**Quarantine** - Depending on the type of cleaning mode you are using, we recommend that you configure an action to be performed on infected messages (messages that couldn't be cleaned by the time of the scan). This option can be set in the Advanced settings window **Server protection > Antivirus and antispyware > IBM Lotus Domino > Mail / Database**.

If the option to move messages into email quarantine is enabled, you need to configure the quarantine under **Server protection > IBM Lotus Domino > Quarantine**.

**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: \( \text{number of ThreatSense scan engines} = (\text{number of physical CPUs} \times 2) + 1 \). Also, the **number of scan threads** should be equal or higher as the **number of ThreatSense 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.
4. IBM Lotus Domino server protection

ESET Mail Security provides protection for the IBM Lotus Domino messaging server (depending on the type of servers used in your environment). There are three essential types of protection: Antivirus, Antispam and the application of user-defined rules.

This section describes the Advanced Setup tree (FS) where the settings for the IBM Lotus Domino server protection can be modified. The chapters are in the same structure as in the actual product.

Click Detect installed servers to display currently detected IBM Lotus Domino servers.

4.1 IBM Lotus domino

In this section, you can set the general settings for ESET Mail Security.

Protected IBM Lotus Domino servers: - List of all detected IBM Lotus Domino servers (partitions). If the check box is selected, the server is protected by the ESET Mail Security. Changes will be active after the IBM Lotus Domino server restart.

Protected tasks - List of all important server tasks protected by the ESET Mail Security. Server tasks are protected by default. To add more tasks or remove default tasks, click Select... any change requires restarting the IBM Lotus Domino server or the affected task.

SMTP scanning

When deleting messages, send SMTP reject response:

- If unchecked, the server sends an OK SMTP response to the sender's Mail Transfer Agent (MTA) in the format '250 2.5.0 – Requested mail action okay, completed' and then performs a silent drop.
- If checked, an SMTP reject response is sent back to the sender's MTA. You can type a response message in the following format:

<table>
<thead>
<tr>
<th>Primary response code</th>
<th>Complementary status code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>554</td>
<td>5.6.0</td>
<td>Invalid content</td>
</tr>
</tbody>
</table>

4.1.1 Protected processes

You can add (>>) or remove (<) important server processes from the List of Domino processes that will be protected by the ESET Mail Security or write them into the window manually and separate them with a comma (,).

Protected by default are the mail transferring processes (router, smtp, imap, pop3) and the server task. Protection of the server task can not be disabled.

4.1.2 Quarantine settings

One of the basic steps in setting up protection in ESET Mail Security is creating the quarantine that safely stores infected notes. Only the administrator of the IBM Lotus Domino mail server has access to the quarantine. This quarantine is excluded from additional scanning.

The quarantine has different view options, depending on the note type (mail, document), subcategory and reason for storing the file in the quarantine (spam, infected file, user-defined rule). It is possible to recover a quarantined note, recovered notes will be copied into the original database in which they were stored. These notes will be scanned again after recovery. If the reason for quarantine is no longer present, a note will be handled normally. If these reasons persist, a note will be stored in the quarantine again. Notes are not scanned by the antispam module after recovery.

Note: Only the administrator has access to the quarantine. In order for the quarantine to work properly, scripts must be enabled when the administrator opens the quarantine for the first time.

Quarantine

- **Automatically create quarantine** - By default, this option is enabled. It will automatically create a server database (NSF) where quarantined messages or documents are stored.

- **Quarantine filename**: Choose a name for the quarantine. By default, it is eQuarantine.nsf.

Note: The quarantine is created after the first infected file is found and sent to the quarantine. If the Automatically
create quarantine option is not selected and the quarantine is not created, the file will be processed. The quarantine is created from the EsetQuarantine.ntf template, which is copied into the IBM Lotus Domino data folder during the installation. Each IBM Lotus Domino server partition has its own quarantine.

Maintenance

- **Automatically delete notes in quarantine:**

  - **Delete notes older than (days):** - Automatically deletes quarantined notes after a selected amount of time. The predefined value is 30 days.

4.2 On-demand database scan

Configure the On-demand database scan by clicking Setup and adjusting the ThreatSense engine parameters setup. See the chapter Database for more information.

4.3 Rules

Rules allow you to manually define email and database entries filtering conditions, and actions to take with filtered emails/notes. Rules are applied according to a set of combined conditions. Multiple conditions are combined with logical operators, applying the rule when the conditions are met. The Hits column (next to each rule name) displays the number of times the rule was successfully applied. The rules are applied on all 3 levels (SMTP/NRPC/Database).

**NOTE:** By default, messages and notes are scanned on multiple levels. Thus the rule can be applied multiple times and the Hits count increases accordingly.

- **Add...** - Adds a new rule.
- **Edit...** - Modifies an existing rule.
- **Remove** - Removes a selected rule.
- **Clear** - Clears the rule counter (the Hits column).
- **Move up** - Moves a selected rule up in the list.
- **Move down** - Moves a selected rule down in the list.

Deselecting a check box (to the left of each rule name) deactivates the current rule. This allows for the rule to be reactivated again if needed. By default, all rules are unchecked (inactive).

**NOTE:** You can also use system variables (for example, %PATH%\%) when configuring rules.

**NOTE:** If a new rule has been added or an existing rule has been modified, a message rescan will automatically use the new/modified rules (when starting a new scan).

4.4 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 server performance.

If Synchronized writing without using cache is enabled, all the log entries will immediately be written in the log file without being stored in the log cache. By default, ESET Mail Security components running in IBM Lotus Domino server 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 Mail Security writes the name of all triggered rules into the log file.
- **Log spam score** - Use this option to have spam related activity written to the Antispam log. When the mail server receives a SPAM message, information about this is written into the log providing details such as the Time/Date, Sender, Recipient, Subject, SPAM Score, Reason and Action. This is useful when you need to track down what SPAM messages were received when and what action was taken.
- **Log Greylisting activity** - Enable this option if you want to have Greylisting related activity written into the Greylisting log. It provides information such as Time/Date, HELO Domain, IP address, Sender, Recipient, Action, etc.
- **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, set the Minimum logging verbosity to **Diagnostic records** in the **Tools > Log files > Minimum logging verbosity** setting.

  **Note:** These logs can be found in the MailServer folder. The path depends on the operating system, for Windows 2008 R2 it is `C:\ProgramData\ESET\ESET Mail Security\MailServer`.

### 4.5 Performance

In this section, you can improve program performance by defining a folder to store temporary files in. If no folder is specified, ESET Mail Security 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 IBM Lotus Domino 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.

### 4.6 Antivirus and antispyware settings

You can enable antivirus and antispyware mail server protection by selecting the check box next to **Enable antivirus and antispyware server protection**. **ThreatSense engine parameters setup** is accessible by clicking **Setup...**.

**Enable Antivirus and antispyware protection** - Enable/disable all antivirus and antispyware modules. Disabling this protection does not disable the antispam module and the user-defined rules, the rules are applied on every level.

  **NOTE:** Antivirus and antispyware protection is turned on automatically after every restart of the service/computer.

#### 4.6.1 IBM Lotus Domino

IBM Lotus Domino antivirus and antispyware protection allows you to enable, disable or adjust the settings of all antivirus and antispyware modules for both mail and database protection.

**Scan OLE objects** - If this option is selected, the antivirus protection will scan OLE (Object linking and embedding) objects/documents.

#### 4.6.1.1 Mail

Main settings for the antivirus and antispyware protection for both internet and internal mail. Monitoring and protection of mail communication is enabled by default.

**SMTP**

- **Enable antivirus and antispyware protection of SMTP** - Enables the monitoring and protection of all communication from the SMTP. Selected by default.

  **Action to take if cleaning not possible:** If the cleaning of an infected message is not possible, you can choose between three actions:

    - **Retain message** - No action is taken and the message is left untouched (info texts can still be appended).
    - **Quarantine message** - Sends the message to the quarantine (`eQuarantine.nsf` by default).
    - **Delete message** - Deletes the message completely.

  **Note:** Cleaning an infected message can cause the attachment to be deleted.

**Internal Mail (NRPC)**

- **Enable antivirus and antispyware protection of internal mail** - Enables the monitoring and protection of all communication from the NRPC. Selected by default.

  **Action to take if cleaning not possible:** If the cleaning of an infected file (attachment) is not possible, you can choose between four actions:

    - **Retain message** - No action is taken and the message is left untouched (info texts can still be appended).
**Quarantine message** - Sends the message to the quarantine (eQuarantine.nsf by default).

**Delete infected object** - Deletes only the infected object and leaves the message. This does not apply for rfc messages - they can only be deleted completely.

**Replace infected object with text file** - You can choose to replace the infected object with information about the infection (and the action taken) in the message body. This does not apply for rfc messages - they can only be deleted completely.

**Delete message** - Deletes the message completely.

**Write data to document header to prevent duplicate scanning of messages designated for multiple recipients** - Once the message is scanned on the server level (and the proper action is taken), information about this scan will be written to the document header. This is especially useful for messages designated for multiple recipients because it ensures that the same message is not scanned every time it is retrieved by a client. This information will be removed once the message is delivered.

**NOTE**: For outgoing email (to the Internet), the NRPC settings apply.

**NOTE**: Encrypted mail and documents are not scanned.

### 4.6.1.2 Database

Settings for database protection. The monitoring of database communication (reading/writing) is enabled by default.

- **Enable protection** - Notes are monitored and scanned for possible threats (enabled by default). The user-defined rules are still active.

- **Action to take if cleaning not possible** - If the cleaning of an infected note is not possible, you can choose between four actions:
  - **Retain note** - No action is taken and the note is left untouched (info texts can still be appended).
  - **Quarantine note** - Sends the note to the quarantine (eQuarantine.nsf by default).
  - **Delete infected object** - Deletes only the infected object from the note. This does not apply to rfc notes - they can only be deleted completely.
  - **Replace infected object with text file** - You can choose to replace the infected object with information about the infection (and the action taken) in the note. This does not apply to rfc notes - they can only be deleted completely.
  - **Delete note** - The whole note is deleted.

- **Scan on read** - Files are scanned when they are retrieved from the database.

- **Scan on write** - Files are scanned when they are written to the database.

**Note**: When you disable these options (Scan on read/write), the EMSL Plugin will be unregistered from all Database actions, which means that the Antivirus module and the User-defined rules are disabled.

- **Prevent repeated scanning** - Once the note has been scanned, it will not be scanned again until ESET Mail Security is updated with a new virus signature database or a rule change.

- **Max file size limit**: Maximum size limit for files that will be processed by ESET Mail Security.

- **Excluded databases from scan** - Databases that are completely excluded from scanning by antivirus and antispyware modules and user-defined rules. Be careful about which databases you exclude because exclusions represent a potential security risk. By default, the server databases Names.nsf, Admin4.nsf and Log.nsf are excluded. You can add excluded databases manually by typing them into the edit box separated with a comma (,), for example: mail\admin.nsf,help\test.nsf.

**NOTE**: Encrypted mail and documents are not scanned.
4.6.2 Actions

Choose actions that are performed after the scan by the antivirus and antispyware modules:

**Write ID to the header of scanned messages** - Information about the scan (virus signature database, actions performed, etc.) will be written to the header of a scanned message. This option applies to all messages, but only to infected notes (except the retain action).

**Write information about taken action to the header of scanned messages** - Information about the scan result (virus name or clean state) will be written to the header of a scanned message. This option applies to all messages, but only to infected notes.

4.6.3 Alerts and notifications

Apart from the actions performed after a scan, you can choose whether you want to append info texts to the body of messages and notes (if they have a body).

**Add to the body of scanned messages:**
- **Do not append to messages** - Text that includes scan results will not be appended to messages.
- **Append to infected messages only** - Text that includes scan results will only be appended to infected messages.
- **Append to all scanned messages** - Text that includes scan results will be appended to scanned messages that arrived through the server mailbox (i.e., mail)

If enabled, text that includes scan results will be added to the end of each message. However, you can also select the **Add note to the subject of infected messages** option. If selected, a template will be added to the subject of the infected message so they can be easily filtered. You can also select the template in the field below or leave the default value - [virus %VIRUSNAME%].

**NOTE:** If a note is infected, both options (Append to infected messages only and Append to all scanned messages) are applied (except the retain action).

**NOTE:** Signed mail and documents are scanned, but the info texts are not written to the body - only to the header. This is in order to keep the integrity of the signature. However, if the mail or document contains an infiltration, the proper action is taken (clean, delete, etc) and it is possible that the signature will be changed.

4.6.4 Automatic exclusions

The Automatic exclusions lists contains files excluded from scanning based on best practices and developer standards. 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 Mail Security 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 excluded from scanning (by default) by selecting the appropriate check box included in scanning or by deselecting it with the following results:

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 want to make sure the 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 want to remove or modify some of the standard exclusions. If you want to remove exclusions from the list without restarting the server, you will need to remove them manually (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.
Most of the **Automatic exclusions** of server applications/operating systems are selected based on Microsoft's recommendations. For details, please visit this [link](#).

**NOTE**: IBM Lotus Domino temporary folders are excluded by default. However, some IBM Lotus Domino tasks and templates use non-standard temp folders and they may be reported by the real time file system protection before ESET Mail Security performs an action. If you are experiencing such issues, we recommend that you exclude these folders manually. Following IBM Lotus Domino server folders configured in the `notes.ini` file are excluded automatically: `Directory`, `VIEW_REBUILD_DIR`, `TransLog_Path`.

### 4.7 Antispam protection

In the **Antispam protection** section, you can enable or disable spam protection for the installed mail server, configure antispam engine parameters and set other levels of protection.

**NOTE**: It is necessary that the Antispam database is regularly updated in order for the Antispam module to provide the best possible protection. To successfully allow regular updates to the Antispam database, you will need to make sure that ESET Mail Security has access to particular IP addresses on particular ports. For further information on what IP's and ports to enable on your third-party firewall, read this [KB article](#).

**NOTE**: Also, a mirror cannot be used for Antispam database updates. For the Antispam database updates to properly function, ESET Mail Security needs to have access to IP addresses listed in the above mentioned KB article. Without access to these IP's, the Antispam module will not be able to provide most accurate results, thus the most accurate results.

#### 4.7.1 IBM Lotus Domino antispam protection

Antispam protection for messages that are handled by the IBM Lotus Domino server.

**Action to take on spam messages** - Select the action that is taken when a spam message is recognized:

- **Retain message** - No action is taken and the message is left untouched (info texts can still be appended).
- **Quarantine message** - Sends the message to the quarantine (`eQuarantine.nsf` by default).
- **Delete message** - Deletes the message completely.

**Write spam score to the header of scanned messages** - Writes the spam score assigned by the antispam module to the header of each scanned message.

**Use Lotus Domino server whitelists to automatically bypass antispam protection** - Whitelist(s) defined by the administrator are automatically checked when the IBM Lotus Domino starts (and every hour since) and data defined in these whitelists (IP addresses or hostnames) are excluded from scanning by the antispam module and greylisting.

**Enable Greylisting** activates a feature that protects users from spam using the following technique: The ESET Mail Security plug-in will send a “temporarily reject” SMTP return value (default is 451/4.7.1) for any received email that is not from a recognized sender. A legitimate server will try to resend the message after a delay. Spam servers typically don’t attempt to resend the message, as they usually go through thousands of email addresses and do not waste time resending. Greylisting is an additional layer of antispam protection and does not have any effect on the spam evaluation capabilities of the antispam module.

When evaluating the message source the method takes into account the configurations of the **Approved IP addresses** list and the **Ignored IP addresses** list.

The **SMTP response for temporarily denied connections** field defines the SMTP temporary denial response sent to the SMTP server if a message is refused.

Example of SMTP response message:

<table>
<thead>
<tr>
<th>Primary response code</th>
<th>Complementary status code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>451</td>
<td>4.7.1</td>
<td>Please try again later</td>
</tr>
</tbody>
</table>

**Warning**: Incorrect syntax in SMTP response codes may lead to the malfunction of greylisting protection. As a result, spam messages may be delivered to clients or messages may not be delivered at all.

**Time limit for the initial connection denial (min.)** - When a message is delivered for the first time and temporarily refused, this parameter defines the time period during which the message will always be refused (measured from the first refusal). After the defined time period has elapsed, the message will be successfully received. The minimum value you can enter is 1 minute.
**Unverified connections expiration time (hours)** – This parameter defines the minimum time interval for which triplet data will be stored. A valid server must resend a desired message before this period expires. This value must be greater than the value of **Time limit for the initial connection denial**.

**Verified connections expiration time (days)** – The minimum number of days for which triplet information is stored, during which emails from a particular sender will be received without any delay. This value must be greater than the value of **Unverified connections expiration time**.

**NOTE:** You can also use system variables when defining the SMTP reject response.

### 4.7.2 Antispam engine

After clicking **Setup**, a window will open where you can configure the **Antispam engine parameters**.

The ESET Mail Security Antispam engine assigns a spam score from 0 to 100 to every scanned message. By changing the limits of spam scores in this section, you can influence whether the message will be classified as SPAM (depends on the SPAM score), if the message will be recorded to the antispam log and what data is included in the antispam statistics.

#### 4.7.2.1 Antispam engine parameter setup

##### 4.7.2.1.1 Analysis

In this section, you can configure how messages are analysed for SPAM and subsequently processed.

- **Scan message attachments** - This option lets you choose whether the antispam engine will scan and consider attachments when computing the spam score.

- **Use both MIME sections** - The antispam engine will analyze both text/plain and text/html MIME sections in a message. If additional performance is desired, it is possible to only analyze one section. If this option is unchecked (disabled), then only one section will be analyzed.

- **Memory size for score calculation (in bytes)** - This option instructs the antispam engine not to read more than a configurable number of bytes from the message buffer when processing rules.

- **Memory size for sample calculation (in bytes)** - This option instructs the antispam engine not to read more than the defined bytes when computing the message fingerprint. This is useful for getting consistent fingerprints.

- **Use LegitRepute cache memory** - Enables usage of a LegitRepute cache to reduce false positives especially for newsletters.

- **Convert to UNICODE** - Improves accuracy and throughput for email message bodies in Unicode especially double-byte languages by converting the message into single-bytes.

- **Use domain cache memory** - Enables usage of a domain reputation cache. If enabled, domains are extracted from messages and compared against a domain reputation cache.

##### 4.7.2.1.1.1 Samples

- **Use cache memory** - Enables usage of a fingerprint cache (Enabled by default).

- **Turn on MSF** - Allows for use of an alternate fingerprinting algorithm known as MSF. When enabled, you will be able to set following limits and thresholds:

  - **Number of messages designating a bulk message** - This option specifies how many similar messages are required in order to consider a message bulk.

  - **Frequency of clearing cache memory** - This option specifies an internal variable which determines how frequently the in-memory MSF cache is pruned.

  - **Two samples match sensitivity** - This option specifies the match percentage threshold for two fingerprints. If the match percentage is higher than this threshold then messages are considered to be the same.

  - **Number of samples stored in memory** - This option specifies the number of MSF fingerprints to keep in memory. The higher the number, the more memory is used but also the higher the accuracy.
4.7.2.1.1 SpamCompiler

**Turn on SpamCompiler** - Speeds up rules processing but requires a little bit more memory.

**Prefered version** - Specifies what SpamCompiler version to use. When set to **Automatic**, the antispam engine will choose the best engine to use.

**Use cache memory** - If this option is enabled, SpamCompiler will store the compiled data on disk instead of memory in order to reduce memory usage.

**List of cache memory files** - This option specifies which rules files are compiled on disk instead of memory.

Set rule files indexes which will be stored in cache memory on disk. To manage rule file indexes you can:

- Add...
- Edit..
- Remove

**NOTE**: Only numbers are acceptable characters.

4.7.2.1.2 Training

**Use training for message fingerprint score** - Enables fingerprint score offset training.

**Use training words** - This option controls whether Bayesian Word Token analysis is used. Accuracy can be greatly improved but more memory is used and it is slightly slower.

- **Number of words in cache memory** - This option specifies the number of word tokens to cache at any time. The higher the number, the more memory is used but also the higher the accuracy. To enter the number, enable option **Use training words** first.

**Use training database only for reading** - This option controls whether the word, rules, and fingerprint training databases can be modified or are read-only after the initial load. A read-only training database is faster.

- **Automatic training sensitivity** - Sets a threshold for auto-training. If a message is scored at or above the high threshold, that message is considered a definite spam and is then used to train all the enabled Bayesian modules (rules and/or word) but not sender or fingerprint. If a message is scored at or below the low threshold, that message is considered a definite ham and is then used to train all the enabled Bayesian modules (rules and/or word) but not sender or fingerprint. To enter the high and low threshold number, enable option **Use training database only for reading** first.

**Minimum amount of training data** - Initially, only the rule weights are used to compute the spam score. Once a minimum set of training data is achieved, rule/word training data replaces the rule weights. The default minimum is 100 which means that it must be trained on at least 100 equivalent known ham messages and 100 equivalent spam messages for a total of 200 messages before the training data replaces the rule weights. If the number is too low then the accuracy could be poor due to insufficient data. If the number is too high, then the training data will not be fully taken advantage of. A value of 0 will cause rule weights to always be ignored.

**Use only training data** - Controls whether to give full weight to training data. If this option is enabled then scoring will be based solely on training data. If this option is disabled (unchecked) then both rules and training data will be used.

**Number of scanned messages before writing them to disk** - While training, the antispam engine will process a configurable amount of messages before writing the training database to disk. This option determines how many messages to process before writing to disk. For maximum performance, this number should be as large as possible. In an unusual case when a program is unexpectedly terminated before buffer has been written to disk, the training performed since the last disk write will be lost. The buffer is written to disk on normal termination.

**Use country data for training** - Controls whether country routing information should be considered when training and scoring messages.
4.7.2.1.3 Rules

Use rules - This option controls whether slower heuristic rules are used. Accuracy can be greatly improved but more memory is used and it is much slower.

- Use rule set extension - Enables the extended rule set.
- Use second rule set extension - Enables the second extension to rule set.

Rule weight: - This option allows overriding weights associated with individual rules.

List of downloaded rule files: - This option specifies which rule files are downloaded.

Category weight: - Allows the end user to adjust the weights of categories used in sc18 and in files used in custom rules list. Category: Name of category, currently limited to SPAM, PHISH, BOUNCE, ADULT, FRAUD, BLANK, FORWARD and REPLY. This field is case insensitive. Score: Any integer or BLOCK or APPROVE. The weight of rules matching the corresponding category will be multiplied by the scaling factor to produce a new effective weight.

Custom rules list: - Allows user to specify a custom list of rules (i.e. spam, ham, or phishing words/phrases). Custom rules files contain phrases in the following format on separate lines: phrase, type, confidence, caseSensitivity phrase can be any text except commas. Any commas in the phrase should be deleted. type can be either SPAM, PHISH, BOUNCE, ADULT, or FRAUD. If anything other than those are specified, the TYPE is automatically assumed to be SPAM. Confidence can be from 1 to 100. If type is SPAM, then 100 indicates a higher confidence of spamminess. If type is PHISH, then 100 indicates a higher confidence of phishiness. If type is BOUNCE, then 100 indicates a higher confidence that phrase is related to bounces. A higher confidence is more likely to impact the final score. A value of 100 is a special case. If type is SPAM, then 100 will score the message as 100. If type is PHISH, then 100 will score the message as 100. If type is BOUNCE, then 100 will score the message as 100. As always, any whitelist overrides any blacklist. caseSensitivity value of 1 means that the phrase will be case sensitive; 0 means that the phrase will be case insensitive. Examples:

spamming is fun, SPAM, 100,0
phishing is Phun, PHISH, 90,1
return to sender, BOUNCE, 80,0

The first line means that all variations of “spamming is fun” are considered as SPAM with a confidence of 100. The phrase is case insensitive. The second line means that all variations of “phishing is phun” are considered as PHISH with a confidence 90. The phrase is case sensitive. The third line means that all variations of “return to sender” are considered as BOUNCE with a confidence 80. The phrase is case insensitive.

Clear older rules after their update - The antispam engine, by default, will clean up older rule files from the configuration directory when a new file is retrieved from the SpamCatcher network. However, some users of the antispam engine will want to archive older rule files. This can be done by disabling this cleanup feature.

Show notification after successful update of rules -

4.7.2.1.3.1 Rule weight

Set rule file indexes and their weight. To add a rule weight, press Add... button. To modify existing, press Edit... button. To delete, press Remove button. Specify Index: and Weight: values.

4.7.2.1.3.2 List of downloaded rule files

Set rule file indexes which should be downloaded to disk. Use Add, Edit and Remove buttons to manage rule file indexes.
4.7.2.1.3.3 Category weight
Set rule categories and their weight. Use Add..., Edit... and Remove button to manage categories and their weight.

To add a category weight select a Category: from list. Available are:

- SPAM
- Phishing
- Non-delivery report
- Mature content messages
- Fraudulent messages
- Empty messages
- Forwarding messages
- Replying messages

Then select an action:

- Allow
- Block
- Weight:

4.7.2.1.3.4 Custom rules list
Select the list of files containing custom rules which will be used for message analysis. Browse for a text file (*.txt). Use Add, Edit and Remove buttons to manage custom rules list.

4.7.2.1.4 Filtering
In this section, you can configure allowed, blocked and ignored lists by specifying criteria such as IP address or range, domain name, email address, etc. To add, modify or remove criteria, simply navigate to the list you want to manage and click on the appropriate button to do so.

4.7.2.1.4.1 Allowed senders
Whitelisted senders and domains can contain an email address or a domain. Addresses are entered in the format "mailbox@domain" and domains simply in the format "domain".

NOTE: Leading and trailing white space is ignored, regular expressions are not supported and asterisk "*" is ignored as well.

4.7.2.1.4.2 Blocked senders
Blacklisted senders and domains can contain an email address or a domain. Addresses are entered in the format "mailbox@domain" and domains simply in the format "domain".

NOTE: Leading and trailing white space is ignored, regular expressions are not supported and asterisk "*" is ignored as well.

4.7.2.1.4.3 Allowed IP addresses
This option allows you to specify IP's which should be approved. Ranges can be specified in three ways:

a) starting IP - ending IP
b) IP address and network mask
c) IP address

If the first non-ignored IP in Received: headers match any in this list then message is scored a 0 and no other checks are made.
4.7.2.1.4.4 Ignored IP addresses
This option allows you to specify IP's which should be ignored when doing RBL checks. The following are always implicitly ignored:

10.0.0.0/8, 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0

Ranges can be specified in three ways:

a) starting IP - ending IP
b) IP address and network mask
c) IP address

4.7.2.1.4.5 Blocked IP addresses
This option allows you to specify IP's which should be blocked. Ranges can be specified in three ways:

a) starting IP - ending IP
b) IP address and network mask
c) IP address

If any IP addresses in Received: headers match any in this list then message is scored a 100 and no other checks are made.

4.7.2.1.4.6 Allowed domains
This option allows you to specify body domains and IP's which should should always be approved.

4.7.2.1.4.7 Ignored domains
This option allows you to specify body domains which should always be excluded from the DNSBL checks and ignored.

4.7.2.1.4.8 Blocked domains
This option allows you to specify body domains and IP's which should should always be blocked.

4.7.2.1.4.9 Spoofed senders
Allows blocking spammers who spoof your domain name and other domain names. For example, spammers often use the recipient's domain name as the From: domain name. This list allows you to specify which mail servers are allowed to use which domain names in the From: address.

4.7.2.1.5 Verification
Verification is an additional feature of Antispam protection. It allows for messages being verified by the means of external servers according to defined criteria. Choose a list from the setup tree to configure its criteria. The lists are following:

- RBL (Realtime Blackhole List)
- LBL (Last Blackhole List)
- DNSBL (DNS Blocklist)

4.7.2.1.5.1 RBL (Realtime Blackhole List)

RBL servers: - Specifies a list of Realtime Blackhole List (RBL) servers to query when analyzing messages. Please refer to the RBL section in this document for further information.

RBL verification sensitivity: - Since RBL checks can introduce latency and a decrease in performance, this option allows running RBLs check conditionally based on the score prior to RBL checks. If score is greater than the "high" value then only those RBL servers which can bring score below "high" value are queried. If score is less than the "low" value then only those RBL servers which can bring score above "low" value are queried. If score is between "low" and "high" then all RBL servers are queried.

RBL request execution limit (in seconds): - This option allows setting a maximum timeout for finishing all RBL queries. RBL responses are only used from those RBL servers which responded in time. If value is "0" then no timeout is enforced.
Maximum number of verified addresses against RBL: - This option allows limiting how many IP addresses are queried against the RBL server. Note that the total number of RBL queries will be the number of IP addresses in the Received: headers (up to a maximum of RBL maxcheck IP addresses) multiplied by the number of RBL servers specified in RBL list. If the value is "0" then unlimited number of received headers are checked. Note that IP's which match against the ignored IP list option do not count towards the RBL IP addresses limit.

To manage the list, use Add..., Edit... or Remove buttons.

The list consists of three columns:

Address
Response
Score

4.7.2.1.5.2 LBL (Last Blackhole List)

LBL servers: - The Last Connecting IP is queried against the LBL server. You can specify a different DNS lookup for the last connecting incoming IP. For the last connecting incoming IP, the LBL list is queried instead of RBL list. Otherwise, the RBL list options such as RBL threshold are also applied to the LBL list.

IP addresses not verified against LBL: - If the Last Connecting IP matches with an IP on the list, then that IP is queried against the RBL server(s) instead of the LBL server(s).

To manage the list, use Add..., Edit... or Remove buttons.

The list consists of three columns:

Address
Response
Score

Here, you can specify IP addresses which will not be verified against LBL. To manage the list, use Add..., Edit... or Remove buttons.

4.7.2.1.5.3 DNSBL (DNS Block List)

DNSBL servers: - Specifies a list of DNS Blocklist (DNSBL) servers to query with domains and IP's extracted from the message body.

DNSBL verification sensitivity: - If score is greater than the "high" value then only those DNSBL servers which can bring score below "high" value are queried. If score is less than the "low" value then only those DNSBL servers which can bring score above "low" value are queried. If score is between "low" and "high" then all DNSBL servers are queried.

DNSBL request execution limit (in seconds): - Allows setting a maximum timeout for finishing all DNSBL queries.

Maximum number of verified domains against DNSBL: - Allows limiting how many domains and IP's are queried against the DNS Blocklist server.

To manage the list, use Add..., Edit... or Remove buttons.

The list consists of three columns:

Address
Response
Score

4.7.2.1.6 DNS

Use cache memory - Enable internal caching of DNS requests.

Number of DNS requests stored in memory: - Limits the number of entries in internal DNS cache.

Save cache memory to disk - If enabled, DNS cache will store entries on disk on shutdown and read from disk on initialization.

DNS server address: - DNS servers can now be explicitly specified to override the default.

Direct DNS access: - When set to yes and if DNS server is not specified, then the antispam engine will make LiveFeed requests directly to the LiveFeed servers. This option is ignored if DNS server is specified as it has precedence. This option should be set to Yes when direct queries are more efficient than the default DNS servers.
DNS request lifetime (in seconds): - This option allows setting a minimum TTL for entries in the antispam engine's internal DNS cache. The option is specified in seconds. For those DNS responses whose TTL value is less than specified minimum TTL, the antispam engine's internal cache will use specified TTL instead of the TTL value of the DNS response.

4.7.2.1.7 Score

Turn on score history - Enables tracking of historical scores for repeat senders.

Stop analysis when SPAM score threshold has been reached - This option allows you to tell the antispam engine to stop analyzing the message once a score has been reached. This can reduce the number of rules and other checks that are performed, thus improving throughput.

Use accelerated analysis before threshold score for a clean message has been reached - This option allows you to tell the antispam engine to skip slow rule checks if the message is likely to be ham.

Message categorization

- **Score value from which a message is regarded as SPAM**: Antispam engine assigns scanned message a score from 0 to 100. Setting the score value borders affects what messages are considered as SPAM and what messages aren't. If you set incorrect values, it may decrease quality of the antispam engine's detection results.

- **Score value which sets a border when a message is regarded as probable SPAM or probably clean**: Antispam engine assigns scanned message a score from 0 to 100. Setting the score value borders affects what messages are considered as SPAM and what messages aren't. If you set incorrect values, it may decrease quality of the antispam engine's detection results.

- **Score value up to which a message is regarded as certainly clean**: Antispam engine assigns scanned message a score from 0 to 100. Setting the score value borders affects what messages are considered as SPAM and what messages aren't. If you set incorrect values, it may decrease quality of the antispam engine's detection results.

4.7.2.1.8 Spambait

Spam addresses: - If the RCPT TO: address from SMTP envelope matches an email address in this list, then the statistics file will record tokens in email message as being sent to a spambait address. Addresses must match exactly ignoring case, wildcard entries are not supported.

Addresses regarded as nonexistent: - If the RCPT TO: address from SMTP envelope matches an email address in this list, then the statistics file will record tokens in email message as being sent to a nonexistent address. Addresses must match exactly ignoring case, wildcard entries are not supported.

4.7.2.1.8.1 Spambait addresses

You can set email addresses which will only receive SPAM. To add an email address, type it in a standard format and press **Add** button. To modify existing email address, use **Edit** button. To delete, press **Remove** button.

4.7.2.1.8.2 Addresses regarded as nonexistent

You can set email addresses which will appear as nonexistent to the outside. To add an email address, type it in a standard format and press **Add** button. To modify existing email address, use **Edit** button. To delete, press **Remove** button.

4.7.2.1.9 Communication

Single SpamLabs request duration (in seconds): - Limit how long single request to the Antispam protection SpamLabs can take. The value is specified in units of integral seconds. The value of "0" disables this feature and no limit will be placed.

Use v.4x protocol: - Communicate with the Antispam protection SpamLabs to determine scoring via old slower v4.x protocol. When you set this option to **Automatically**, it allows Antispam engine to automatically use the netcheck feature as a fallback to LiveFeed queries.

- **Range of v4.x protocol usage**: Since networks can introduce latency and a decrease in performance, this option allows running network checks conditionally based on the score. Network is only queried if score is at or between the "low" and "high" range specified via this option.

LiveFeed server address: - Specifies which server to query for LiveFeed requests.
**LiveFeed request lifetime (in seconds):** - This option allows setting a minimum TTL for entries in the antispam engine's internal LiveFeed cache. The option is specified in seconds. For those LiveFeed responses whose TTL value is less than specified minimum TTL, the antispam engine's internal cache will use specified TTL instead of the TTL value of the LiveFeed response.

**Proxy server authentication type:** - Specifies what type of a HTTP proxy authentication should be used.

### 4.7.2.1.10 Performance

**Maximum size of the used thread stack:** - Sets the maximum thread stack size to use. If the thread stack size is set to 64KB, then this variable should be set to 100 or less. If the thread stack size is set to greater than 1MB, then this variable should be set to 10000 or less. If this variable is set below 200, accuracy can be reduced by a couple of percentages.

**Required throughput (in messages per second):** - This option allows you to specify the desired throughput in messages per second. The antispam engine will attempt to reach that level by optimizing the rules that are run. It is possible that accuracy may be reduced. A value of 0 disables the option.

**Join incremental files into one** - The antispam engine, by default, will merge multiple incr files and a full file into a single updated full file. This is done to reduce file clutter in the configuration directory.

**Download only incremental files** - The antispam engine, by default, will attempt to download the most size efficient combination of full and incr file. The antispam engine can be forced to only download incr file by setting this option to yes.

**Maximum size of incremental files:** - In order to reduce cpu usage while rule files are updated, the on-disk cache files (sc*.tmp) are no longer regenerated on every single rule update. Instead they are regenerated when there is a newer sc*.bin.full file or when the sum of the sc*.bin.incr grows beyond the number of bytes specified in maximum size of incremental files.

**Temporary files location:** - This parameter controls where the antispam engine will create temporary files.

### 4.7.2.1.11 Regional settings

**List of home languages:** - This option permits you to set languages which are preferred in your email messages. The country codes are two character ISO-639 language codes.

**List of home countries:** - This option allows specifying a list of countries which are considered "home" countries. Messages routed through a country which is not on this list will be scored more aggressively. If this option is empty then no penalty will occur.

**List of blocked countries:** - Allows blocking by country. If an IP address in a received header matches a listed country the email will be considered as SPAM. The country codes aren't applied to sender addresses. Note that it is possible for a message to have traveled through various countries before reaching the final destination. Also, this option is only 98% accurate so blocking countries can result in false positives.

**List of blocked charsets:** - Allows blocking by character-set. Default SPAM score value is set to 100, but you can adjust it for each blocked char-set separately. Note that language to char-set mapping is not 100% accurate so blocking char-sets can result in false positives.

#### 4.7.2.1.11.1 List of home languages

Set languages which you consider as home languages and in which you prefer to receive messages. To add a home language, select it from the **Language codes** column and press **Add** button. This will move the language to the "Home" languages column. To remove the language from "Home" languages column, select its code and press **Remove** button.

**Block non-home languages:** - This option controls whether or not languages, which are not listed in the "Home" column, will be blocked. There are three options:

- **Yes**
- **No**
- **Automatically**

List of language codes (based on ISO 639):

- Afrikaans: af
- Amharic: am
- Arabic: ar
- Byelorussian: be
<table>
<thead>
<tr>
<th>Language</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgarian</td>
<td>bg</td>
</tr>
<tr>
<td>Catalan</td>
<td>ca</td>
</tr>
<tr>
<td>Czech</td>
<td>cs</td>
</tr>
<tr>
<td>Welsh</td>
<td>cy</td>
</tr>
<tr>
<td>Danish</td>
<td>da</td>
</tr>
<tr>
<td>German</td>
<td>de</td>
</tr>
<tr>
<td>Greek</td>
<td>el</td>
</tr>
<tr>
<td>English</td>
<td>en</td>
</tr>
<tr>
<td>Esperanto</td>
<td>eo</td>
</tr>
<tr>
<td>Spanish</td>
<td>es</td>
</tr>
<tr>
<td>Estonian</td>
<td>et</td>
</tr>
<tr>
<td>Basque</td>
<td>eu</td>
</tr>
<tr>
<td>Persian</td>
<td>fa</td>
</tr>
<tr>
<td>Finnish</td>
<td>fi</td>
</tr>
<tr>
<td>French</td>
<td>fr</td>
</tr>
<tr>
<td>Frisian</td>
<td>fy</td>
</tr>
<tr>
<td>Irish</td>
<td>ga</td>
</tr>
<tr>
<td>Gaelic</td>
<td>gd</td>
</tr>
<tr>
<td>Hebrew</td>
<td>he</td>
</tr>
<tr>
<td>Hindi</td>
<td>hi</td>
</tr>
<tr>
<td>Croatian</td>
<td>hr</td>
</tr>
<tr>
<td>Hungarian</td>
<td>hu</td>
</tr>
<tr>
<td>Armenian</td>
<td>hy</td>
</tr>
<tr>
<td>Indonesian</td>
<td>id</td>
</tr>
<tr>
<td>Icelandic</td>
<td>is</td>
</tr>
<tr>
<td>Italian</td>
<td>it</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja</td>
</tr>
<tr>
<td>Georgian</td>
<td>ka</td>
</tr>
<tr>
<td>Korean</td>
<td>ko</td>
</tr>
<tr>
<td>Latin</td>
<td>la</td>
</tr>
<tr>
<td>Lithuanian</td>
<td>lt</td>
</tr>
<tr>
<td>Latvian</td>
<td>lv</td>
</tr>
<tr>
<td>Marathi</td>
<td>mr</td>
</tr>
<tr>
<td>Malay</td>
<td>ms</td>
</tr>
<tr>
<td>Nepali</td>
<td>ne</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl</td>
</tr>
<tr>
<td>Norwegian</td>
<td>no</td>
</tr>
<tr>
<td>Polish</td>
<td>pl</td>
</tr>
<tr>
<td>Portuguese</td>
<td>pt</td>
</tr>
<tr>
<td>Quechua</td>
<td>qu</td>
</tr>
<tr>
<td>Rhaeto-Romance</td>
<td>rm</td>
</tr>
<tr>
<td>Romanian</td>
<td>ro</td>
</tr>
<tr>
<td>Russian</td>
<td>ru</td>
</tr>
<tr>
<td>Sanskrit</td>
<td>sa</td>
</tr>
<tr>
<td>Scots</td>
<td>sco</td>
</tr>
<tr>
<td>Slovak</td>
<td>sk</td>
</tr>
<tr>
<td>Slovenian</td>
<td>sl</td>
</tr>
<tr>
<td>Albanian</td>
<td>sq</td>
</tr>
<tr>
<td>Serbian</td>
<td>sr</td>
</tr>
<tr>
<td>Swedish</td>
<td>sv</td>
</tr>
<tr>
<td>Swahili</td>
<td>sw</td>
</tr>
<tr>
<td>Tamil</td>
<td>ta</td>
</tr>
<tr>
<td>Thai</td>
<td>th</td>
</tr>
<tr>
<td>Tagalog</td>
<td>tl</td>
</tr>
<tr>
<td>Turkish</td>
<td>tr</td>
</tr>
<tr>
<td>Ukrainian</td>
<td>uk</td>
</tr>
<tr>
<td>Vietnamese</td>
<td>vi</td>
</tr>
<tr>
<td>Yiddish</td>
<td>yi</td>
</tr>
<tr>
<td>Chinese</td>
<td>zh</td>
</tr>
</tbody>
</table>
4.7.2.1.11.2 List of home countries

Set countries which you consider as home countries and from which you prefer to receive messages. To add a home country, select it from the **Country code**: column and press **Add** button. This will move the country to the **Home countries** column. To remove the country from **Home countries** column, select the country code and press **Remove** button.

List of country codes (based on ISO 3166):

<table>
<thead>
<tr>
<th>Country code</th>
<th>Country name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>AFGHANISTAN</td>
</tr>
<tr>
<td>AX</td>
<td>ÅLAND ISLANDS</td>
</tr>
<tr>
<td>AL</td>
<td>ALBANIA</td>
</tr>
<tr>
<td>DZ</td>
<td>ALGERIA</td>
</tr>
<tr>
<td>AS</td>
<td>AMERICAN SAMOA</td>
</tr>
<tr>
<td>AD</td>
<td>ANDORRA</td>
</tr>
<tr>
<td>AO</td>
<td>ANGOLA</td>
</tr>
<tr>
<td>AI</td>
<td>ANGUILLA</td>
</tr>
<tr>
<td>AQ</td>
<td>ANTARCTICA</td>
</tr>
<tr>
<td>AG</td>
<td>ANTIGUA AND BARBUDA</td>
</tr>
<tr>
<td>AR</td>
<td>ARGENTINA</td>
</tr>
<tr>
<td>AM</td>
<td>ARMENIA</td>
</tr>
<tr>
<td>AW</td>
<td>ARUBA</td>
</tr>
<tr>
<td>AU</td>
<td>AUSTRALIA</td>
</tr>
<tr>
<td>AT</td>
<td>AUSTRIA</td>
</tr>
<tr>
<td>AZ</td>
<td>AZERBAIJAN</td>
</tr>
<tr>
<td>BS</td>
<td>BAHAMAS</td>
</tr>
<tr>
<td>BH</td>
<td>BAHRAIN</td>
</tr>
<tr>
<td>BD</td>
<td>BANGLADESH</td>
</tr>
<tr>
<td>BB</td>
<td>BARBADOS</td>
</tr>
<tr>
<td>BY</td>
<td>BELARUS</td>
</tr>
<tr>
<td>BE</td>
<td>BELGIUM</td>
</tr>
<tr>
<td>BZ</td>
<td>BELIZE</td>
</tr>
<tr>
<td>BJ</td>
<td>BENIN</td>
</tr>
<tr>
<td>BM</td>
<td>BERMUDA</td>
</tr>
<tr>
<td>BT</td>
<td>BHUTAN</td>
</tr>
<tr>
<td>BO</td>
<td>BOLIVIA</td>
</tr>
<tr>
<td>BA</td>
<td>BOSNIA AND HERZEGOVINA</td>
</tr>
<tr>
<td>BW</td>
<td>BOTSWANA</td>
</tr>
<tr>
<td>BV</td>
<td>BOUVEY ISLAND</td>
</tr>
<tr>
<td>BR</td>
<td>BRAZIL</td>
</tr>
<tr>
<td>IO</td>
<td>BRITISH INDIAN OCEAN TERRITORY</td>
</tr>
<tr>
<td>BN</td>
<td>BRUNEI DARUSSALAM</td>
</tr>
<tr>
<td>BG</td>
<td>BULGARIA</td>
</tr>
<tr>
<td>BF</td>
<td>BURKINA FASO</td>
</tr>
<tr>
<td>BI</td>
<td>BURUNDI</td>
</tr>
<tr>
<td>KH</td>
<td>CAMBODIA</td>
</tr>
<tr>
<td>CM</td>
<td>CAMEROON</td>
</tr>
<tr>
<td>CA</td>
<td>CANADA</td>
</tr>
<tr>
<td>CV</td>
<td>CAPE VERDE</td>
</tr>
<tr>
<td>KY</td>
<td>CAYMAN ISLANDS</td>
</tr>
<tr>
<td>CF</td>
<td>CENTRAL AFRICAN REPUBLIC</td>
</tr>
<tr>
<td>TD</td>
<td>CHAD</td>
</tr>
<tr>
<td>CL</td>
<td>CHILE</td>
</tr>
<tr>
<td>CN</td>
<td>CHINA</td>
</tr>
<tr>
<td>CX</td>
<td>CHRISTMAS ISLAND</td>
</tr>
<tr>
<td>CC</td>
<td>Cocos (Keeling) Islands</td>
</tr>
<tr>
<td>CO</td>
<td>COLOMBIA</td>
</tr>
<tr>
<td>KM</td>
<td>COMOROS</td>
</tr>
<tr>
<td>CG</td>
<td>CONGO</td>
</tr>
<tr>
<td>CD</td>
<td>CONGO, THE DEMOCRATIC REPUBLIC OF</td>
</tr>
<tr>
<td>CK</td>
<td>THE</td>
</tr>
<tr>
<td>CR</td>
<td>COSTA RICA</td>
</tr>
<tr>
<td>CI</td>
<td>CÔTE D'IVOIRE</td>
</tr>
<tr>
<td>HR</td>
<td>CROATIA</td>
</tr>
<tr>
<td>CU</td>
<td>CUBA</td>
</tr>
<tr>
<td>CY</td>
<td>CYPRUS</td>
</tr>
<tr>
<td>CZ</td>
<td>CZECH REPUBLIC</td>
</tr>
<tr>
<td>Country</td>
<td>Code</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>MACAO</td>
<td>MO</td>
</tr>
<tr>
<td>MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF</td>
<td>MK</td>
</tr>
<tr>
<td>MADAGASCAR</td>
<td>MG</td>
</tr>
<tr>
<td>MALAWI</td>
<td>MW</td>
</tr>
<tr>
<td>MALAYSIA</td>
<td>MY</td>
</tr>
<tr>
<td>MALDIVES</td>
<td>MV</td>
</tr>
<tr>
<td>MALI</td>
<td>ML</td>
</tr>
<tr>
<td>MALTA</td>
<td>MT</td>
</tr>
<tr>
<td>MARSHALL ISLANDS</td>
<td>MH</td>
</tr>
<tr>
<td>MARTINIQUE</td>
<td>MQ</td>
</tr>
<tr>
<td>MAURITANIA</td>
<td>MR</td>
</tr>
<tr>
<td>MAURITIUS</td>
<td>MU</td>
</tr>
<tr>
<td>MAYOTTE</td>
<td>YT</td>
</tr>
<tr>
<td>MEXICO</td>
<td>MX</td>
</tr>
<tr>
<td>MICRONESIA, FEDERATED STATES OF</td>
<td>FM</td>
</tr>
<tr>
<td>MOLDOVA, REPUBLIC OF</td>
<td>MD</td>
</tr>
<tr>
<td>MONACO</td>
<td>MC</td>
</tr>
<tr>
<td>MONGOLIA</td>
<td>MN</td>
</tr>
<tr>
<td>MONTSERRAT</td>
<td>MS</td>
</tr>
<tr>
<td>MOROCCO</td>
<td>MA</td>
</tr>
<tr>
<td>MOZAMBIQUE</td>
<td>MZ</td>
</tr>
<tr>
<td>MYANMAR</td>
<td>MM</td>
</tr>
<tr>
<td>NAMIBIA</td>
<td>NA</td>
</tr>
<tr>
<td>NAURU</td>
<td>NR</td>
</tr>
<tr>
<td>NEPAL</td>
<td>NP</td>
</tr>
<tr>
<td>NETHERLANDS</td>
<td>NL</td>
</tr>
<tr>
<td>NETHERLANDS ANTILLES</td>
<td>AN</td>
</tr>
<tr>
<td>NEW CALEDONIA</td>
<td>NC</td>
</tr>
<tr>
<td>NEW ZEALAND</td>
<td>NZ</td>
</tr>
<tr>
<td>NICARAGUA</td>
<td>NI</td>
</tr>
<tr>
<td>NIGER</td>
<td>NE</td>
</tr>
<tr>
<td>NIGERIA</td>
<td>NG</td>
</tr>
<tr>
<td>NIUE</td>
<td>NU</td>
</tr>
<tr>
<td>NORFOLK ISLAND</td>
<td>NF</td>
</tr>
<tr>
<td>NORTHERN MARIANA ISLANDS</td>
<td>MP</td>
</tr>
<tr>
<td>NORWAY</td>
<td>NO</td>
</tr>
<tr>
<td>OMAN</td>
<td>OM</td>
</tr>
<tr>
<td>PAKISTAN</td>
<td>PK</td>
</tr>
<tr>
<td>PALAU</td>
<td>PW</td>
</tr>
<tr>
<td>PALESTINIAN TERRITORY, OCCUPIED</td>
<td>PS</td>
</tr>
<tr>
<td>PANAMA</td>
<td>PA</td>
</tr>
<tr>
<td>PAPUA NEW GUINEA</td>
<td>PG</td>
</tr>
<tr>
<td>PARAGUAY</td>
<td>PY</td>
</tr>
<tr>
<td>PERU</td>
<td>PE</td>
</tr>
<tr>
<td>PHILIPPINES</td>
<td>PH</td>
</tr>
<tr>
<td>PITCAIRN</td>
<td>PN</td>
</tr>
<tr>
<td>POLAND</td>
<td>PL</td>
</tr>
<tr>
<td>PORTUGAL</td>
<td>PT</td>
</tr>
<tr>
<td>PUERTO RICO</td>
<td>PR</td>
</tr>
<tr>
<td>QATAR</td>
<td>QA</td>
</tr>
<tr>
<td>RÉUNION</td>
<td>RE</td>
</tr>
<tr>
<td>ROMANIA</td>
<td>RO</td>
</tr>
<tr>
<td>RUSSIAN FEDERATION</td>
<td>RU</td>
</tr>
<tr>
<td>RWANDA</td>
<td>RW</td>
</tr>
<tr>
<td>SAINT HELENA</td>
<td>SH</td>
</tr>
<tr>
<td>SAINT KITTS AND NEVIS</td>
<td>KN</td>
</tr>
<tr>
<td>SAINT LUCIA</td>
<td>LC</td>
</tr>
<tr>
<td>SAINT PIERRE AND MIQUELON</td>
<td>PM</td>
</tr>
<tr>
<td>SAINT VINCENT AND THE GRENADINES</td>
<td>VC</td>
</tr>
<tr>
<td>SAMOA</td>
<td>WS</td>
</tr>
<tr>
<td>SAN MARINO</td>
<td>SM</td>
</tr>
<tr>
<td>SAO TOME AND PRINCIPE</td>
<td>ST</td>
</tr>
<tr>
<td>SAUDI ARABIA</td>
<td>SA</td>
</tr>
<tr>
<td>SENEGAL</td>
<td>SN</td>
</tr>
<tr>
<td>SERBIA AND MONTENEGRO</td>
<td>CS</td>
</tr>
<tr>
<td>SEYCHELLES</td>
<td>SC</td>
</tr>
<tr>
<td>SIERRA LEONE</td>
<td>SL</td>
</tr>
</tbody>
</table>
**4.7.2.1.11.3 List of blocked countries**

Set countries which you want to block and from which you do not want to receive messages. To add a country to Blocked countries: list, select it from the Country code: column and press Add button. To remove the country from Blocked countries: list, select the country code and press Remove button.

For list of specific country codes see List of home countries topic.
4.7.2.1.11.4 List of blocked charsets

Set the char-sets you want to block. Messages in these char-sets will not be received. To add a char-set, select it from the Charsets: column and press Add button. This will move the char-set to the Blocked charsets: column. To remove the char-set from Blocked charsets: column, select the char-set code and press Remove button.

While adding a char-set to blocked char-sets, you can specify your own value for SPAM score for this particular char-set. Default is 100. You can define score for each char-set separately.

4.7.2.1.12 Log files

Turn on detailed logging - Enables increased verbose logging.

Output rerouting files: - Redirects log output file to the directory specified in this field. Press ... button to browse for directory instead of typing it manually.

4.7.2.1.13 Statistics

Turn on statistical data logging - Logs IP's, Domains, URL's, suspicious words, etc. to the conf file system. Logs can be automatically uploaded to antispam engine's analysis servers. The logs can be converted to plain text for viewing.

• Send statistical data for analysis - Launches a thread to automatically upload statistics files to antispam engine's analysis servers.

• Analysis server address: - URL where statistics files will be uploaded.

4.7.2.1.14 Options

Automatic configuration: - Sets options based on user-inputted system, performance, and resource requirements.

Create configuration file - Creates antispam.cfg file which contains antispam engine configuration. It can be found in C:\ProgramData\ESET\ESET Mail Security\ServerAntispam (Windows Server 2008) or C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam (Windows Server 2000 and 2003).

4.7.3 Alerts and notifications

You can choose to add an info text to the subject of a recognized SPAM message, so they can be easily sorted.

Add note to the subject of spam messages - By default, this option is enabled and a note is added to the subject of messages recognized as spam messages. This way, you can easily sort out the spam messages.

Select a Template added to the subject of spam messages by writing into the field below, or leave the default text as [SPAM].

4.8 FAQ

Q: After installing ESET Mail Security with Antispam, emails stopped being delivered into mailboxes.

A: If Greylisting is enabled, this is normal behavior. In the first hours of full operation emails may arrive with several hours of delay. If the issue continues for a longer period, we recommend you turn off (or reconfigure) Greylisting.

Q: How long can the list of file types be in one rule?

A: The file extensions list can contain a maximum of 255 characters in a single rule.

Q: Why did the rule counter increase by more than one after receiving a single message?

A: The rules are checked against a message when it is delivered to the server mail.box. When the message is scanned again, the rule counter may increase by 2 or more. The rule can be applied for the message body and the message attachment. Furthermore, rules can be applied during a database scan (e.g., repeated mailbox-store scan after a virus signature database update), which can increase the rule counter.

Q: Can I define the level of spam score the message has to attain to be classified as SPAM?

A: Yes you can set this limit in ESET Mail Security (see the Antispam engine chapter).
5. Computer protection

While providing protection for IBM Lotus Domino, ESET Mail Security has all of the necessary tools to ensure protection of the server itself (resident shield, web-access protection, email client protection and antispam).

This section describes the Main menu of the product (the chapters are sorted accordingly) and the Advanced setup tree with sections related to the main menu.

5.1 Program menu

In the main program menu, some of the most important setup options and features are available. This menu is located in the upper right corner of the main window.

Program menu items available:

- **User interface**
  - Reset window layout – Resizes program windows to the default size and position.

- **Setup**
  - Username and Password setup... - Lets you insert/change your authentication data for ESET Mail Security.
  - Proxy server setup - Enables you to configure a proxy server if it is used to connect to the Internet.
  - Antivirus and antispyware - Displays the Setup window for the Antivirus and antispyware module.
  - Antispam protection - Displays the Setup window for the Antispam module.
  - Import/export settings - Enables you to import/export the configuration of ESET Mail Security from/to a file.
  - Advanced setup... - Opens the advanced setup options dialog window enabling you to configure ESET Mail Security.

- **Tools**
  - Log files, Quarantine, Scheduler/Planner and SysInspector - Opens dialog windows related to the given tool in ESET Mail Security.
  - Submit file for analysis... – Opens a dialog window enabling you to submit suspicious files for analysis to ESET's virus labs.

  **NOTE:** File size limit for submitted files is 3 Mb.

- **Help**
  - The menu contains options available in the ESET Mail Security interactive help pages. It also includes links to the company's web page, Virus encyclopedia, Virus radar and to the technical support query form.

5.2 Protection status

Protection status informs you about the security and current protection level of your computer.

The status window also shows the total number of blocked attacks, as well as information about the installed version of the virus signature database. The information about the program's expiration date can also be found here.

**Protection status:**

The green Protection status icon indicates that maximum protection is ensured.

The red icon signals critical problems – maximum protection of your computer is not ensured. Possible reasons are:

- Real-time file system protection is disabled
- Product license is expired

The yellow icon indicates that the antispam protection is disabled, that there is a problem with updating (outdated virus signature database, cannot update), or that the license is nearing its expiration date.
Antivirus protection is disabled - This problem is signaled by a red display and a red exclamation point next to the Antivirus and antispyware item. You can re-enable antivirus protection by clicking Enable real-time file system protection or Start all antivirus and antispyware protection modules.

Antispam protection disabled - This problem is signaled by a red exclamation point next to the Antispam protection item. You can re-enable the antispam protection by clicking Enable in Setup > Antispam module.

License is almost expired - This is indicated by the protection status icon turning yellow and displaying an exclamation point. After the license expires the program will not be able to update and the protection status icon will turn red. We recommend following the instructions in the alert window to renew your license.

5.2.1 Watch activity

1. To see current File system activity in graph form, click Protection status > Watch activity. At the bottom of the graph is a timeline that records File system activity in real time based on the selected time span.

2. From the Activity drop-down menu you can also select to view Mail server protection performance. The graph display and options for File system activity and Mail server protection performance are the same except that the latter displays average performance (red) and current performance (blue).

To change the time span click Toggle view. The following options are available:

- **Step 1 second (last 10 minutes)** - The graph refreshes every second and the timeline covers the last 10 minutes.
- **Step 1 minute (last 24 hours)** - The graph is refreshed every minute and the timeline covers the last 24 hours.
- **Step 1 hour (last month)** - The graph is refreshed every hour and the timeline covers the last month.
- **Step 1 hour (selected month)** - The graph is refreshed every hour and the timeline covers the last X selected months.

The vertical axis of the File system activity graph represents read data (red) and written data (blue). Both values are given in kilobytes. If you mouse over either read data or written data in the legend below the graph, the graph will only display data for that activity type.

5.2.2 Statistics

To view a graph of statistical data related to ESET Mail Security's protection modules, click Protection status > Statistics. Select the desired protection module from the Statistics drop-down menu to see the corresponding graph and legend. If you mouse over an item in the legend, only the data for that item will display on the graph.

The following statistical graphs are available:

- **Antivirus and Antispyware protection** - Displays the number of infected and cleaned objects.
- **Real-time file system protection** - Only displays objects that were read or written to the file system.
- **Email client protection** - Only displays objects that were sent or received by email clients.
- **Web access protection** - Only displays objects downloaded by web browsers.
- **Mail server protection** - Displays antivirus and antispyware mail server statistics.
- **Mail server antispam protection** - Displays the entire history of antispam statistics.
- **Mail server protection activity** - Displays objects verified_blocked/deleted by the mail server.
- **Mail server protection performance** - Displays data scanned on the SMTP, NRPC and database level.
- **Mail server greylisting protection** - Includes antispam statistics generated by the Greylisting method.

The antispam server protection - details - The Antispam engine parameter settings can influence to what category of the antispam statistics will a specific message be added.

The Not scanned category is comprised of:

**General** - All messages that were scanned while the antispam protection has been disabled on any layer.
5.3 Database scan

If you suspect that a file in your database is infected, run an On-demand database scan to examine your databases for infiltrations. From a security point of view, it is essential that database 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 on-access scanner when they were saved to the database. This can happen if the on-access scanner was disabled at the time of infection (excluded databases), or if the virus signature database is not up-to-date. Database action settings are applied to scanned notes and documents.

Click Custom scan... to configure a custom database scan.

Information about the last scan is displayed in the lower part of the main window.

Note: The On-demand scan is performed by the LMON_SCANNER task that was copied into the IBM Lotus Domino folder during the installation. The On-demand scan can also be operated from the Domino console. Enter tell LMON_SCANNER help for all supported commands.

5.3.1 On-demand database scan

You can select the databases you want to scan in this section. Click on your server in the Scan targets list to display every database on this server. Select the checkbox next to a database to include this database in the scan.

Scan excluded databases - Includes excluded databases in the scan. Excluded databases can be configured and reviewed here.

Setup - You can create a customized scan profile to fit your needs. See the ThreatSense engine parameters setup section for a description of each parameter and instructions on how to select specific Scan targets.

Save - Save the specific configuration and click OK to close this window and run the scan immediately.

5.4 Computer scan

If you suspect that your computer is infected, or it is exhibiting abnormal behavior, 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.

Click Smart scan to run a computer scan immediately. You can start a New scan, track the progress of the scan(s) below - in the Running scans section, or open a scan in a New window.

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.

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... or click Scan setup... in the Computer scan part of the main window and then On-demand computer scan > Profiles... The Configuration profiles window has a drop-down menu containing all 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 for a description of each parameter of the scan setup and select specific Scan targets.

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 Add.... 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.
5.4.1 Computer scan - Window

The scan progress window shows the current status of the scan and information about the number of files found to contain malicious code.

Note: It is normal that some files, such as password protected files or files exclusively being used by the system (typically pagefile.sys and certain log files), cannot be scanned.

**Scan progress** - The progress bar shows the percentage of already-scanned objects compared to objects still to be scanned. The value is derived from the whole number of objects included in scanning.

**Target** - The name of the currently scanned object.

**Number of threats** - Shows the total number of threats found so far during the scan.

**Scroll scan log** - If enabled, the scan log will scroll down automatically as new entries are added so that most recent entries are visible.

- **Pause** - Pauses the scan.
- **Stop** - Terminates the scan.
- **To background** - Moves the scan to the background. A list of scans currently in progress is available in the Computer scan section in the main program menu where you can bring them to the foreground at a later time, if necessary.

5.4.2 Scan targets

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

- **Scan profile** - Choose a profile to be used for scanning chosen targets.

- **Scan targets** - Select from the following options:
  - By profile settings - uses targets specified in the selected profile
  - Removable media - selects all removable media
  - Local drives - selects all local drives
  - Network drives - selects all mapped network drives
  - No selection - cancels selection of targets

Select the check boxes in the tree structure corresponding to the objects you wish to scan.

The editable line under the folder tree structure serves to quickly move to the selected target within the folder tree structure, or to directly add the desired target. Adding a scan target directly is only possible if there is no selection performed in the folder tree structure (by default there is no selection).

- **Scan without cleaning** - Infected items are not cleaned automatically. Scanning without cleaning serves to obtain an overview of the current protection status. Information about scanning is saved to a scan log.

- **Setup...** - Click this button to set up the scanner in detail. The available options are described in **Scanner setup**.

- **Save** - Saves changes made in selection of targets, including selections made within the folder tree structure.

5.4.2.1 Scan Setup

Select additional scan settings for the **ThreatSense engine parameters setup**.

- **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** - With Smart Optimization enabled the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods each, applying them to specific file types. The Smart Optimization is not rigidly defined within the product. Quite on the contrary, the ESET Development Team keeps
it flexible implementing new changes continuosly which get then integrated into the ESET security solution via the regular updates. Is the Smart Optimization disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

**Preserve last access timestamp** - Check 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. For more information, see the section describing finished scans.

### 5.4.2.1.1 Scan completed successfully

Scan results are displayed after the scan has been performed. If the scan has been moved to background, the scan results are displayed in a standalone window. The following information is included:

- Time required for the scan.
- Number of all scanned objects.
- Number of infected objects found during the scan.
- Number of successfully cleaned objects.

### 5.4.3 Scan setup

This section provides options for selecting scanning parameters.

**Selected profile** - A particular set of parameters used by the On-demand scanner. To create a new one, click Profiles.... You can choose between an In-depth scan, a Context menu scan or a Smart scan.

**On-demand scanner setup for selected profile**

**ThreatSense engine parameter setup** - Click Setup... to set the options for the currently active profile.

**Scan targets** - Click Setup... to Select scan targets.

### 5.4.3.1 Select scan targets

The Select scan targets setup allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations.

The Scan targets drop-down menu allows you to select predefined scan targets:

- **By profile settings** - Targets specified in the selected profile
- **Removable media** - All removable media
- **Local drives** - All local drives
- **Network drives** - All mapped network drives
- **No selection** - Cancels target selection

Select the check boxes next to the objects you wish to scan.

To quickly navigate to a scan target or to directly add a desired target, enter it into the blank field below the folder list. This is only possible if no objects have been selected in the folder list.

### 5.4.4 Command line

ESET Mail Security'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
– quar-dir = FOLDER
– aind

**Targets:**
- files
- no-files
- boots
- no-boots
- arch
- no-arch
- max-archive-level = LEVEL
- scan-timeout = LIMIT
- max-arch-size=SIZE
- mail
- no-mail
- sfx
- no-sfx
- rtp
- no-rtp
- exclude = FOLDER
- subdir
- no-subdir
- max-subdir-level = LEVEL
- symlink
- no-symlink
- ext-remove = EXTENSIONS
- ext-exclude = EXTENSIONS

**Methods:**
- adware
- no-adware
- unsafe
- no-unsafe
- unwanted
- no-unwanted
- pattern
- no-pattern
- heur

load modules from FOLDER
quarantine FOLDER
show activity indicator
scan files (default)
do not scan files
scan boot sectors (default)
do not scan boot sectors
scan archives (default)
do not scan archives
maximum archive nesting LEVEL
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.
scan only the first SIZE bytes in archives (default 0 = unlimited)
scan email files
do not scan email files
scan self-extracting archives
do not scan self-extracting archives
scan runtime packers
do not scan runtime packers
exclude FOLDER from scanning
scan subfolders (default)
do not scan subfolders
maximum subfolder nesting LEVEL (default 0 = unlimited)
follow symbolic links (default)
skip symbolic links
exclude EXTENSIONS delimited by colon from scanning
scan for Adware/Spyware/Riskware
do not scan for Adware/Spyware/Riskware
scan for potentially unsafe applications
do not scan for potentially unsafe applications
scan for potentially unwanted applications
do not scan for potentially unwanted applications
use signatures
do not use signatures
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.

5.5 Updating the program

Regular updating of ESET Mail Security 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.

To open the Update setup, click F5 (Advanced Setup) > Update.

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 Mail Security.
5.5.1 Update
This section contains important information about program updates. ESET Mail Security system updates are critical to maintaining maximum security. The Update module ensures that the program is always up to date in two ways - by updating the virus signature database and updating system components.

**Update virus signature database** - Click to update the virus signature database immediately.

The main Update window shows the current update status. It is important that this section always displays **Update is not necessary - the virus signature database is current**. If this is not the case, the program is out of date, which increases the risk of infection. Please update the virus signature database as soon as possible.

**Username and Password setup** - Opens a window that allows you to enter authentication data. Authentication data (username and password) is sent to your email address after purchase or registration.

**Last successful update** - The date of the last update. It should refer to a recent date, which means that the virus signature database is current.

**Version of virus signature database** - The virus signature database number, which is also an active link to ESET's website listing all signatures added within the given update.

Register... Use this link to register with ESET and receive your authentication data. This button will only be visible if the username and password are not entered correctly and verified.

**Update process**
After clicking **Update virus signature database**, the download process begins. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Abort**.

5.5.1.1 Username and Password setup
In order for the program to download updates and thus keep the system protected against newly emerging threats, a valid username and password must be entered. The username and password was delivered to you after purchase or activation of a serial number.

**NOTE**: Enter the username and password carefully as you received them. Both are case sensitive. In order to ensure correct transcription, we recommend copying and pasting the data from the registration email for maximum accuracy.

5.5.1.2 Operating system updates
The **System updates** window shows the list of available updates ready to be downloaded and installed. Information about new operating system updates is also shown in the **Protection status** section in the main window. The update priority level is shown next to the name of the update. You can modify the **Operating system update - settings**.

Click **Run system update** to start downloading and installing operating system updates (if available).

5.5.1.2.1 Update information
Information about Windows updates. The name and number of the update are displayed at the top of the window followed by the priority and a description of the problem solved by the update.

5.5.1.2.2 Operating system update - settings
The Windows update feature is an important component for protecting users from malicious software. For this reason, it is vital to install Microsoft Windows updates as soon as they become available. ESET Mail Security notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates** - No system updates will be offered for download.
- **Optional updates** - Updates marked as optional and higher will be offered for download.
- **Recommended updates** - Updates marked as recommended and higher will be offered for download.
- **Important updates** - Updates marked as important and higher will be offered for download.
- **Critical updates** - Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server.
Therefore, the system update information may not be immediately available after saving changes.

5.5.2 Update setup

The options in this window enable you to define the program's behavior during updates, or immediately after that. For updates to be downloaded properly, it is essential to correctly fill in all parameters. If you use a firewall, please make sure that the program is allowed to communicate with the Internet (i.e. http communication).

Selected profile - The currently used update profile. Click Profiles... to create a new profile.

Update server - The Update server is a location where updates are stored. If you use an ESET server, please leave the default option Choose automatically selected. When using a local HTTP server – also known as the Mirror - the update server should be set as follows: http://computer_name_or_its_IP_address:2221.

Username, Password - These are your authentication data.

Access to ESET update servers (i.e. the option Choose automatically in the Update Server field is selected) is subject to verification of a valid username and password.

When using a local Mirror server, the verification depends on its configuration. By default, no verification is required, i.e. the Username and Password fields are left empty.

Click the Setup button next to Advanced update setup to display a window containing advanced update options.

In the case of problems with update, click the Clear... button to flush the folder with temporary update files.

Do not display notification about successful update - Turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full screen application or a game is running.

5.5.2.1 Update mode

The program enables you to predefine its behavior if a new program component update is available.

Program component update

The program component update brings new features, or makes changes to those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a restart may be required.

- **Never update program components** - Program component updates will not be performed at all. This option is suitable for server installations, since servers are usually only restarted when they are undergoing maintenance.

- **Always update program components** - A program component update will be downloaded and installed automatically. Please remember that a computer restart may be required.

- **Ask before downloading program components** - If there is a new program component update available, the program will display a dialog window allowing you to download it.

**Restart after program component upgrade** - To provide proper functionality of the program following program component updates, the system must be restarted.

- **Never restart computer** - You will not be asked to restart, even if it is required. Please note that this is not recommended since your computer might not work properly until the next restart.

- **Offer computer restart if necessary** - After a program component update, a dialog window will appear, prompting you to restart your computer.

- **If necessary, restart computer without notifying** - After a program component update, your computer will be restarted (if required).

**Ask before downloading update** - Select this option to display a notification when a new update is available.

**Ask if an update file is greater than** - If the update file size is greater than the specified value, the program will display a notification.

**Enable test mode** - If enabled, beta-modules will be downloaded during the update that allow the user to test new features of the product. You can find a list of current modules in Help > About.
5.5.2.2 HTTP Proxy

This section should be filled in if your computer is connected to the Internet via a proxy server. The settings are taken from Internet Explorer during program installation, but if they are subsequently changed (for example if you change your ISP), please check that the HTTP proxy settings are correct in this window, otherwise the program will not be able to connect to the update servers.

**Use global proxy server settings** - If checked, the program will use data entered in the global setup tab.

**Do not use proxy server** - No proxy server is used for connecting to the Internet.

**Connection through a proxy server** - Check this box if your computer uses a proxy server to connect to the Internet.

**Proxy server, Port** - Enter the address and port of the proxy server you use.

**Username, password** - These are your authentication data to access the proxy server. Fill in these fields only if a username and password are required. Please note that these fields are not for your password/username for ESET Mail Security, and should only be supplied if you know you need a password to access the internet via a proxy server.

5.5.2.3 LAN connection setup

For updating from a local Windows NT-based server, authentication is required for updated computers. If the local system account is not granted access to the mirror server directory (where the updates are stored), it is necessary to specify the account used by the program to access the local update server.

**System account (default)** - The program will use the system account for authentication. Normally, the authentication should work. If you experience problems, it is recommended to use a specified user.

**Current user** - The program will use the account of the currently logged in user for authentication. In this case, updates will not be possible at times when there is no user logged in, because the program will not be able to establish connection to the server.

**Specified user** - The program will use the account of the specified user for authentication. Use this method when the system account connection failed. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

**Disconnect from server after update** - Select this option if connection to the server remains active even after updates have been downloaded.

5.5.2.4 Mirror

In situations where there are many workstations in a LAN environment, creating a mirror server can prevent potential network traffic overloads. Update files are downloaded centrally to the local mirror server and then distributed to all workstations, instead of being repeatedly downloaded by each workstation.

Following options are available:

**Create update mirror** - Select this checkbox to have the mirror module copy update files.

**Provide update files via the internal HTTP server** - If enabled, update files can simply be accessed through HTTP. Click Advanced setup to configure extended mirror options.

**Folder to store mirrored files** - Click to browse and locate the destination folder.

**Username, Password** - If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the Username and Password specified must have write privileges for the selected folder.

If the option **Provide update files via the internal HTTP server** is selected, no username and password will be required.

The list of Available versions shows all language versions that are currently supported by the mirror server configured by the user.
5.5.2.4.1 Advanced setup

The Advanced setup window contains complementary options for distributing update files via the HTTP protocol and for specifying the LAN access mode. The following options are available:

**HTTP Server:**
Provides copies of update files for client computers via the HTTP protocol. For the server to work properly, the mirror folder should be located on the same server where ERA server is running. On client computers, in the section Setup > Update > Update server, insert a new server in the form `http://server_name:2221` (provided the port 2221 is set). For authentication to the mirror folder, use username and password of an account created on the windows server from where you download updates.

**Server port** - Here you can specify the HTTP port number for the mirror server providing program updates for workstations.

**Authentication** - By default, no authentication to the HTTP server is required (the value NONE). Select BASIC to use base64 encoding with basic username and password authentication. The NTLM value utilizes the capabilities of the Microsoft authentication protocol NTLM. Authentication usernames and passwords correspond to existing users on the system with the mirror feature activated.

**Connect to the update server as** - Select the (user) identity to be applied by the module creating the update files within the LAN.

- **System account (default)** - The program will use the system account for authentication. Normally, the authentication should work. If you experience problems, it is recommended to use a specified user.
- **Current user** - The program will use the account of the currently logged in user for authentication. In this case, updates will not be possible at times when there is no user logged in, because the program will not be able to establish connection to the server.
- **Specified user** - The program will use the account of the specified user for authentication. Use this method when the system account connection failed. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

**Disconnect from server after update**
Select this option to provide termination of the update connection, so that it will not remain active. If not enabled, connections are terminated by the operating system.

**Program components**

- **Never update program components** - If you select this option, program components will not be updated on the target machines which are updating from the mirror, only virus signature database will get updated. Even though the program components will still be downloaded, they will not be applied to the mirror.
- **Upgrade components** - When you press this button, the program component updates (PCU) will be applied to the mirror. With next virus signature database update the target machines, which are updating from the mirror, will also get program components installed.

5.6 Setup

The ESET Mail Security setup menu allow you to adjust the protection levels of your computer and network.

The Setup menu contains the following options:

- **Antivirus and antispyware protection**
- **Antispam protection**

Click any component to adjust the behavior of the corresponding protection module:

**Configure server protection** - Clicking this option will open the ESET Mail Security - IBM Lotus Domino server protection section in the Advanced setup (F5).

**Set up Username and Password for update** - Insert/change the authentication data used to access ESET's update servers.

**Configure proxy server** - Configure a proxy server if it is used to connect to the Internet.

**Import and export settings** - Load setup parameters using an .xml configuration file, or save the current setup
parameters to a configuration file.

**Enter entire Advanced setup...** - Display Advanced setup options available in ESET Mail Security.

### 5.6.1 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.

The **Antivirus and antispyware** protection setup menu allows you to enable/disable/configure the following components:

- **Real-time file system protection** - Click **Edit exclusions** to open the Exclusion setup window, which allows you to exclude files and folders from real-time file system protection scanning.

- **Document protection**

- **Email client protection** (if enabled)

- **Mail server protection**

- **Web access protection** (if enabled)

Toggle **Enable/Disable** to activate or disable each respective type of protection. Click **Configure** to modify configuration of the module.

Click **Configure computer scan** to adjust the parameters of the **On-demand scan** (manually executed scan).

The antivirus and antispyware protection modules can also be enabled/disabled in Advanced setup (F5). In Advanced setup, navigate to **Computer protection > Antivirus and antispyware**.

#### 5.6.1.1 Antivirus and antispyware protection setup

**Enable Antivirus and antispyware protection** - Enables you to start or stop all modules.

**Enable Antistealth technology** - The Antistealth technology is a sophisticated system providing detection of dangerous programs – rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.

**Enable self-defense** - Provides protection against unauthorized deleting or disabling of ESET Mail Security or its components.

**Automatic startup file check**

**ThreatSense engine parameter setup** - Advanced setup options, e.g. file extensions you wish to control, detection methods used, etc. Click **Setup...** to open a window with the advanced virus scanner options.

**NOTE**: The antivirus and antispyware protection checks files run automatically on system startup. This scan is run on a regular basis, for more information see the chapter **Scheduler**.

#### 5.6.1.2 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.
5.6.1.2.1 Control setup

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), 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 Setup... next to ThreatSense engine parameter setup, click Other and select or deselect the checkbox next to Enable Smart optimization.

Configure the Media to scan and the Scan on (Event-triggered scanning) options for real-time file system protection.

By default, Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (e.g., if there is a conflict with another Real-time scanner), real-time protection can be terminated by deselecting the checkbox next to Start Real-time file system protection automatically option.

5.6.1.2.1.1 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.

5.6.1.2.1.2 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.

5.6.1.2.1.3 Advanced scan options

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

- Runtime packers - Toggles scanning of runtime packers.
- Self-extracting archives - Toggles scanning of self-extracting archives (SFX).
- Advanced heuristics - Turns advanced heuristics on/off. Advanced heuristics detects newly created threats before the virus signature database update is released.
- Default archive scan settings - If selected, the default archive scan parameters are used.
- Archive nesting level - Deselect default archive scan settings and specify the maximum level of scanning for archives.
- **Maximum files size** - Allows you to set the maximum file size for archives to be scanned.

**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 selecting the checkbox next to **Advanced heuristics on file execution**). Note that advanced heuristics may slow the execution of some programs due to increased system requirements.

- **Advanced heuristics on file execution** - By default, advanced heuristics is not used when files are executed. However, in some cases you may want to enable this option. Note that advanced heuristics may slow the execution of some programs due to increased system requirements.

- **Advanced heuristics on executing files from removable media** - If enabled, a scan with advanced heuristics is used when running an executable from removable media. Click **Exceptions** to define removable media for which ThreatSense engine parameters are used (advanced heuristics is disabled here by default).

Removable media can contain malicious code and put your computer at risk. ESET Mail Security provides the option to block removable media.

The **Removable media** window allows you to block and allow specific devices.

The following options are available for selected devices:

- **Block removable media** - Select this option to block removable media (The **Allowed removable media** list can only be modified if this option enabled)

- **Enable advanced heuristics on file execution** - Select this option to use advanced heuristics to scan files executed from removable media

### 5.6.1.2.2 Cleaning levels

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

- 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 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.

### 5.6.1.2.3 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 Mail Security, 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).

### 5.6.1.2.4 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](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.
5.6.1.2.5 What to do if real-time protection does not work

In the next chapter, we describe issues 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.

If real-time protection is not initiated at system startup, it is probably because the Automatic real-time file system protection startup option is disabled. To enable this option, navigate to Advanced setup (FS) 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 check box next to Start Real-time file system protection automatically 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 before installing ESET Mail Security.

**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.

5.6.1.2.6 Document protection

**Integrate into system** - Starts the document protection module and integrates it into your computer's operating system.

**Enable document protection** - Enables / disables document protection. The document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements.

To set the ThreatSense engine parameters setup for the Document protection, click Setup....

**NOTE**: This feature is activated by applications which use the Microsoft Antivirus API (e.g., Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).

5.6.1.3 Email client protection

Email protection provides control of email communication received through the POP3 protocol. Using the plug-in program for IBM Lotus Notes, ESET Mail Security 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.

**Enable email client antivirus and antispyware protection** - This option is enabled by default. Messages received by clients are scanned by the antivirus and antispyware modules and protected. You can configure additional settings by clicking Setup.... For more information, see the chapter ThreatSense engine parameters setup.

**Alerts and notifications**

**Append tag messages to received and read email**:

- **Never** - The text with the scan results information will not be appended to email.
- **To infected email only** - The text with the scan results information will only be appended to infected email.
- **To all scanned email** - The text with the scan results information will be appended to all scanned email.

**Append note to the subject of received and read infected email** - A template will be added to the subject of a received and read infected email.

**Append tag messages to sent email**:

- **Never** - The text with the scan results information will not be appended to email.
- **To infected email only** - The text with the scan results information will only be appended to infected email.
- **To all scanned email** - The text with the scan results information will be appended to all scanned email.

**Append note to the subject of sent infected email** - A template will be added to the subject of a sent infected email.

**Template added to the subject of infected email**: You can select a template that will be added to the subject of infected email. By default, it is [virus %VIRUSNAME%], where the variable %VIRUSNAME% will be replaced by the actual virus name.

### 5.6.1.3.1 POP3, POP3s

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application (in this case IBM Lotus Notes). ESET Mail Security provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. 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.

**Enable POP3 protocol checking** - If enabled, all traffic through POP3 is monitored for malicious software.

**Ports used by POP3 protocol** - A list of ports used by the POP3 protocol (110 by default).

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 select the check box next to **Enable application protocol content filtering**. See the **Protocol filtering** section for more details on filtering and configuration. This type of communication uses an encrypted channel to transfer information between server and client. ESET Mail Security checks communications utilizing the SSL (Secure Socket Layer) and TLS (Transport Layer Security) encryption methods.

#### POP3S filtering mode

- **Do not use POP3S checking** - encrypted communication will not be checked
- **Use POP3S protocol checking for selected ports** - Check this option to enable POP3S checking only for ports defined in **Ports used by POP3S protocol**.
- **Ports used by POP3S protocol** - A list of POP3S ports to check (995 by default).

### 5.6.1.3.1.1 Email clients

POP3 protocol scanning is an important part of email communication security. ESET Mail Security allows you to define which applications are used as email programs, in order to ensure that the communication stream with the email server is checked for the presence of malicious code.

The list of applications marked as email clients is accessible from the ESET Mail Security Advanced setup window (F5 key). Navigate to **Antivirus and antispyware > Email client protection > POP3, POP3S > Email clients**. In this window, ESET Mail Security displays a list of detected installed applications that can be marked by the user. In the event that the desired application is not listed, click **Add** to add it to the list.

### 5.6.1.3.1.2 Compatibility

By default, the POP3 scanner runs in maximum efficiency mode which means that all features are enabled. 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, navigate to **Antivirus and antispyware > Email protection > POP3, POP3S > Compatibility** in the Advanced setup tree.

**Maximum efficiency** - This is the default setting; it is perfectly compatible with most email clients. If a virus is detected, it is blocked by the scanner and an alert window with options to delete or rename the attachment is displayed (the options **Delete** or **Clean** must be activated, or the **Strict** or **Default** cleaning level must be enabled).

**Medium compatibility** - The scanner will work properly, but its efficiency may be limited due to compatibility. 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.

**Maximum compatibility** - If an infiltration is detected, an alert panel will pop up, but no action can be taken. 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.

### 5.6.1.4 Web access protection

Web access protection monitors the communication to and from the internet. We recommend that you leave the **Enable web access antivirus and antispyware protection** option enabled, as leaving it disabled is a security risk.

You can access the **ThreatSense engine parameters setup** by clicking **Setup**.

#### 5.6.1.4.1 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 Mail Security is configured to use the standards of most Internet browsers. However, the HTTP scanner setup options can be modified in **Advanced Setup (F5) > Computer protection > Antivirus and antispyware > Web access protection > HTTP, HTTPS**.

In the main HTTP filter window, you can select or deselect the checkbox next to **Enable HTTP checking**. You can also define the port numbers used for HTTP communication. Ports 80, 8080 and 3128 are predefined.

HTTP 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**. Port 443 is predefined.
- **Ports used by HTTPS protocol** - A list of HTTP ports to check. Port 443 is set by default.

#### 5.6.1.4.1.1 Address management

This section enables you to specify HTTP addresses to block, allow or exclude from checking. The **Add**, **Edit**, **Remove** and **Export** buttons 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.

Click **Lists** to create custom HTTP lists.

- **Allow access only to HTTP addresses in the list of allowed addresses** - If enabled, this option automatically blocks all addresses that are not included in the list of allowed addresses.
- **List active** - Select this option to apply the current list (so that the included addresses are allowed, blocked, or excluded from scanning depending on the type of the list).
- **Notify when applying address from the list** - If this option is enabled and the user visits a website present in an active list, a notification window will be displayed.
- **Add.../From file** - Allows you to add an address to the list manually (Add), or from a simple text file (From file). The From file option enables you to add multiple email addresses that are saved in a text file.
- **Edit...** - Enables you to manually edit addresses - e.g. by adding a mask ("*" and "?").
- **Remove/Remove all** - Click **Remove** to delete the selected address from the list. To delete all addresses, select **Remove all**.
- **Export...** - This option enables you to save addresses from the current list to a simple text file.

**NOTE:** 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.
This section enables you to specify lists of HTTP addresses that will be blocked, allowed or excluded from checking.

By default, the following three lists are available:

- **List of addresses excluded from filtering** - No checking for malicious code will be performed on any address added to this list.
- **List of blocked addresses/masks** - The user will not be allowed to access addresses specified in this list.
- **List of allowed addresses** - If the check box next to **Allow access only to HTTP addresses in the list of allowed addresses** is selected, the user will be allowed to access addresses specified in this list only.

Click **Add** to create a new list. To delete selected lists, click **Remove**.

Specify lists of HTTP addresses/masks that will be blocked, allowed or excluded from checking.

**Address list type**

Three list types are available:

- **List of addresses excluded from filtering** - No checking for malicious code will be performed on any address added to this list
- **List of blocked addresses/masks** - The user will not be allowed to access addresses specified in this list.
- **List of allowed addresses** - If the checkbox next to **Allow access only to HTTP addresses in the list of allowed addresses** is selected, the user will be allowed to access addresses specified in this list only.

**List name** - Specify the name of the list.

**List description** - Enter a short description for the list (optional).

### 5.6.1.4.1.2 Active mode

ESET Mail Security also contains a Web browsers feature that allows you to define whether a given application is a browser or not. If an application is marked as a browser, all communication from this application is monitored regardless of the port numbers being used.

The Web browsers feature complements the HTTP checking feature, as HTTP checking only takes place on predefined ports. However, many Internet services utilize changing or unknown port numbers. To account for this, the Web browsers feature can establish control of port communications regardless of the connection parameters.

The list of applications marked as web browsers is accessible directly from the **Web browsers** submenu of the **HTTP, HTTPs** branch in the Advanced setup tree. 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 mode by selecting the check box next to the desired application.

### 5.6.1.5 Performance

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

**NOTE**: Changes made here will be applied only after a restart.
5.6.1.6 Exclusions

This section enables you to exclude files and folders from scanning. We do not recommend that you alter these options, to ensure that all objects are scanned for threats.

There are predefined exclusions by default. These exclusions help prevent conflicts with the system files and certain applications and ensure smooth system performance. These exclusions are predefined by the Automatic exclusions functionality of ESET Mail Security. Please see the article Automatic exclusions for further details.

Path – Path to excluded files and folders.

Threat - If there is a name of a threat next to an excluded file, it means that the file is only excluded for the given threat, not completely. Therefore if that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can be used only for certain types of infiltrations and it can be created either in the threat alert window reporting the infiltration (click Show advanced options and then select Exclude from detection), or in Setup > Quarantine using the context menu option Restore and exclude from detection on the quarantined file.

Add... - Excludes objects from detection. See the chapter Add or edit exclusions for more information.

Edit... – enables you to edit selected entries. See the chapter Add or edit exclusions for more information.

Remove – removes selected entries.

Default – cancels all exclusions.

To exclude an object from scanning:

1. Select Add...
2. Enter the path to an object or select it in the tree structure below.

5.6.1.6.1 Add or edit exclusions

You can add or edit exclusions using one of the following methods:

- Enter the file path of the object you want excluded.
- Select the object you want excluded from the tree structure.

If using the first method, wildcards described in the Exclusion format section can be used.

5.6.1.6.2 Exclusion format

When configuring exclusions in the resident scanner, special symbols (wildcards such as "*" and "?" ) can be used.

Examples:
- If you wish to exclude all files in a folder, type the path to the folder and use the mask "*.*".
- If you want to exclude doc files only, use the mask "*.doc".
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say "D"), use the following format: "D?????.exe". Question marks replace the missing (unknown) characters.

5.6.1.7 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.

Enable application protocol content filtering - If enabled, all HTTP and POP3 traffic will be checked by the antivirus scanner. This feature will remain enabled only until next server restart/shutdown. If a server is restarted, application protocol filtering will not be enabled again.

If you wish to have application protocol content filtering enabled even after server reboot, you need to select the checkbox next to Start application protocol protection automatically. This will automatically enable application protocol filtering after restarting the server.
NOTE: Starting with Windows Vista Service Pack 1 and Windows Server 2008, the new Windows Filtering Platform (WFP) architecture is used to check network communication. Since WFP technology uses special monitoring techniques, the Protocol filtering section is not available.

Monitoring all communication is ensured by routing the traffic to the internal proxy server where it is scanned for threats. Routing can be enabled for:

- **HTTP and POP3 ports** - Limits routing the traffic to the internal proxy server only for HTTP and POP3 ports.
- **Applications marked as Internet browsers and email clients** - Limits routing the traffic to the internal proxy server only for the applications marked as Internet browsers and email clients.
- **Ports and applications marked as Internet browsers or email clients** - Enables routing of all traffic on HTTP and POP3 ports as well as all the communication of the applications marked as Internet browsers and email clients on the internal proxy server.

NOTE: When the Enable application protocol content filtering option is deselected (disabled), POP3 and POP3S filtering is also turned off. When you click POP3, POP3s in the Advanced setup tree, you will see that the options are not available. Once you enable protocol filtering, you will be able to configure POP3/POP3S filtering again.

### 5.6.1.7.1 Excluded applications

To exclude the communication of specific network-aware applications from content filtering, select them from the list. HTTP/POP3 communication of the selected applications will not be checked for threats. We recommend using this option only for applications that do not work properly with their communication being checked.

### 5.6.1.7.2 SSL

ESET Mail Security 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 use SSL protocol checking** - If selected, the program will not scan communications over SSL.

**Apply created exceptions based on certificates** -

**Block encrypted communication utilizing the obsolete protocol SSL v2**

### 5.6.1.7.2.1 Certificates

If a certificate cannot be verified using the Trusted Root Certification Authorities store, following actions can be taken (Protocol filtering > SSL > Certificates):

**Add the root certificate to known browsers** - For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET, spol s r.o. be added in the list of known root certificates (publishers). Select this option to automatically add the ESET root certificate to the known browsers (e.g., Opera, Firefox). For browsers using the system certification store, the certificate is added automatically (e.g., Internet Explorer). To apply the certificate to unsupported browsers, click View Certificate > Details > Copy to File... and then manually import it into the browser.

**End certificate validity**

If the certificate cannot be verified using the TRCA certificate store:

- **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.

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

The **Trusted certificates** section lists all untrusted certificates that have been reclassified as trusted by the user. ESET Mail Security will check the content of encrypted communications utilizing certificates in this list.

To delete selected items from the list, click the **Remove** button.

Click **Show** to display information about the selected certificate.

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.

To delete selected items from the list, click the **Remove** button.

Click **Show** to display information about the selected certificate.

If the computer is configured for SSL protocol scanning, a dialog window prompting you to choose an action may be opened when there is an attempt to establish an encrypted communication (using an unknown certificate). The dialog window contains the following information: name of the application that initiated the communication and name of the certificate used. If the certificate is not located in the Trusted Root Certification Authorities store, it is considered to be untrusted. The following actions are available for certificates:

**Yes** - The certificate will be temporarily marked as trusted for the current session - the alert window will not be displayed on the next attempt to use the certificate.

**Yes, always** - Marks the certificate as trusted and adds it to the list of trusted certificates - no alert windows are displayed for trusted certificates

**No** - Marks the certificate as untrusted for the current session - the alert window will be displayed on the next attempt to use the certificate.

**Exclude** - Adds the certificate to the list of excluded certificates - data transferred over the given encrypted channel will not be checked at all.

### 5.6.1.8 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**
- System startup file check
- **Email client protection**
- **Web access protection**
- **On-demand computer scan**

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.

5.6.1.8.1 Objects

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** - The program supports the following extensions: DBX (Outlook Express) and EML.
- **Archives** - The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.
- **Self-extracting archives** - Self-extracting archives (SFX) are archives needing no specialized programs - archives - to decompress themselves.
- **Runtime packers** - After executing, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner supports (thanks to emulation of code) many more types of packers.

5.6.1.8.2 Options

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

- **Heuristics** - A heuristic is an algorithm analyzing the (malicious) activity of programs. The main advantage is the ability to identify malicious software which did not exist, or was not known by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.
- **Advanced heuristics** - The advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. Thanks to the advanced heuristics, the detecting capabilities of the program are significantly higher.
- **Adware/Spyware/Riskware** - This category includes software collecting various information about users without their informed consent and also software displaying advertising material.
- **Potentially unwanted applications** - Potentially unwanted applications are not necessarily intended to be malicious, but they may affect the performance of your computer in a certain 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
- **Potentially unsafe applications** - Potentially unsafe applications is the classification used for commercial, legitimate software. It includes programs such as remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). This option is disabled by default.
5.6.1.8.3 Cleaning

This tab enables you to configure behavior of the scanner for cleaning infected files.

**No cleaning** - Infected files will not be cleaned automatically. The program will show up a warning window and allow the user to choose an action.

**Warning:**

If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode, the whole archive would be deleted where all the files it contains are infected files. In strict cleaning mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

**Default level** - 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 offers a selection of follow-up actions. The same happens if a predefined action couldn’t be completed.

**Strict cleaning** - The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is offered an action to take in a warning window.

5.6.1.8.4 Extension

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 unchecked, the list changes to show all currently scanned file extensions.

- **Scan all files** - Select this option to scan all files by default. If unchecked, the default set of extensions will be scanned (those known to contain malicious code).

- **Extension** - Typing an extension activates the Add button, which adds the new extension to the list. Click the extension in the list and then click the Remove button to delete the extension from the list.

- **Do not scan extensionless files** - This checkbox excludes scanning of files with no extension.

- **Default** - To scan the default set of extensions only, click on the Default button and confirm.

Excluding files from scanning is sometimes necessary if scanning certain file types prevents the program which is using the extensions from running properly.

5.6.1.8.5 Limits

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

**Default object settings:**

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

- **Maximum scan time for object (sec.)** - Defines the maximum time value for scanning of 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. This setting is related to archive scanning.

**Default archive scan settings:**

- **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 (bytes)** - This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If scanning of an archive is prematurely terminated for that reason, the archive will remain unchecked.
5.6.1.8.6 Other

Additional settings for the ThreatSense engine parameters setup:

- **Log all objects** - If this option is selected, the log file will show all the scanned files, even those not infected (as an example, if an infiltration is found within an archive, the log will list also clean files contained within the archive).

- **Enable Smart optimization** - With Smart Optimization enabled the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods each, applying them to specific file types. The Smart Optimization is not rigidly defined within the product. Quite on the contrary, the ESET Development Team keeps it flexible implementing new changes continuously which get then integrated into the ESET security solution via the regular updates. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

5.6.1.9 An infiltration is detected

Infiltrations can reach the system from various entry points, such as 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 Mail Security and click **Computer scan**.
- Click **Smart scan** (for more information, see section **Computer scan**).
- 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 Mail Security, suppose that an infiltration is detected by the real-time file system monitor using 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.

5.6.2 Antispam protection setup

The **Antispam protection** setup window allows you to enable/disable Email client protection and Mail server protection. Click **Configure**... to access the advanced setup options for the **antispam protection**.

**Temporarily disable antispam protection** - Temporarily deactivates both, Email client protection and Mail server protection, at the same time.
5.6.3 Proxy server

In large LAN networks, the connection of your computer to the Internet can be mediated by a proxy server. If this is the case, the following settings need to be defined. Otherwise the program will not be able to update itself automatically.

**Use proxy server** - Should be checked if your computer uses a proxy server to connect to the Internet.

**Proxy server** - Enter the IP address / name of the proxy server you use.

**Port** - Enter the port of the proxy server you use.

**Proxy server requires authentication** - If the proxy server requires authentication, these fields should be filled in with a valid username and password, granting access to the proxy server.

**Username, Password** - Please note that these fields are not for your password/username for ESET Mail Security, and should only be supplied if you know you need a password to access the Internet via a proxy server.

**Detect proxy server** - Click this button to automatically detect proxy server settings.

5.6.4 Import and Export settings

Importing and exporting configurations of ESET Mail Security are available under Setup.

Both import and export use the .xml file type. Import and export are useful if you need to backup the current configuration of ESET Mail Security 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 Mail Security on multiple systems – they can easily import an .xml file to transfer the desired settings.

Importing a configuration is very easy. From the main menu, click **Setup > Import and export settings...**, and then select **Import settings**. Enter the path of the configuration file or click ... to browse for the configuration file you wish to import.

The steps used to export a configuration are very similar. From the main menu, click **Setup > Import and export settings... > Export settings** and enter the **File name** of the configuration file (i.e. export.xml). Use the browser to select a location on your computer to save the configuration file.

5.7 Tools

The Tools menu includes modules that help simplify program administration and offer additional options for advanced users. This menu is only available in Advanced mode, and includes the following tools:

- **Log files**
- **Quarantine**
- **Scheduler**
- **SysInspector**

Submit file for analysis... - Allows you to submit a suspicious file for analysis to ESET's virus labs.

**NOTE**: File size limit for submitted files is 3 Mb.

Create Rescue CD - Launches the Rescue CD creation wizard.

5.7.1 Log files

The Log files section 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 Mail Security environment.

Antispam and greylisting protection logs (found under other logs under Tools > Log files) contain detailed information about messages that were subject to scanning and the consequent actions performed on those messages. Logs can be very useful when looking for undelivered email, trying to figure why a message was marked as spam, etc.

**Antispam** - All messages categorized by the ESET Mail Security as spam or probable spam are recorded here.
5.7.1.1 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 filtering options, only records that are relevant (according to those filtering options) are shown in the **Log files** window for easy and quick access.

To open the **Log filtering** window, click **Filter...** once in **Tools > Log files**, or press Ctrl + Shift + F on your keyboard.

**NOTE:** To search for a particular record, you can use the **Find in log** functionality instead, or in conjunction with Log filtering.

By specifying certain filtering options, only records that are relevant (according to those filtering 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 filtering options you use, the narrower the results will be.

**What:** - Enter 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 record 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** field.

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

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

Once you are finished with configuring filtering options, click on **OK** to apply the filter. The **Log files** window will show only corresponding records according to the filter options.
5.7.1.2  Find in log

In addition to Log filtering, 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 enter 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 on your keyboard.

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

What: - Enter 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 field.

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

Search up - Searches from current position upwards.

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

5.7.2  Quarantine

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

The quarantine folder is where infected or suspicious files are stored in a benign form. The resident protection module quarantines all newly created and modified suspicious files by default, but you can quarantine any file you wish.

Right-click any quarantined object in the Quarantine window to perform the following actions with the file: add, restore, restore to a new location, restore and exclude from detection, remove or submit for analysis to ESET’s laboratory.

- ESET Mail Security automatically quarantines deleted files (if you have not canceled this option in the alert window). If
desired, you can quarantine any suspicious file manually by clicking **Quarantine**... 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**... 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.

- 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 a 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 it and send the file to ESET Customer Care.

### 5.7.3 Scheduler

**Scheduler** can be found in the ESET Mail Security main menu under **Tools**. The scheduler contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used. The scheduler manages and launches scheduled tasks with predefined configuration and properties. The configuration and properties section contains information such as the date and time as well as specified profiles to be used during execution of the task. Right-click anywhere in the **Scheduler** window to perform the following actions: display detailed information, perform the task immediately, add a new task, or delete an existing task. Select/deselect the check boxes next to each entry to activate/deactivate the tasks.

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)

1. 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 **Edit**... .

2. To create a new task in **Scheduler**, click **Add**... 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.

1) Click **Add**... at the bottom of the window.

2) Select the desired task from the drop-down menu. In this case, select **Update**.

3) Enter the name of the task and select one of the following timing options:

a) **Once** - The task will be performed only once, at the predefined date and time.

b) **Repeatedly** - The task will be performed at the specified interval (in hours).

c) **Daily** - The task will run each day at the specified time.

d) **Weekly** - The task will run one or more times a week, on the selected day(s) and time.

e) **Event triggered** - The task will be performed on a specified event.

1) Depending on the timing option you select in the previous step, one of the following dialog windows will be displayed:

   - **Once** - The task will be performed at the predefined date and time.
   - **Repeatedly** - The task will be performed at the specified time interval.
   - **Daily** - The task will run repeatedly each day at the specified time.
   - **Weekly** - The task will be run on the selected day and time.
2) In case the task could not be run at the predefined time, you can specify when it will be performed again:
   - wait until the next scheduled time
   - run the task as soon as possible
   - run the task immediately if the time since the last task execution exceeds -- hours

3) In the last step you can review the task to be scheduled. Click Finish to apply the task.

A dialog window will appear allowing you to select profiles to be used for the scheduled task. Here you can specify a primary and alternate profile, which will be 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.

5.7.4 ESET Sysinspector

ESET Sysinspector is an application that thoroughly inspects your computer, gathers detailed information about system components, such as installed drivers and applications, network connections or important registry entries and assesses the risk level of each component. The information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection.

The SysInspector window displays the following information about created logs:

- **Time** - The time of log creation.
- **Comment** - A short comment.
- **User** - The name of the user who created the log.
- **Status** - The status of log creation.

The following actions are available:

- **Compare** – Compares two existing logs.
- **Create** – Creates a new log.
- **Delete** – Removes selected logs from the list.

After right-clicking one or more selected logs, the following additional options are available from the context menu:

- **Show** – Opens the selected log in SysInspector (the same as double-clicking a log).
- **Delete all** – Deletes all logs.
- **Export** – Exports the log to an xml file or zipped .xml.

5.7.4.1 Create a computer status snapshot

Enter a short comment describing the log to be created and click Add. Please wait until the ESET Sysinspector log is complete (Status is Created). Generating the log can be slowed by your hardware configuration and system data, and may take several minutes.

5.8 User interface options

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

- 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. Use this check box to toggle between ESET graphics and a standard windows layout. This field will be in the indeterminate stage (little square inside the checkbox) after the program installation. This means that this setting depends on the current configuration of the Windows High Contrast function. If High Contrast is turned on, the graphical interface of ESET Mail Security will switch over to the non-graphical mode automatically. The non-graphical mode in ESET products, as well as the High Contrast – Windows function are accessibility features designed for people who have vision impairment to enable them to work with a computer more easily.

- The **Display menu** option turns the menu display on or off in the upper panel of the program.

- If you wish to disable the ESET Mail Security splash-screen, deselect the checkbox next to Show splash-screen at startup.
• At the top of the ESET Mail Security main program window is a Standard menu which can be activated or disabled based on the Use standard menu option.

• If the checkbox next to Show tooltips is selected, 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 that 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 checkbox next to Use animated icons for progress indication. If you want the program to sound a warning if an important event takes place, select the checkbox next to Use sound signal.

The User interface features also include the option to password-protect the ESET Mail Security 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….

5.8.1 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 Mail Security.

• The first item is Display alerts. Disabling this option will disable all alert windows and is only suitable for 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 checkbox next to 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 checkbox next to Display notifications on desktop. More detailed options – notification display time and window transparency can be modified by clicking Configure notifications….

• To configure the duration of the balloon tips display time, see the option Display balloon tips in taskbar (for sec.).

• With the Display only notifications requiring user’s interaction option, you can turn on/off displaying of messages requiring user’s interaction.

• Select the check box next to Display only notifications requiring user’s interaction when running applications in full screen mode to suppress all non-interactive notifications.

Click Advanced setup... to open the alerts and notifications advanced setup window.

5.8.1.1 Advanced setup

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:

• Critical warnings – Displays all critical warning, such as error starting Antivirus protection, etc.
• Errors – Only errors messages such as “Error downloading file” and critical warnings will be displayed.
• Warnings – Displays all critical warnings, errors and warning messages.
• Diagnostic records – Displays all informative messages including successful updates and all records above.
• Diagnostic records – Displays all information needed to fine-tune the program, diagnose issues and all messages above.

The second 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 Mail Security. 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.
5.8.2 Hidden notification windows

If the Do not show this message again option was selected for any notification window (alert) which was previously displayed, that window will appear in the list of hidden notification windows. Actions that are now executed automatically are displayed in the **Confirm** column.

**Show** – Shows a preview of notification windows that are currently not displayed and for which an automatic action is configured.

**Remove** – Removes items from the Hidden messageboxes list. All notification windows removed from the list will be displayed again.

5.8.3 Access setup

In order to provide maximum security for your system, it is essential for ESET Mail Security to be correctly configured. Any unqualified change may result in a loss of important data. This option is located in the Access setup submenu under **User interface** in the Advanced setup tree. To avoid unauthorized modifications, setup parameters of ESET Mail Security can be password protected.

**Password protect settings** – Locks/unlocks the program’s setup parameters. Select or deselect the check box to open the Password setup window.

To set or change a password to protect the setup parameter, click Set password....

**Require full administrator rights for limited administrator accounts** – Select this option to prompt the current user (if he or she does not have administrator rights) to enter administrator username and password when modifying certain system parameters (similar to UAC in Windows operating systems). Protected modifications include disabling protection modules or turning off the firewall.

5.8.3.1 Password

To avoid unauthorized modification, the setup parameters of ESET Mail Security can be password protected. We recommend that you choose a strong password.

5.8.3.2 Change password

To change the password for protecting the setup parameters, click Set password, enter the old password, new password, and click **OK**.

5.8.4 Context menu

The context menu is displayed after right-clicking a selected object. The menu lists all options available to perform on the object.

It is possible to integrate the ESET Mail Security control elements into the context menu. More detailed setup options for this functionality are available in advanced options, in the **User Interface** and **Context menu** sections.

**Integrate into the context menu** - It is possible to integrate the ESET Mail Security control elements into the context menu.

**Menu type** - The following options are available in the **Menu type** drop-down menu:

- Full (scan first) - Activates all context menu options; the main menu will display the **Scan with ESET Mail Security** option.

- Full (clean first) - Activates all context menu options; the main menu will display the **Clean with ESET Mail Security** option.

- Only scan - Only the **Scan with ESET Mail Security** option will be displayed in the context menu.

- Only clean - Only the **Clean with ESET Mail Security** option will be displayed in the context menu.

**Confirmations** - Displays an additional warning when a user attempts to apply a context menu option on more objects than specified in **Ask if the number of files exceeds**... By default this option is set to eight objects.
5.9 ThreatSense.Net

Enable ThreatSense.Net Early Warning System - The ThreatSense.Net tab provides an option for enabling / disabling the Early Warning System that serves for submitting suspicious files and anonymous statistical information to ESET's labs.

Advanced Settings... - Opens a window with additional Early Warning System settings

For more information about the ThreatSense.Net Early Warning System technology, and to review ESET's privacy statement, click the hyperlink at the bottom of the pane. If you have used the ThreatSense.Net Early Warning System before and have disabled it, there still may be data packages to send. Even after deactivating this feature, such packages will be sent to ESET on the next occasion. Afterwards, no further packages will be created.

5.9.1 Suspicious files

This section allows you to adjust options for the submission of suspicious files.

Suspicious files - Here you can specify whether suspicious files are to be submitted to ESET's lab for analysis and, if so, which ones.

Never submit - Files will never be sent out for analysis. However, if ESET Mail Security is set to display an alert window when a threat is detected, by selecting the appropriate option you will be able to submit the file anyway.

Ask before submitting - Suspicious files will be collected and the program will prompt you before the files are submitted.

Submit without asking - Any suspicious files will be sent out automatically without prompting you first.

When to submit - You can decide when the packages with statistical information will be submitted to ESET. The available options are:

As soon as possible - When selected, statistical information will be submitted as soon as possible after a statistical package has been created (recommended if permanent Internet connection is available).

During update - When selected, statistical packages will be collected and uploaded during an update (recommended for dial-up users).

Exclusion filter - The files listed will never be sent to ESET's labs for analysis, even if they contain a suspicious code. It is useful to exclude files which may carry potentially confidential information, such as documents or spreadsheets. The most common file types are excluded by default.

Add - Opens a dialog window for adding a file to the exclusion list.

Edit... - Opens an edit dialog.

Remove - Removes selected extensions from the list.

Contact email (optional) - The contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. You will not get a response from ESET unless more information is required.

5.9.1.1 Exclusion

You can add a file or a whole folder to the exclusions list. Use wildcards to cover a group of files. A question mark (?) represents a single variable character whereas an asterisk (*) represents a variable string of zero or more characters. For example, if you decide to exclude *.TXT, all text files are excluded. You can also exclude a folder, for example C:\Users\Administrator\Documents\*. and all files in this folder are excluded.
5.9.2 File

If you find a suspiciously behaving file on your computer, you can submit it to ESET’s virus lab for analysis. If the file turns out to be a malicious application, its detection will be added in one of the upcoming updates.

Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/ZIP, protect the archive with the password "infected" and send it to samples@eset.com. Please remember to be informative in the subject field and enclose as much information about the file as possible (e.g., the website you downloaded it from).

**Note:** Before submitting a file to ESET, make sure it fulfills either of the following criteria: (i) the file is not detected at all (ii) the file is incorrectly detected as a threat. You will not receive a response unless further information is required for analysis.

- **File** - The name of the file you intend to submit.
- **Comment** - A short description of the file and its activity.
- **Contact email** - The contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. Entering a contact email is optional. You will not get a response from ESET unless more information is required, since each day our servers receive tens of thousands of files, which makes it impossible to reply to all submissions.
5.9.3 Statistics

The Statistics tab displays options for sending statistical information. The ThreatSense.Net Early Warning System collects anonymous information about your computer related to newly detected threats, which may include the name of the infiltration, information about the date and time it was detected, the version of ESET Mail Security, and information about your computer’s operating system version and the Location setting. The statistics are normally delivered to ESET’s server once or twice a day.

An example of a statistical package submitted:

```
# version=3
# utc_time=2010-06-07 13:07:25.073
# local_time=2010-06-07 15:07:25 (+0100, Central Europe Daylight Time)
# utc_time_from=2010-06-07 11:43:10
# utc_time_to=2010-06-07 13:07:25
# country="Slovakia"
# language="en\033"
# osver=5.1.2600 NT Service Pack 3
# engine=7255
# components=4.2.35
# ui=b41e247294e90795
# cpu_count=4,1,4
# cpu_feat=174c
# mem=c8
# hdd=2

2010-06-07 11: moduleid=1010101 virus="~OK" count=22
2010-06-07 11: moduleid=1020100 virus="~OK" count=1
2010-06-07 11: moduleid=1030200 virus="~OK" count=6
2010-06-07 12: moduleid=1010101 virus="~OK" count=127
2010-06-07 12: moduleid=1020100 virus="~OK" count=4
2010-06-07 12: moduleid=1030200 virus="~OK" count=200
2010-06-07 13: moduleid=1010101 virus="~OK" count=41
2010-06-07 13: moduleid=1020100 virus="~OK" count=1
2010-06-07 13: moduleid=1030200 virus="~OK" count=8
```

Enable submission of anonymous statistical information - Activates submission of statistical information.

You can decide when the packages with statistical information will be submitted to ESET (in the When to submit section). The available options are:

- **As soon as possible** - when selected, statistical information will be submitted as soon as possible after a statistical package has been created (recommended if permanent Internet connection is available).
- **During update** - when selected, statistical packages will be collected and uploaded during an update (recommended for dial-up users).
5.9.4 Submission

The Submission tab allows you to force the submission of files and enable logging of the data sent to ESET.

- **By means of Remote Administrator or directly to ESET** - Files will be submitted by all means available.
- **By means of Remote Administrator** - Suspicious files will be sent to ESET Remote Administrator server and consequently sent to ESET’s labs for further analysis.
- **Directly to ESET** - If checked, suspicious files will be sent directly to ESET’s lab.

**Submit now** - Clicking Submit now forces the manual submission of files that have been collected. Using ThreatSense Net technology, the program submits all files that have not yet been submitted to ESET by any other user.

**Enable logging** - If checked, submission of suspicious files and statistical packages will be logged in the log of events.

5.9.4.1 Submission of suspicious files

If you want to submit a suspicious file, you can do it in the file submission confirmation dialog window. Suspicious files resembling infiltrations in their content or behavior are submitted to ESET for analysis by means of ThreatSense Net technology.

**File** - This section shows the list of files ready for submitting. Deselect the checkbox next to any file to exclude it from the list - such files will no longer be submitted and displayed in the list.

**Select all files** - Select this checkbox to select all files in the above list.

**Submit** - Click to submit selected files.

**Cancel** - Closes the dialog window without submitting any file.

**Do not show this window and submit files without asking** - Select this option to submit files automatically without user interaction.

**NOTE**: File size limit for submitted files is 3 Mb.

5.10 Miscellaneous

The Miscellaneous setup screen contains complementary setup options for ESET Mail Security:

- **Proxy server**
- **License Management**
- **Remote administration**

5.10.1 Proxy server

In large LAN networks, the connection of your computer to the Internet can be mediated by a proxy server. If this is the case, the following settings need to be defined. Otherwise the program will not be able to update itself automatically.

**Use proxy server** - Should be checked if your computer uses a proxy server to connect to the Internet.

**Proxy server, Port** - Enter the IP address and port of the proxy server you use.

**Proxy server requires authentication** - If the proxy server requires authentication, the fields should be filled in with a valid username and password, granting access to the proxy server.

**Username, Password** - These are your authentication data to access the proxy server. Fill in these fields only if a username and password are required.

**Detect proxy server** - Click this button to automatically detect proxy server settings.
5.10.2 License Management

It is important to enter the license file for ESET Mail Security for IBM Lotus Domino. Without it, email protection on the IBM Lotus Domino Server will not work properly. If you do not add the license file during installation, you can do so later in Advanced setup (F5), under **Miscellaneous > Licenses**.

ESET Mail Security allows you to use several licenses simultaneously by merging them, as described below:

1) Two or more licenses for 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), the only difference being 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.

To add/remove a license key, click on the corresponding button of the license manager window. If you are interested in purchasing ESET products, click **Order**... You will be redirected to the online store website (the **Order**... button is only available when a license key is expired).

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

5.10.2.1 Verify license validity

Validity of currently entered license information (username and password). The License validity window displays the expiration date for the username and password entered in the update setup. Correctly entered authentication data is necessary for the virus signature database and program updates to remain up-to-date, which is the most important aspect of any security software.


5.10.3 Remote administration

ESET Remote Administrator is a program that serves to manage ESET's products in larger networks. Using remote administration, you can control the program as if you were working directly on your computer. You can install, configure, view logs, schedule update tasks, configure scan tasks, etc. Communication between ESET Remote Administrator (ERAS) and ESET security products requires correct configuration on both end points.

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

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

- **Interval between connections to server (min.)** - This designates the frequency that ESET Mail Security will connect to the ERA Server. If it is set to 0, information will be submitted every 5 seconds.

- **Primary server, Secondary server** - Usually, only the Primary server needs to be configured. If you are running multiple ERA servers on the network, you can opt to add another, secondary ERA server connection. It will serve as the fallback solution. This way, if the Primary server becomes inaccessible, the ESET security solution will automatically contact the Secondary ERAS. Simultaneously, it will attempt to reestablish the connection to the Primary server. After this connection is active again, ESET security solution will switch back to the Primary server. Configuring two remote administration server profiles is best used for mobile clients with notes connecting both from the local network and from outside the network.

- **Server address** - Network address (DNS Name or IP 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.

- **Never connect to server with unsecured communication** - Select this option to disable connecting to ERA servers where unauthenticated access is enabled (see ERA console > Server Options > Security > Enable unauthenticated access for Clients).
Click **OK** to confirm changes and apply the settings. ESET Mail Security will use these settings to connect to the ERA Server.

### 5.11 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.

#### 5.11.1 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](http://go.eset.eu/AIK)) or ([http://go.eset.eu/ADK](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

#### 5.11.2 How to create rescue CD

To launch the ESET SysRescue wizard, click **Start** > **Programs** > **ESET** > **ESET Mail Security** > **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](http://go.eset.eu/AIK)) or Windows ADK ([http://go.eset.eu/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, select the target media where ESET SysRescue will be located.
5.11.3 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.

5.11.4 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**
- **ESET Antivirus**
- **Advanced**
- **Internet protocol**
- **Bootable USB device** (when the target USB device is selected)
- **Burning** (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.

5.11.4.1 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.

5.11.4.2 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.
5.11.4.3 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.

5.11.4.4 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.

5.11.4.5 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.

5.11.4.6 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.
5.11.5 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.

5.11.5.1 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.

5.12 ESET Sysinspector

5.12.1 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.

5.12.1.1 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.
5.12.2 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.).

5.12.2.1 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.
"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.

5.12.2.2 **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.

5.12.2.2.1 **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
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
- new value, not present in the previous log
- − removed value, present in the previous log only
- removed value, present in the previous log only
- ◯ value / file has been changed
- modified value / 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

5.12.3 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.
5.12.4 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.

5.12.4.1 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.

5.12.4.2 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\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...

In this example the module khbekhb.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 (iaakmp)
[...

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 0-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.
5.12.4.3 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.

5.12.5 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 “SysInpsector-%COMPUTERNAME%-%YMMDD-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.
6. eShell

eShell (short for ESET Shell) is a command line interface for ESET Mail Security. 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 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 `eshell` with appropriate parameters. For example:

  ```plaintext
  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](#).

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 `eshell` and pressing the Enter key

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

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.
6.1 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 Mail Security 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>)
- 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).
6.2 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 Mail Security 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 Mail Security 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:

```
estart 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:
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 Mail Security (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.

### 6.2.1 Context - AV

**ANTISTEALTH**

Enable Anti-Stealth.

**SYNTAX:**

```plaintext
[get] | restore antistealth
set antistealth disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**CLEANLEVEL**

Cleaning level.

**SYNTAX:**

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

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

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

**EXCLUSIONS**

Exclusions.

**SYNTAX:**

```plaintext
[get] | clear exclusions
add | remove exclusions <exclusion>
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **add** - Add item
- **remove** - Removes item

**ARGUMENTS:**

- **exclusion** - Excluded file/folder/mask

**EXTENSIONS**
Scanned/excluded extensions.

SYNTAX:

[get] | restore extensions
add | remove extensions <extension> | /all | /extless

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:

extension - Extension
all - All files
extless - Extensionless files

SELFDEFENSE

Self-defense.

SYNTAX:

[get] | restore selfdefense
set selfdefense disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

STATUS

Antivirus protection status.

SYNTAX:

[get] | restore status
set status disabled | enabled

OPERATIONS:

get - Show antivirus protection status
set - Disable/Enable antivirus protection
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disable antivirus protection
enabled - Enable antivirus protection
6.2.2 Context - AV DOCUMENT

CLEANLEVEL
Cleaning level.

SYNTAX:

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

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

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

EXTENSIONS
Scanned/excluded extensions.

SYNTAX:

[get] | restore extensions
add | remove extensions <extension> | /all | /extless

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:

extension - Extension
all - All files
extless - Extensionless files

INTEGRATION
Integrate document protection into system.

SYNTAX:

[get] | restore integration
set integration disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
STATUS
Current document protection status.

SYNTAX:
[get] | restore status
set status disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.3 Context - AV EMAIL
ACTION
Action for infected messages.

SYNTAX:
[get] | restore action
set action none | delete | movedeleted | moveto

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
none - No action
delete - Delete message
movedeleted - Move to deleted
moveto - Move to folder

CLIENTS
Email clients.

SYNTAX:
[get] clients
add | remove clients <path>

OPERATIONS:
get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:
path - Applications path
NOTE: With filtering by application only, you must specify which applications serve as email clients. If an application is not marked as an email client, email may not be scanned.

**QUARANTINE**

Infected messages folder.

**SYNTAX:**

```
[get] | restore quarantine
set quarantine <string>
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **string** - Folder name

**STATUS**

Email client protection status.

**SYNTAX:**

```
[get] | restore status
set status disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**6.2.4 Context - AV EMAIL GENERAL**

**CLEANLEVEL**

Cleaning level.

**SYNTAX:**

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

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **none** - Do not clean
- **normal** - Standard cleaning
- **strict** - Strict cleaning
EXTENSIONS
Scanned/excluded extensions.

SYNTAX:

```
[get] | restore extensions

add | remove extensions <extension> | /all | /extless
```

OPERATIONS:

- get - Returns current setting/status
- add - Add item
- remove - Removes item
- restore - Restores default settings/object/file

ARGUMENTS:

- extension - Extension
- all - All files
- extless - Extensionless files

6.2.5 Context - AV LIMITS ARCHIVE

LEVEL
Archive nesting level.

SYNTAX:

```
[get] | restore level

set level <number>
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- number - Level from 1 to 20 or 0 for default settings

SIZE
Maximum size of file in archive (kB).

SYNTAX:

```
[get] | restore size

set size <number>
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- number - Size in kB or 0 for default settings
6.2.6 Context - AV LIMITS OBJECTS

SIZE
Maximum archive size (kB).
SYNTAX:
[get] | restore size
set size <number>
OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:
number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).
SYNTAX:
[get] | restore timeout
set timeout <number>
OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:
number - Time in seconds or 0 for default settings

6.2.7 Context - AV NETFILTER

AUTOSTART
Run HTTP and POP3 application protocol content filtering automatically.
SYNTAX:
[get] | restore autostart
set autostart disabled | enabled
OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXCLUDED
Applications excluded from protocol filtering.
SYNTAX:

[get] excluded
add | remove excluded <path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:

path - Applications path

MODE
Redirect traffic for filtering.

SYNTAX:

[get] | restore mode
set mode ports | application | both

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

ports - HTTP and POP3 ports
application - Applications marked as Internet browsers or email clients
both - Ports and applications marked as Internet browsers or email clients

STATUS
Enable HTTP and POP3 application protocol content filtering.

SYNTAX:

[get] | restore status
set status disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
6.2.8 Context - AV NETFILTER PROTOCOL SSL

BLOCKSSL2

Block encrypted communication utilizing the obsolete protocol SSL v2.

SYNTAX:

[get] | restore blockssl2
set blockssl2 disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXCEPTIONS

Apply created exceptions based on certificates.

SYNTAX:

[get] | restore exceptions
set exceptions disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MODE

SSL filtering mode.

SYNTAX:

[get] | restore mode
set mode always | ask | none

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

always - Always use SSL checking
ask - Ask about non-visited sites (exclusions can be set)
none - Do not use SSL protocol checking
6.2.9 Context - AV NETFILTER PROTOCOL SSL CERTIFICATE

ADDTOBROWSERS
Add the root certificate to known browsers.

SYNTAX:

[get] | restore addtobrowsers
set addtobrowsers disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

NOTE: To properly check SSL-encrypted traffic, the root certificate for ESET, spol. s r.o used to sign certificates will be added to the Trusted Root Certification Authorities (TRCA) certificate store.

EXCLUDED
List of certificates excluded from content filtering.

SYNTAX:

[get] excluded
remove excluded <name>

OPERATIONS:

get - Returns current setting/status
remove - Removes item

ARGUMENTS:

name - Certificate name

NOTTRUSTED
Not trusted if the certificate is invalid or corrupt.

SYNTAX:

[get] | restore nottrusted
set nottrusted ask | block

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

ask - Ask about certificate validity
block - Block communication that uses the certificate

TRUSTED
List of trusted certificates.
SYNTAX:
```
[get] trusted
remove trusted <name>
```

OPERATIONS:
```
get - Returns current setting/status
remove - Removes item
```

ARGUMENTS:
```
name - Certificate name
```

UNKNOWNROOT
Unknown root - if the certificate cannot be verified using the TRCA certificate store.

SYNTAX:
```
[get] | restore unknownroot
set unknownroot ask | block
```

OPERATIONS:
```
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
```

ARGUMENTS:
```
ask - Ask about certificate validity
block - Block communication that uses the certificate
```

6.2.10  Context - AV OBJECTS

ARCHIVE
Scan archives.

SYNTAX:
```
[get] | restore archive
set archive disabled | enabled
```

OPERATIONS:
```
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
```

ARGUMENTS:
```
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
```

BOOT
Scan boot sectors.

SYNTAX:
```
[get] | restore boot
set boot disabled | enabled
```

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EMAIL
Scan email files.

SYNTAX:
[get] | restore email
set email disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MEMORY
Scan memory.

SYNTAX:
[get] | restore memory
set memory disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.

SYNTAX:
[get] | restore runtime
set runtime disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX
Scan self-extracting archives.

SYNTAX:

[get] | restore sfx
set sfx disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.11 Context - AV OPTIONS

ADVHEURISTICS
Use advanced heuristics.

SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HEURISTICS
Use heuristics.

SYNTAX:

[get] | restore heuristics
set heuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting

enabled - Enables function/activates setting

UNSAFE
Detection of potentially unsafe applications.
SYNTAX:

[get] | restore unsafe
set unsafe disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED
Detection of potentially unwanted applications.
SYNTAX:

[get] | restore unwanted
set unwanted disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.12 Context - AV OTHER
LOGALL
Log all objects.
SYNTAX:

[get] | restore logall
set logall disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPTIMIZE
Smart optimization.

SYNTAX:

[get] | restore optimize

set optimize disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.13 Context - AV REALTIME

AUTOSTART

Start real-time protection automatically.

SYNTAX:

[get] | restore autostart

set autostart disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

CLEANLEVEL

Cleaning level

SYNTAX:

[get] | restore cleanlevel

set cleanlevel none | normal | strict

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

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

EXTENSIONS

Scanned/excluded extensions.
SYNTAX:

[get] | restore extensions
add | remove extensions <extension> | /all | /extless

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:

extension - Extension
all - All files
extless - Extensionless files

STATUS

Real-time computer protection status.

SYNTAX:

[get] | restore status
set status disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.14 Context - AV REALTIME DISK

FLOPPY

Scan removable media.

SYNTAX:

[get] | restore floppy
set floppy disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

LOCAL

Scan local drives.
SYNTAX:

[get] | restore local
set local disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

NETWORK

Scan network drives.

SYNTAX:

[get] | restore network
set network disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.15 Context - AV REALTIME EVENT

CREATE

Scan files on creation.

SYNTAX:

[get] | restore create
set create disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXECUTE

Scan files on execution.

SYNTAX:

[get] | restore execute
set execute disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FLOPPY ACCESS
Scan on floppy access.

SYNTAX:
[get] | restore floppyaccess
set floppyaccess disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPEN
Scan files on opening.

SYNTAX:
[get] | restore open
set open disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SHUTDOWN
Scan on computer shutdown.

SYNTAX:
[get] | restore shutdown
set shutdown disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.16 Context - AV REALTIME EXECUTABLE
ADVHEURISTICS
Enable advanced heuristics on file execution.
SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.17 Context - AV REALTIME EXECUTABLE FROMREMOVABLE
ADVHEURISTICS
Enable advanced heuristics on file execution from removable media.
SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXCLUSION
USB drive exclusions.
SYNTAX:

[get] | restore exclusion
select exclusion none | <drive> | all

OPERATIONS:

get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:

none - Deselect all drives
drive - Letter of a drive to select/deselect
call - Select all drives

NOTE: Use this option to allow exceptions from scanning using Advanced heuristics on file execution. Advanced heuristics settings for hard drives will be applied to selected devices.

6.2.18 Context - AV REALTIME LIMITS ARCHIVE

LEVEL

Archive nesting level.

SYNTAX:

[get] | restore level
set level <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Level from 1 to 20 or 0 for default settings

SIZE

Maximum size of file in archive (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

6.2.19 Context - AV REALTIME LIMITS OBJECTS

SIZE

Maximum archive size (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
  number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).
SYNTAX:
  [get] | restore timeout
  set timeout <number>

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  number - Time in seconds or 0 for default settings

6.2.20 Context - AV REALTIME OBJECTS

BOOT
Scan boot sectors.
SYNTAX:
  [get] | restore boot
  set boot disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.
SYNTAX:
  [get] | restore runtime
  set runtime disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.21 Context - AV REALTIME ONWRITE

ADVHEURISTICS
Enable advanced heuristics for new and modified files.
SYNTAX:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan new and modified runtime archives.
SYNTAX:

```
[get] | restore runtime
set runtime disabled | enabled
```

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX
Scan new and modified self-extracting archives.
SYNTAX:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
6.2.22 Context - AV REALTIME ONWRITE ARCHIVE

LEVEL

Archive nesting depth.

SYNTAX:

[get] | restore level
set level <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Level (0 - 20)

SIZE

Maximum size of a scanned archived file (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size (kB)

6.2.23 Context - AV REALTIME OPTIONS

ADVHEURISTICS

Use advanced heuristics.

SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HEURISTICS

Use heuristics.
SYNTAX:

[get] | restore heuristics

set heuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNSAFE

Detection of potentially unsafe applications.

SYNTAX:

[get] | restore unsafe

set unsafe disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED

Detection of potentially unwanted applications.

SYNTAX:

[get] | restore unwanted

set unwanted disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
6.2.24 Context - AV REALTIME OTHER

LOGALL
Log all objects.
SYNTAX:

```
[get] | restore logall
set logall disabled | enabled
```

OPERATIONS:
- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:
- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

OPTIMIZE
Smart optimization.
SYNTAX:

```
[get] | restore optimize
set optimize disabled | enabled
```

OPERATIONS:
- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:
- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

6.2.25 Context - AV REALTIME REMOVABLE

BLOCK
Block removable media.
SYNTAX:

```
[get] | restore block
set block disabled | enabled
```

OPERATIONS:
- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:
- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting
EXCLUSION

Allowed removable media.

SYNTAX:

[get] | restore exclusion

select exclusion none | <drive> | all

OPERATIONS:

get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:

none - Deselect all drives
drive - Letter of a drive to select/deselect
all - Select all drives

NOTE: Use this option to enable access to removable media (CD, floppy disks, USB drives). Marking a media results in removing access restrictions when attempting to access that specific media.

6.2.26 Context - AV WEB

BROWSERS

Internet browsers.

SYNTAX:

[get] browsers

add | remove browsers <path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:

path - Applications path

NOTE: To increase security, we recommend that you mark any application used as an Internet browser by checking the appropriate box. If an application is not marked as a web browser, data transferred using that application may not be scanned.

CLEANLEVEL

Cleaning level.

SYNTAX:

[get] | restore cleanlevel

set cleanlevel none | normal | strict

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
none - Do not clean
normal - Standard cleaning
strict - Strict cleaning

EXTENSIONS
Scanned/excluded extensions.

SYNTAX:
[get] | restore extensions
add | remove extensions <extension> | /all | /extless

OPERATIONS:
get - Returns current setting/status
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:
extension - Extension
all - All files
extless - Extensionless files

STATUS
Web access protection.

SYNTAX:
[get] | restore status
set status disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.27 Context - AV WEB ADDRESSMGMT
ADDRESS
Address management in the selected list.

SYNTAX:
[get] | clear address
add | remove address <address>
import | export address <path>

OPERATIONS:
get - Returns current setting/status
add - Add item
remove - Removes item
import - Imports from file
export - Exports to file
clear - Removes all items/files

ARGUMENTS:
address - Address
path - File path

LIST
Address list management.
SYNTAX:

[get] | restore list
set list <listname> disabled | enabled
select | remove list <listname>
add list allowed <listname> | blocked <listname> | excluded <listname>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
select - Select for editing
add - Add item
remove - Removes item

ARGUMENTS:
listname - List name
disabled - Do not use list
enabled - Use list
allowed - List of allowed addresses
blocked - List of blocked addresses
excluded - List of addresses excluded from filtering

NOTE: To edit the selected list (marked with - x) use the `av web addressmgmt address` command.

NOTIFY
Notify when applying address from the list.
SYNTAX:

[get] | restore notify
set notify disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

WHITELISTED
Allow access only to HTTP addresses in the list of allowed addresses.

SYNTAX:
```plaintext
[get] | restore whitelisted
set whitelisted disabled | enabled
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

6.2.28 Context - AV WEB LIMITS ARCHIVE

LEVEL
Archive nesting level.

SYNTAX:
```plaintext
[get] | restore level
set level <number>
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- number - Level from 1 to 20 or 0 for default settings

SIZE
Maximum size of file in archive (kB).

SYNTAX:
```plaintext
[get] | restore size
set size <number>
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- number - Size in kB or 0 for default settings
6.2.29 Context - AV WEB LIMITS OBJECTS

SIZE
Maximum archive size (kB).
SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).
SYNTAX:

[get] | restore timeout
set timeout <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Time in seconds or 0 for default settings

6.2.30 Context - AV WEB OBJECTS

ARCHIVE
Scan archives.
SYNTAX:

[get] | restore archive
set archive disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

BOOT
Scan boot sectors.
SYNTAX:

get | restore boot

set boot disabled | enabled

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting

enabled - Enables function/activates setting

EMAIL

Scan email files.

SYNTAX:

[get] | restore email

set email disabled | enabled

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting

enabled - Enables function/activates setting

FILE

Scan files.

SYNTAX:

[get] | restore file

set file disabled | enabled

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting

enabled - Enables function/activates setting

MEMORY

Scan memory.

SYNTAX:

[get] | restore memory

set memory disabled | enabled
OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
   enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.

SYNTAX:
   [get] | restore runtime
   set runtime disabled | enabled

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
   enabled - Enables function/activates setting

SFX
Scan self-extracting archives.

SYNTAX:
   [get] | restore sfx
   set sfx disabled | enabled

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
   enabled - Enables function/activates setting

6.2.31 Context - AV WEB OPTIONS

ADVHEURISTICS
Use advanced heuristics.

SYNTAX:
   [get] | restore advheuristics
   set advheuristics disabled | enabled

OPERATIONS:
   get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
generated - Enables function/activates setting

ADWARE
Detection of Adware/Spyware/Riskware.
SYNTAX:
[get] | restore adware
set adware disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
generated - Enables function/activates setting

HEURISTICS
Use heuristics.
SYNTAX:
[get] | restore heuristics
set heuristics disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
generated - Enables function/activates setting

SIGNATURES
Use signatures.
SYNTAX:
[get] | restore signatures
set signatures disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNSAFE
Detection of potentially unsafe applications.
SYNTAX:

[get] | restore unsafe
set unsafe disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED
Detection of potentially unwanted applications.
SYNTAX:

[get] | restore unwanted
set unwanted disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.32   Context - AV WEB OPTIONS BROWSERS

ACTIVEMODE
Active mode for Internet browsers.
SYNTAX:

[get] activemode
add | remove activemode <path>

OPERATIONS:
get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:
path - Applications path

NOTE: Programs added to the list are automatically added to the Internet browsers list.
6.2.33  Context - AV WEB OTHER

LOGALL

Log all objects.

SYNTAX:

[get] | restore logall
set logall disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPTIMIZE

Smart optimization.

SYNTAX:

[get] | restore optimize
set optimize disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.34  Context - AV WEB PROTOCOL HTTP

PORTS

Ports used by HTTP.

SYNTAX:

[get] | restore ports
set ports [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Port numbers separated by a colon

USE
Scan HTTP.

SYNTAX:

```
[get] | restore use
set use disabled | enabled
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **disabled**: Disables function/deactivates setting
- **enabled**: Enables function/activates setting

### 6.2.35 Context - AV WEB PROTOCOL HTTPS

#### MODE

HTTPS filtering mode.

SYNTAX:

```
[get] | restore mode
set mode none | ports | browsers
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **none**: Do not use protocol checking
- **ports**: Use HTTPS protocol checking for selected ports
- **browsers**: Use HTTPS protocol checking for applications marked as browsers that use selected ports

### PORTS

Ports used by HTTPS protocol.

SYNTAX:

```
[get] | restore ports
set ports [<string>]
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **string**: Port numbers delimited by a comma
6.2.36 Context - GENERAL

CONFIG
Import/export settings.
SYNTAX:

    import | export config <path>

OPERATIONS:

    import - Imports from file
    export - Exports to file

ARGUMENTS:

    path - File path

LICENSE
License management.
SYNTAX:

    [get] license
    import license <path>
    export license <ID> <path>
    remove license <ID>

OPERATIONS:

    get - Returns current setting/status
    remove - Removes item
    import - Imports from file
    export - Exports to file

ARGUMENTS:

    path - License file path
    ID - License ID

6.2.37 Context - GENERAL ACCESS

ADMIN
Administrator rights settings protection.
SYNTAX:

    [get] | restore admin
    set admin disabled | enabled

OPERATIONS:

    get - Returns current setting/status
    set - Sets value/status
    restore - Restores default settings/object/file

ARGUMENTS:

    disabled - Disables function/deactivates setting
    enabled - Enables function/activates setting
BATCH
Execute commands entered as arguments when eShell is running.

SYNTAX:

```
[get] | restore batch
set batch disabled | <time> | always
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `disabled` - Disabled
- `time` - Time interval in minutes (1 - 1440 minutes)
- `always` - Always

PASSWORD
This password is used for password-protected commands. Normally, to execute a password-protected commands you are prompted to type in a password. This is for security reasons. It applies to commands such as those that disable antivirus protection and those that may affect ESET Mail Security functionality. You will be prompted for password every time you execute such command. Alternatively, you can define this password for your current eShell session and you will not be prompted to enter password. For more details click here.

For interactive password input (recommended) leave parameters empty. To reset password enter empty password.

CONTEXT PATH:

```
general access
```

SYNTAX:

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

OPERATIONS:

- `get` - Show password
- `set` - Set password
- `restore` - Reset 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` - Use this to set password, simply enter your password (if no password is entered, settings protection is not used)
- `restore password` - This command clears existing password (settings protection will not be used)

GUI EQUIVALENT:

- click here to see how this is configured via GUI
6.2.38  Context - GENERAL ESHELL

ALIAS

Alias management.

SYNTAX:

```
[get] | clear | restore alias
add alias [.] <alias>=<command>
remove alias <alias>
import | export alias <path>
```

OPERATIONS:

```
get - Returns current setting/status
add - Add item
remove - Removes item
import - Imports from file
export - Exports to file
restore - Restores default settings/object/file
```

ARGUMENTS:

```
. - Create global alias
alias - New alias
command - Associated command (command validity not checked)
alias - Alias to delete
path - File path
```

LISTER

Use lister.

SYNTAX:

```
[get] | restore lister
set lister disabled | enabled
```

OPERATIONS:

```
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
```

ARGUMENTS:

```
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
```
6.2.39 Context - GENERAL ESHELL COLOR

ALIAS

Alias color.

SYNTAX:

[get] | restore alias

set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

COMMAND

Command color.

SYNTAX:

[get] | restore command

set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

CONTEXT
Context color.

SYNTAX:

[get] | restore context

set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green
| cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

DEFAULT
Base color.

SYNTAX:

[get] | restore default

set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green |
| cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

DISABLED
N/A color.

SYNTAX:

[get] | restore disabled

set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue |
green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

ERROR

Color of error messages.

SYNTAX:

[get] | restore error

set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

**INTERACTIVE**

Interactive operations color.

**SYNTAX:**

```
[get] | restore interactive
```

```
set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

**OPERATIONS:**

```
get - Returns current setting/status
```

```
set - Sets value/status
```

```
restore - Restores default settings/object/file
```

**ARGUMENTS:**

```
black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White
```

**LIST1**

List color 1.

**SYNTAX:**

```
[get] | restore list1
```

```
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

**OPERATIONS:**

```
get - Returns current setting/status
```

```
set - Sets value/status
```
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

LIST2
List color 2.

SYNTAX:

[get] | restore list2

set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

SUCCESS
Status OK color.

SYNTAX:

[get] | restore success

set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

WARNING
Color of warning messages.

SYNTAX:

[get] | restore warning

set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyane - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

6.2.40  Context - GENERAL ESHELL OUTPUT
UTF8

UTF8 encoded output.

SYNTAX:

[get] | restore utf8

set utf8 disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

NOTE: For correct display, command line should use a TrueType font like 'Lucida Console'.
6.2.41 Context - GENERAL ESHELL STARTUP
LOADCOMMANDS
Load all commands on startup.
SYNTAX:
```
[get] | restore loadcommands
set loadcommands disabled | enabled
```
OPERATIONS:
```
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
```
ARGUMENTS:
```
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
```
STATUS
Display protection status on startup.
SYNTAX:
```
[get] | restore status
set status disabled | enabled
```
OPERATIONS:
```
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
```
ARGUMENTS:
```
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
```
6.2.42 Context - GENERAL ESHELL VIEW
CMDHELP
Display help on command failure.
SYNTAX:
```
[get] | restore cmdhelp
set cmdhelp disabled | enabled
```
OPERATIONS:
```
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
```
ARGUMENTS:
```
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
```
COLORS
Use colors.
SYNTAX:

[get] | restore colors
set colors disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FITWIDTH
Trim text to fit width.
SYNTAX:

[get] | restore fitwidth
set fitwidth disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

GLOBAL
Display global commands.
SYNTAX:

[get] | restore global
set global disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HIDDEN
Display hidden commands.
SYNTAX:
OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPERATIONS

Display operations in commands list.

SYNTAX:

[get] | restore operations
set operations disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SHORTLIST

Display short command list on context change.

SYNTAX:

[get] | restore shortlist
set shortlist disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SYNTAXHINT

Display command syntax hints.

SYNTAX:

[get] | restore syntaxhint
set syntaxhint disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

VALUESONLY
Display only values without description.

SYNTAX:

[get] | restore valuesonly
set valuesonly disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.43 Context - GENERAL PERFORMANCE
SCANNERS
Number of running scans.

SYNTAX:

[get] | restore scanners
set scanners <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Count (1 - 20)

6.2.44 Context - GENERAL PROXY
ADDRESS
Proxy server address.

SYNTAX:

[get] | restore address
set address [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Address

DETECT
Detects proxy server configuration.
SYNTAX:

detect

LOGIN
Login name.
SYNTAX:

[get] | restore login
set login [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Name

PASSWORD
Proxy server password.
SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to entering password as parameter
password - Password

PORT
Port
SYNTAX:

[get] | restore port
set port <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
**RESTORE**

Restores default settings/object/file

**ARGUMENTS:**

- **number** - Port number

**USE**

Use proxy server.

**SYNTAX:**

```
[get] | restore use
set use disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

---

**6.2.45 Context - GENERAL QUARANTINE RESCAN**

**UPDATE**

Scan quarantined files after every update.

**SYNTAX:**

```
[get] | restore update
set update disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

---

**6.2.46 Context - GENERAL REMOTE INTERVAL**

Connection interval (minutes).

**SYNTAX:**

```
[get] | restore interval
set interval <number>
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file
ARGUMENTS:

number - Time in minutes (1 - 1440)

USE
ERA Server connection.

SYNTAX:

[get] | restore use
    set use disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.47 Context - GENERAL REMOTE SERVER PRIMARY ADDRESS
ERA Server address.

SYNTAX:

[get] | restore address
    set address [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Address

ENCRYPT
Block unencrypted connection.

SYNTAX:

[get] | restore encrypt
    set encrypt disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

PASSWORD
ERA Server password.

SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to entering password as parameter
password - Password

PORT

ERA Server port.

SYNTAX:

[get] | restore port
set port <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Port number

6.2.48 Context - GENERAL REMOTE SERVER SECONDARY ADDRESS

ERA Server address.

SYNTAX:

[get] | restore address
set address [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Address

ENCRYPT

Block unencrypted connection.

SYNTAX:

[get] | restore encrypt
set encrypt disabled | enabled
OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

PASSWORD
ERA Server password.

SYNTAX:
- [get] | restore password
- set password [plain <password>]

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- plain - Switch to entering password as parameter
- password - Password

PORT
ERA Server port.

SYNTAX:
- [get] | restore port
- set port <number>

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- number - Port number

6.2.49 Context - GENERAL TS.NET

EXCLUSION
Exclude from submission.

SYNTAX:
- [get] | restore exclusion
- add | remove exclusion <exclusion>

OPERATIONS:
- get - Returns current setting/status
- add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:
  exclusion - Extension

FROM
Contact e-mail.

SYNTAX:
  [get] | restore from
  set from [<string>]

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  string - E-mail address

LOGING
Log creation.

SYNTAX:
  [get] | restore loging
  set loging disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

SENDING
Submission of suspicious files.

SYNTAX:
  [get] | restore sending
  set sending none | ask | auto

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  none - Do not submit
  ask - Confirm before sending for analysis
auto - Send for analysis without confirmation

VIA
Means of file submission.

SYNTAX:

[get] | restore via
set via auto | ra | direct

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

auto - By means of Remote Administrator or directly to ESET
ra - By means of Remote Administrator
direct - Directly to ESET

WHEN
When to submit suspicious files.

SYNTAX:

[get] | restore when
set when asap | update

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

asap - As soon as possible
update - During update

6.2.50 Context - GENERAL TS.NET STATISTICS

SENDING
Statistic information submission.

SYNTAX:

[get] | restore sending
set sending disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
WHEN
Submission of anonymous statistical information.

SYNTAX:

[get] | restore when
    set when asap | update

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

asap - As soon as possible
update - During update

6.2.51 Context - SCANNER
CLEANLEVEL
Cleaning level.

SYNTAX:

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

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

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

EXTENSIONS
Scanned/excluded extensions.

SYNTAX:

[get] | restore extensions
    add | remove extensions <extension> | /all | /extless

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:

extension - Extension
all - All files
extless - Extensionless files

PROFILE
Computer scan profile management.

SYNTAX:
```
[get] profile
  select | remove profile <name>

  add profile new: <name> [copyfrom: <name>]  
```

OPERATIONS:
```
get - Returns current setting/status
select - Selects item
add - Add item
remove - Removes item
```

ARGUMENTS:
```
name - Profile name
new - New profile
copyfrom - Copy settings from profile
```

NOTE: Other context commands refer to the active profile (marked with -x). For the active profile selection use `select scanner profile <profile name>`.

SCAN
Computer scan.

SYNTAX:
```
[get] | clear scan
  start scan [readonly] 

  pause | resume | stop scan <ID> | all
```

OPERATIONS:
```
get - Show running and completed scans
start - Run computer scan for the selected profile
stop - Stop scan
resume - Continue paused scan
pause - Pause scan
clear - Remove completed scans from list
```

ARGUMENTS:
```
readonly - Scan without cleaning
ID - Scan ID for command execution
all - Execute command for all scans
```

TARGET
Scan targets for active profile.

SYNTAX:
```
[get] target
   add | remove target <path>
```
OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:

path - Path/Scan target

NOTE: For boot sector scan enter X:\${Boot} where ‘x’ is the name of scanned disk.

6.2.52 Context - SCANNER LIMITS ARCHIVE

LEVEL

Archive nesting level.

SYNTAX:

[get] | restore level
set level <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Level from 1 to 20 or 0 for default settings

SIZE

Maximum size of file in archive (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

6.2.53 Context - SCANNER LIMITS OBJECTS

SIZE

Maximum archive size (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).

SYNTAX:

[get] | restore timeout
set timeout <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Time in seconds or 0 for default settings

6.2.54 Context - SCANNER OBJECTS

ARCHIVE
Scan archives.

SYNTAX:

[get] | restore archive
set archive disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

BOOT
Scan boot sectors.

SYNTAX:

[get] | restore boot
set boot disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EMAIL
Scan email files.
SYNTAX:
	[get] | restore email
	set email disabled | enabled
OPERATIONS:

get  - Returns current setting/status
set  - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MEMORY
Scan memory.
SYNTAX:
	[get] | restore memory
	set memory disabled | enabled
OPERATIONS:

get  - Returns current setting/status
set  - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.
SYNTAX:
	[get] | restore runtime
	set runtime disabled | enabled
OPERATIONS:

get  - Returns current setting/status
set  - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX
Scan self-extracting archives.
SYNTAX:

[get] | restore sfx
set sfx disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.55 Context - SCANNER OPTIONS

ADVHEURISTICS
Use advanced heuristics.

SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HEURISTICS
Use heuristics.

SYNTAX:

[get] | restore heuristics
set heuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNSAFE
Detection of potentially unsafe applications.

SYNTAX:

[get] | restore unsafe
set unsafe disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED
Detection of potentially unwanted applications.

SYNTAX:
[get] | restore unwanted
set unwanted disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.56 Context - SCANNER OTHER

ADS
Scan alternate data streams (ADS).

SYNTAX:
[get] | restore ads
set ads disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

LOGALL
Log all objects.

SYNTAX:
[get] | restore logall
set logall disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

LOWPRIORITY
Run background scans with low priority.

SYNTAX:

[get] | restore lowpriority
set lowpriority disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPTIMIZE
Smart optimization.

SYNTAX:

[get] | restore optimize
set optimize disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

PRESERVETIME
Preserve last access timestamp.

SYNTAX:

[get] | restore preservetime
set preservetime disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SCROLL
Scroll scan log.

SYNTAX:

[get] | restore scroll
set scroll disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.57 Context - SERVER
AUTOEXCLUSIONS
Automatic exclusions management.

SYNTAX:

[get] | restore autoexclusions
select autoexclusions <server>

OPERATIONS:

get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:

server - Server name

6.2.58 Context - TOOLS
QUARANTINE
Quarantine.

SYNTAX:

[get] quarantine
add quarantine <path>
send | remove | restore quarantine <ID>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
**RESTORE** - Restores default settings/object/file

**ARGUMENTS:**
- path - File path
- ID - Quarantined file ID

**STATISTICS**
Statistics.

**SYNTAX:**
```
[get] | clear statistics
```

**OPERATIONS:**
- get - Show statistics
- clear - Reset statistics

**SYSINSPECTOR**
SysInspector.

**SYNTAX:**
```
[get] sysinspector
add | remove sysinspector <name>
export sysinspector <name> to:<path>
```

**OPERATIONS:**
- get - Returns current setting/status
- add - Add item
- remove - Removes item
- export - Exports to file

**ARGUMENTS:**
- name - Comment
- path - File name (.zip or .xml)

**6.2.59 Context - TOOLS ACTIVITY**

**FILESYSTEM**
File system activity.

**SYNTAX:**
```
[get] filesystem [count] [seconds | minutes | hours [year-month]]
```

**ARGUMENTS:**
- count - Number of records to show
- seconds - Sampling 1 second
- minutes - Sampling 1 minute
- hours - Sampling 1 hour
- year - Year to display
- month - Month to display
6.2.60  Context - TOOLS LOG

DETECTIONS

This is useful when you need to view information about detected infiltrations.

CONTEXT PATH:

   root

SYNTAX:

   [get] detections [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-<month>-<day> <hour>:<minute>:<second>]
   clear detections

OPERATIONS:

   get - Returns current setting/status
   clear - Removes all items/files

ARGUMENTS:

   count - Show selected number of records
   number - Number of records
   from - Show records from the specified time
   year - Year
   month - Month
   day - Day
   hour - Hour
   minute - Minute
   second - Second
   to - Show records until the selected time

ALIASES:

   virlog

EXAMPLES:

   get detections from 2011-04-14 01:30:00 - Displays all infiltrations detected after 14th of April 2011 01:30:00
   (when defining date, you need to include time as well for the command to work properly)
   clear detections - Clears the whole log

EVENTS

This is useful when you need to view information about various events.

SYNTAX:

   [get] events [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-<month>-<day> <hour>:<minute>:<second>]
   clear events

OPERATIONS:

   get - Returns current setting/status
   clear - Removes all items/files

ARGUMENTS:

   count - Show selected number of records
   number - Number of records
from - Show records from the specified time
year - Year
month - Month
day - Day
hour - Hour
minute - Minute
second - Second
to - Show records until the selected time

ALIASES:
warnlog

EXAMPLES:
get events from 2011-04-14 01:30:00 - Displays all events that occurred after 14th of April 2011 01:30:00 (when defining date, you need to include time as well for the command to work properly)
clear events - Clears the whole log

FILTER
Minimum verbosity of events to display.

SYNTAX:
[get] | restore filter
set filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] [all]] [smart]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
none - No records
critical - Critical errors
errors - Errors
warnings - Warnings
informative - Informative records
diagnostic - Diagnostic records
all - All records
smart - Smart filtering

SCANS
'Computer scan' log or log list.

SYNTAX:
[get] scans [id:<id>] [count:<number>] [from:<year>-<month>-<day> <hour>:<minute>:<second>] [to:<year>-<month>-<day> <hour>:<minute>:<second>] clear scans

OPERATIONS:
get - Returns current setting/status
clear - Removes all items/files

ARGUMENTS:

  id - Show computer scan details with ID
  id - Scan ID
  count - Show only selected number of records
  number - Number of records
  from - Show only records from the selected time
  year - Year
  month - Month
  day - Day
  hour - Hour
  minute - Minute
  second - Second
  to - Show only records from the selected time

VERBOSITY
Minimum logging verbosity.

SYNTAX:

  [get] | restore verbosity

  set verbosity critical | errors | warnings | informative | diagnostic

OPERATIONS:

  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:

  critical - Critical errors
  errors - Errors
  warnings - Warnings
  informative - Informative records
  diagnostic - Diagnostic records

6.2.61 Context - TOOLS LOG CLEANING

TIMEOUT
Log record lifetime (days).

SYNTAX:

  [get] | restore timeout

  set timeout <number>

OPERATIONS:

  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file
ARGUMENTS:
  number - Days (1 - 365)

USE
Automatic log deletion.

SYNTAX:
  [get] | restore use
  set use disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

6.2.62 Context - TOOLS LOG OPTIMIZE

LEVEL
Optimization by exceeding the number of unused records (percentage).

SYNTAX:
  [get] | restore level
  set level <number>

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  number - Percentage of unused records (1 - 100)

NOW
Immediately optimizes protocol files.

SYNTAX:
  now

Command execution may take a few minutes.

USE
Automatic log optimization.

SYNTAX:
  [get] | restore use
  set use disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

6.2.63 Context - TOOLS NOTIFICATION

VERBOSITY

Minimum verbosity for notifications.

SYNTAX:

[get] | restore verbosity

set verbosity critical | errors | warnings | informative | diagnostic

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

critical - Critical errors
diagnostic - Diagnostic records
errors - Errors
warnings - Warnings
informative - Informative records

6.2.64 Context - TOOLS NOTIFICATION EMAIL

FROM

Senders email address.

SYNTAX:

[get] | restore from

set from [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - E-mail address

LOGIN

Login name.

SYNTAX:

[get] | restore login

set login [<string>]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Name

PASSWORD
Password.

SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to entering password as parameter
password - Password

SERVER
SMTP server address.

SYNTAX:

[get] | restore server
set server [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Address

TO
Recipients e-mail address.

SYNTAX:

[get] | restore to
set to [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - E-mail address
USE
Sending events by email.
SYNTAX:

\[\text{[get]} \mid \text{restore use}\]
\[\text{set use disabled} \mid \text{enabled}\]

OPERATIONS:

\textit{get} - Returns current setting/status
\textit{set} - Sets value/status
\textit{restore} - Restores default settings/object/file

ARGUMENTS:

\texttt{disabled} - Disables function/deactivates setting
\texttt{enabled} - Enables function/activates setting

6.2.65 Context - TOOLS NOTIFICATION MESSAGE
ENCODING
Warning messages encoding.
SYNTAX:

\[\text{[get]} \mid \text{restore encoding}\]
\[\text{set encoding nolocal} \mid \text{localcharset} \mid \text{localencoding} \mid \text{ISO-2022-JP}\]

OPERATIONS:

\textit{get} - Returns current setting/status
\textit{set} - Sets value/status
\textit{restore} - Restores default settings/object/file

ARGUMENTS:

\texttt{nolocal} - Do not use national alphabet characters
\texttt{localcharset} - Use national alphabet characters
\texttt{localencoding} - Use national alphabet characters and encoding
\texttt{ISO} - Use ISO-2022-JP encoding (For japanese version only)

6.2.66 Context - TOOLS NOTIFICATION MESSAGE FORMAT
DETECTION
Format of threat warning messages.
SYNTAX:

\[\text{[get]} \mid \text{restore detection}\]
\[\text{set detection } [\text{<string>}]\]

OPERATIONS:

\textit{get} - Returns current setting/status
\textit{set} - Sets value/status
\textit{restore} - Restores default settings/object/file

ARGUMENTS:
string - Message format

Message format options:

%TimeStamp% - Date and time of the event
%Scanner% - Module that has detected the event
%ComputerName% - Computer name
%ProgramName% - Program which has caused the event
%ErrorDescription% - Error description

For massage format, you need to replace key words (listed here between percent sign “%”) with the corresponding values.

NOTE: ESET Mail Security virus messages and warnings have default format. Changing this format is not recommended. You can change the format in case when you are using automatic email handling system.

EVENT

Event format.

SYNTAX:

[get] | restore event
set event [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Message format

Message format options:

%TimeStamp% - Date and time of the event
%Scanner% - Module that has detected the event
%ComputerName% - Computer name
%ProgramName% - Program which has caused the event
%InfectedObject% - Infected object (file, e-mail,...)
%VirusName% - Virus name

For massage format, you need to replace key words (listed here between percent sign “%”) with the corresponding values.

NOTE: ESET Mail Security virus messages and warnings have default format. Changing this format is not recommended. You can change the format in case when you are using automatic email handling system.
6.2.67  Context - TOOLS NOTIFICATION WINPOPUP

ADDRESS

Send notifications to computer names.

SYNTAX:

```
[get] | restore address
set address [<string>]
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `string` - Computer name separated by a comma

TIMEOUT

Interval of sending to LAN computers.

SYNTAX:

```
[get] | restore timeout
set timeout <number>
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `number` - Interval in seconds (1 - 3600)

USE

Send events to LAN computers.

SYNTAX:

```
[get] | restore use
set use disabled | enabled
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting
6.2.68  Context - TOOLS SCHEDULER

ACTION
Scheduled task action.

SYNTAX:

[get] action
  set action external | logmaintenance | startupcheck | status | scan | update

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

external - Run external application
logmaintenance - Log maintenance
startupcheck - Startup scan
status - Create a computer status snapshot
scan - Computer scan
update - Update

TASK
Scheduled tasks.

SYNTAX:

[get] | select task [<ID>]
set task <ID> disabled | enabled
add task <task_name>
remove | start task <ID>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
select - Selects item
add - Add item
remove - Removes item
start - Starts task

ARGUMENTS:

ID - Task ID
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
task_name - Task name

TRIGGER
Task execution.

SYNTAX:

[get] trigger
set trigger once | repeat | daily | weekly | event

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
once - Once
repeat - Repeatedly
daily - Daily
weekly - Weekly
event - Event triggered

6.2.69 Context - TOOLS SCHEDULER EVENT
INTERVAL
Run the task only once within the specified interval (hours).

SYNTAX:
[get] interval
set interval <hours>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
hours - Time in hours (1 - 720 hours)

TYPE
Event triggered task.

SYNTAX:
[get] type
set type startup | startuponcedaily | dialup | engineupdate | appupdate | logon | detection

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
startup - Computer start
startuponcedaily - The first time the computer starts each day
dialup - Dial-up connection to the Internet/VPN
generateupdate - Virus signature update
appupdate - Program component update
logon - User logon
detection - Threat detection
6.2.70  Context - TOOLS SCHEDULER FAILSAFE
EXECUTE
Action to take if the task is not run.
SYNTAX:

```
[get] execute
      set execute asap | iftimeout | no
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status

ARGUMENTS:

- **asap** - Run the task as soon as possible
- **iftimeout** - Run the task immediately if the time since its last execution exceeds specified interval
- **no** - Do not run with delay

**NOTE:** To set a limit enter `SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT <HOURS>`.

TIMEOUT
Task interval (hours).
SYNTAX:

```
[get] timeout
      set timeout <hours>
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status

ARGUMENTS:

- **hours** - Time in hours (1 - 720 hours)

6.2.71  Context - TOOLS SCHEDULER PARAMETERS CHECK
LEVEL
Scan level.
SYNTAX:

```
[get] level
      set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status

ARGUMENTS:

- **before_logon** - Files run before user logon
- **after_logon** - Files run after user logon
- **most_frequent** - Only the most frequently used files
- **frequent** - Frequently used files
common - Commonly used files
rare - Rarely used files
all - Registered files

PRIORITY
Scan priority.
SYNTAX:
[get] priority
set priority [normal | low | lowest | idle]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
  normal - Normal
  low - Lower
  lowest - Lowest
  idle - When idle

6.2.72 Context - TOOLS SCHEDULER PARAMETERS EXTERNAL
ARGUMENTS
Arguments.
SYNTAX:
[get] arguments
set arguments <arguments>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
  arguments - Arguments

DIRECTORY
Work folder.
SYNTAX:
[get] directory
set directory <path>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
  path - Path

EXECUTABLE
Executable file.
SYNTAX:

[get] executable
set executable <path>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

path - Path

6.2.73 Context - TOOLS SCHEDULER PARAMETERS SCAN

PROFILE
Scan profile.

SYNTAX:

[get] profile
set profile <profile>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

profile - Profile name

READONLY
Scan without cleaning.

SYNTAX:

[get] readonly
set readonly disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

TARGET
Scan targets.

SYNTAX:

[get] | clear target
add | remove target <path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
clear - Removes all items/files

ARGUMENTS:
path - Scan path/Target

6.2.74 Context - TOOLS SCHEDULER PARAMETERS UPDATE

PRIMARY
Update profile.

SYNTAX:

[get] primary
set primary [<profile>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

profile - Profile name

SECONDARY
Alternate update profile.

SYNTAX:

[get] secondary
set secondary [<profile>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

profile - Profile name

6.2.75 Context - TOOLS SCHEDULER REPEAT

INTERVAL
Task interval (minutes).

SYNTAX:

[get] interval
set interval <minutes>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

minutes - Time in minutes (1 - 720 hours)
6.2.76 Context - TOOLS SCHEDULER STARTUP

DATE
Task will be run on the selected date.
SYNTAX:

\[ \text{get} \] date
\set date <year>-<month>-<day>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
year - Year
month - Month
day - Day

DAYS
Run the task on the following days.
SYNTAX:

\[ \text{get} \] days
\set | add | remove days none | [monday] [tuesday] [wednesday] [thursday] [friday] [saturday] [sunday] | all

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
add - Adds item
remove - Removes item

ARGUMENTS:
none - No specified day
monday - Monday
tuesday - Tuesday
wednesday - Wednesday
thursday - Thursday
friday - Friday
saturday - Saturday
sunday - Sunday
all - Every day

TIME
Task will be run at the selected time.
SYNTAX:

\[ \text{get} \] time
\set time <hour>:<minute>:<second>
OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status

ARGUMENTS:

- hour - Hour
- minute - Minute
- second - Second

6.2.77 Context - UPDATE

CACHE

Clear update cache.

SYNTAX:

clear cache

COMPONENTS

Update program components.

SYNTAX:

[get] | restore components
set components never | allways | ask

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- never - Do not update
- allways - Always update
- ask - Ask before downloading program components

LOGIN

Login username.

SYNTAX:

[get] | restore login
set login [<string>]

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- string - Name

NOTE: Please enter the Username and Password received after purchase or activation. We strongly recommend that you copy (Ctrl+C) from your registration email and paste it (Ctrl+V).
Password.

SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:

get - Show password
set - Set of delete password
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to enter password as parameter
password - Password

NOTE: Please enter the Username and Password received after purchase or activation. We strongly recommend that you copy (Ctrl+C) from your registration email and paste it (Ctrl+V).

PRERELEASE

Enable pre-release updates.

SYNTAX:

[get] | restore prerelease
set prerelease disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

PROFILE

Update profile management.

SYNTAX:

[get] profile
select | remove profile <name>
add profile new: <name> [copyfrom: <name>]

OPERATIONS:

get - Returns current setting/status
select - Selects item
add - Add item
remove - Removes item

ARGUMENTS:

name - Profile name
new - New profile
copyfrom - Copy setting from profile
NOTE: Other context commands refer to the active profile (marked with - x). For the active profile selection use select update profile <profile name>.

SERVER
Update servers.

SYNTAX:

[get] | restore server
select | add | remove server <server>

OPERATIONS:

get - Returns current setting/status
select - Selects item
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:

server - Server address

STATUS
Show update status.

SYNTAX:

[get] status

UPDATE
Update.

SYNTAX:

start | stop update

OPERATIONS:

start - Run update
stop - Cancel update

6.2.78 Context - UPDATE CONNECTION

DISCONNECT
Disconnect from server after update.

SYNTAX:

[get] | restore disconnect
set disconnect disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
LOGIN
Username.
SYNTAX:

[get] | restore login
set login [<string>]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Name

PASSWORD
Password.
SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:
get - Show password
set - Set or delete password
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to enter password as parameter
password - Password

RUNAS
Connect to LAN as.
SYNTAX:

[get] | restore runas
set runas system | current | specified

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

system - System account (default)
current - Current user
specified - Specified user
6.2.79 Context - UPDATE MIRROR

COMPONENTS
Update program components.

SYNTAX:

[get] | start | restore components
set components disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
start - Start update
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FOLDER
Folder to store mirrored files.

SYNTAX:

[get] | restore folder
set folder [string]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
string - Folder path

LOGIN
Username.

SYNTAX:

[get] | restore login
set login [string]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
string - Name

PASSWORD
Password.

SYNTAX:
[get] | restore password

set password [plain <password>]

OPERATIONS:
get - Show password
set - Set or delete password
restore - Restores default settings/object/file

ARGUMENTS:
plain - Switch to enter password as parameter
password - Password

USE
Create update mirror.

SYNTAX:
[get] | restore use

set use disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

VERSIONS
Update version management.

SYNTAX:
[get] | restore versions

select versions <version>

OPERATIONS:
get - Show available versions
select - Select/Deselect update version
restore - Restores default settings/object/file

ARGUMENTS:
version - Version name
6.2.80  Context - UPDATE MIRROR SERVER

AUTHENTICATION

Use authentication.

SYNTAX:

[get] | restore authentication
set authentication none | basic | ntlm

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

none - No
basic - Basic
ntlm - NTLM

PORT

Port.

SYNTAX:

[get] | restore port
set port <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Port number

USE

Provide update files via internal HTTP server.

SYNTAX:

[get] | restore use
set use disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
6.2.81 Context - UPDATE NOTIFICATION

DOWNLOAD

Ask before downloading update.

SYNTAX:

[get] | restore download
set download disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HIDE

Do not display notification about successful update.

SYNTAX:

[get] | restore hide
set hide disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SIZE

Ask if an update file is greater than (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - File size (kB)

NOTE: To disable update notifications enter 0.
6.2.82 Context - UPDATE PROXY

LOGIN
Username.

SYNTAX:

[get] | restore login
set login [<<string>>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Name

MODE
HTTP proxy setup.

SYNTAX:

[get] | restore mode
set mode global | noproxy | userdefined

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

global - Use global proxy server settings
noproxy - Do not use proxy server
userdefined - Connection through a proxy server

PASSWORD
Password.

SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:

get - Show password
set - Set or delete password
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to enter password as parameter
password - Password

PORT
Proxy server port.
SYNTAX:
  [get] | restore port
  set port <number>

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  number - Port number

SERVER
Proxy server.

SYNTAX:
  [get] | restore server
  set server [<string>]

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  string - Server address

6.2.83  Context - UPDATE SYSTEM

NOTIFY
Notify about missing updates from level.

SYNTAX:
  [get] | restore notify
  set notify no | optional | recommended | important | critical

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  no - No
  optional - Optional
  recommended - Recommended
  important - Important
  critical - Critical

RESTART
Restart computer after program component update.

SYNTAX:
[get] | restore restart

set restart never | ask | auto

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

never - Do not restart
ask - Ask before restart
auto - Restart automatically
7. Help and support

ESET Mail Security contains troubleshooting tools and support information that will assist you in solving such problems.

Help and support

Open help - Click this link to launch the ESET Mail Security help pages

Find quick solution - Select this option to find solutions to the most frequently encountered problems. We recommend that you read through this section before contacting technical support.

Search Internet knowledgebase - The Internet knowledgebase contains answers to the most frequently asked questions and recommended solutions for various issues. Regular updating by ESET's technical specialists makes the knowledge base the most powerful tool for resolving various types of problems.

About ESET Mail Security - Displays a summary of information about ESET Mail Security.

Customer Care - Direct contact to ESET's Customer Care support specialists.

Customer Care support request (recommended) - If you can't find an answer to your problem, please contact our customer care support specialists using the form available directly from ESET Mail Security. This service will provide the fastest answer to your requests, as technical data from the program are automatically submitted along with your query.

Customer Care support request (web form) - If you could not find an answer to your problem, you can use the form on ESET's website to quickly contact our Customer Care department.

7.1 About ESET Mail Security

The system information provides details about the installed version of ESET Mail Security, the installed system components and your license expiration date. At the bottom, you can find information about the operating system and system resources.

7.2 Troubleshooting

The first step in the process of contacting the Customer Care department is to use the support form. Enter the contact information and description of the problem from the customer's point of view. In the upper part of the window, please fill in your First name, Last name and a Contact email. This data identifies you as our customer and provides us with a reply-to address for our Customer Care representatives. To verify, enter the email address again. In the Issue type field, select the area of your problem (antivirus, firewall, infiltration issue, etc.). Then, please fill in the Subject of your request, which should correspond to the given problem. The lower part of the window consists of the Question or issue description area. This area allows you to describe your problem in detail, or to formulate your question for the Customer Care department. Click Next to proceed to the next step.

7.3 Selection of data to submit

This window allows you to select the type of computer information that will be submitted with the description of your problem. We strongly recommend that you leave all options enabled:

- **Send ESET Mail Security program configuration:** Enables submission of all program settings (equivalent of Setup > Import/Export settings).

- **Send detailed information about the system and running processes (SysInspector):** Submits a list of processes currently running on the system. We recommend submitting this information if you suspect your computer has been infected, or if it exhibits abnormal behavior.

- **Send registry data:** Enables submission of the operating system registry. We recommend submitting this information if you suspect your computer has been infected, or if it exhibits abnormal behavior.

- **Send standard system information:** Enables submission of information about the operating system and hardware installed.

The Attachment section allows you to add an attachment if it is relevant to your query (e.g., if you want to send a screen shot or suspicious file to technical support). If you wish to see the data that will be submitted, select the Look at
and confirm before submitting option. Click Next to proceed to the next window.

### 7.4 Confirmation and submitted data

If you selected the Display submitted data before data with confirmation checkbox in the previous step, all submitted data will be displayed in the xml tree structure. Click Next to proceed to the last dialog window.

### 7.5 Finish

The last step in submitting a query. Click Finish to submit your query to ESET's Customer Care department.

### 7.6 Support wait

If you confirm submitting information to ESET Customer Care, ESET Sysinspector will start generating a new system snapshot that will be included in your support query. Please allow a few seconds for the log to be created (the required time may vary depending on the hardware configuration and applications installed on the system).
8. Glossary

8.1 Types of infiltration

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

8.1.1 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.

8.1.2 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.

8.1.3 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—oday, 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

### 8.1.4 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 Mail Security users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

### 8.1.5 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.

### 8.1.6 Spyware

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

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

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

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.
8.1.7 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 Mail Security 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 (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.

8.1.8 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

8.2 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
8.2.1 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.

8.2.2 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.

8.2.3 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.

8.3 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.
8.3.1 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. Action: Delete the message.
- Condition: An incoming email message contains an attachment with an .exe extension. Action: Delete the attachment and deliver the message to the mailbox.
- Condition: An incoming email message arrives from your employer. 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.

8.3.2 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.

8.3.3 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. 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.

8.3.4 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 recommend you use both a whitelist and a blacklist to most effectively filter spam.
8.3.5 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.