ESET GATEWAY SECURITY

Copyright ©2013 by ESET, spol. s r.o.
ESET Gateway Security was developed by ESET, spol. s r.o.

For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced,
stored in a retrieval system or transmitted in any form or by any means,
electronic, mechanical, photocopying, recording, scanning, or otherwise
without permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described
application software without prior notice.

Customer Care: www.eset.com/support

REV. 4/16/2013
3. Work with ESET Gateway Security

3.1 ESET Gateway Security - Server protection

3.1.1 Microsoft Forefront TMG protection
3.1.1.1 HTTP
3.1.1.2 FTP
3.1.1.3 SMTP
3.1.1.4 POP3
3.1.1.5 IMAP
3.1.1.6 Rules
3.1.1.7 Logs
3.1.1.8 Performance
3.1.1.9 Antivirus and antispyware protection
3.1.1.10 Microsoft Forefront TMG protection
3.1.1.11 Analysis
3.1.1.12 Samples
3.1.1.13 SpamCompiler
3.1.1.14 List of cache memory files
3.1.1.15 Training
3.1.1.16 Rules
3.1.1.17 Rule weight
3.1.1.18 Add rule weight
3.1.1.19 List of downloaded rule files
3.1.1.20 Category weight
3.1.1.21 Add category weight
3.1.1.22 Custom rules list
3.1.1.23 Filtering
3.1.1.24 Allowed senders
3.1.1.25 Blocked senders
3.1.1.26 Allowed IP addresses
3.1.1.27 Ignored IP addresses
3.1.1.28 Blocked IP addresses
3.1.1.29 Allowed domains
3.1.1.30 Ignored domains
3.1.1.31 Blocked domains
3.1.1.32 Verification
3.1.1.33 RBL (Realtime Blackhole List)
3.1.1.34 List of RBL servers
3.1.1.35 LBL (Last Blackhole List)
3.1.1.36 List of LBL servers
3.1.1.37 List of skipped IP addresses
3.1.1.38 DNSBL (DNS Block List)
3.1.1.39 List of DNSBL servers
1. Introduction

ESET Gateway Security is an integrated solution specially designed for Microsoft Forefront Threat Management Gateway (TMG) or Internet Security and Acceleration Server (ISA) running on Microsoft Windows Server. It delivers effective and robust protection against various types of malware attacks and spam.

ESET Gateway Security provides three types of protection: Antivirus and Antispyware as well as Antispam.

Some key features of ESET Gateway Security:

- **Automatic Exclusions** – automatic detection and exclusion of critical server files for smooth operation.
- **eShell** (ESET Shell) - new command line control interface that could offer advanced users and administrators more comprehensive options for management of ESET products.
- **SelfDefense** – technology that protects ESET security solutions from being modified or deactivated.
- **Effective Troubleshooting** – with inbuilt advanced tools for resolving various issues: ESET SysInspector for system diagnostics and ESET SysRescue to create a bootable rescue CD.


1.1 System requirements

Operating Systems:

- Microsoft Windows Server 2003 (x86) SP1 SP2
- Microsoft Windows Server 2003 R2 (x86) SP1 SP2
- Microsoft Windows Server 2008 (x64) SP2
- Microsoft Windows Server 2008 R2 (x64) SP1

and either one of the following server application:

- Microsoft Internet Security and Acceleration (ISA) 2006 SP1
- Microsoft Forefront Threat Management Gateway (TMG) 2010 SP1 SP2

Hardware requirements depend on the operating system version in use. We recommend reading the Microsoft Windows Server product documentation for more detailed information on hardware requirements.

**NOTE:** we strongly recommend using the latest service pack on Microsoft server operating system as well as server application. Also, we advise to have the system updated with the latest hotfixes / windows updates.

1.2 Types of protection

There are three types of protection:

- **Antivirus protection**
- **Antispyware protection**
- **Antispam protection**

Antivirus and Antispyware protection is one of the basic functions of the ESET Gateway Security product. This 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 **quarantine**.

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 User interface

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

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

Once you press F5, the advanced setup tree window opens and displays a list of configurable program features. From this window, you can configure the settings and options based on your needs. The tree structure is split into two sections: Server protection and Computer protection. The Computer protection section contains the configurable items for the protection of the server itself.
2. Installation

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

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

There are two ways to execute the installer:

- You can login locally using Administrator account credentials and simply run the installer
- You can be logged in as other user, but need to open command prompt with Run as... and type in Administrator account credentials to have the cmd running as Administrator, then type in the command to execute the installer (e.g. msiexec /i egsp_nt64_ENU.msi but you need to replace egsp_nt64_ENU.msi with the exact file name of the msi installer you have downloaded)

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

1. Typical Installation
2. Custom Installation

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

NOTE: In case you are performing the installation in an array environment, then ESET Gateway Security must be installed on each array member separately. This is necessary for the configuration to be consistent. If you decide to uninstall ESET Gateway Security from one or more array members, then you also need to uninstall ESET Gateway Security from the rest of the array members. Simply said ESET Gateway Security needs to be either installed on all the array members or uninstalled from all the array members. Otherwise the configuration will not be consistent and thus may cause problems.
2.1 Typical Installation

Typical installation mode quickly installs ESET Gateway 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 yet. After ESET Gateway Security has been installed on your system, you can modify the options and configuration settings at any time. This user guide describes these settings and functionality in detail. The Typical installation mode settings provide excellent security coupled with ease of use and high system performance.

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

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

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

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

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

These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.

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

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

2.2 Custom Installation

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

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

Next, enter your Username and Password. This step is the same as the Typical installation mode step (see “Typical installation”).

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

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

If you use a proxy server, it must be correctly configured for virus signature updates to work correctly. If you would like to have the proxy server configured automatically, select the default setting I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer (Recommended) and click Next. If you do not use a proxy server, select the I do not use a proxy server option.
If you prefer to enter the proxy server details yourself, you can configure the proxy server settings manually. To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address** field. In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). If your proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. Once the proxy server details are entered, click **Apply** and confirm the selection.

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

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

**NOTE**: After a program component update, a restart is usually required. We recommend selecting the **Never restart computer** option. The latest component updates will come into effect after the next server restart (whether it is scheduled, manual or otherwise). You can choose **Offer computer restart if necessary** if you would like to be reminded to restart the server after the components were updated. With this setting, you can restart the server right away or postpone the restart and perform it at a later time.
The next installation window offers the option to set a password to protect your program settings. Select the **Protect configuration settings with a password** option and choose a password to enter in the **New password** and **Confirm new password** fields.

The next three installation steps, **ThreatSense.Net Early Warning System**, **Detection of potentially unwanted applications** and SharePoint administrator account credentials are the same as the Typical installation mode steps (see **Typical installation**). Click **Install** in the **Ready to install** window to complete installation.

### 2.3 Terminal Server

If you are installing ESET Gateway Security on Windows Server that acts as a Terminal Server, you might want to disable the ESET Gateway Security GUI to prevent it from starting up every time a user logs in. See **Disable GUI on Terminal Server** for specific steps to disable the GUI.

### 2.4 Upgrading to a newer version

Newer versions of ESET Gateway 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. **Manually upgrade with automatic deployment in a network environment by means of ESET Remote Administrator.**
2.5 On-demand computer scan

After installing ESET Gateway Security, a computer scan for malicious code should be performed. From the main program window, click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see section **On-demand computer scan**.
3. Work with ESET Gateway Security

3.1 ESET Gateway Security - Server protection

ESET Gateway Security provides protection for your server with essential functionalities such as: Antivirus and Antispyware, Resident shield (Real-time protection) and Antispyware protection. You can read more on each type of protection under the ESET Gateway Security - Computer protection section. Additionally, there is a feature called **Automatic exclusions**. This feature identifies critical server applications and server operating system files and automatically adds them to the list of **Exclusions**. This functionality will minimize the risk of potential conflicts and increase the overall performance of the server when running antivirus software.

3.1.1 Microsoft Forefront TMG protection

ESET Gateway Security scans traffic that passes through the Microsoft Forefront TMG or ISA server to your local network. The data that are being transferred via protocols (HTTP, FTP, SMTP, POP3, IMAP) are being scanned for potential viruses, malware or SPAM on particular ports. The traffic is then either passed untouched to its destination in case it is free from malicious code, or, if a virus, malware or SPAM is identified, it is being handled according to how ESET Gateway Security is configured. This is to avoid possible infiltration and thus prevent from any damage the infiltration may cause.

In this advanced setup tree, you can see the configuration of each component of ESET Gateway Security. In here, you are able to modify the configuration and fine-tune it. Under each main section, you can change settings for each protocol individually.

Option **Automatic protection for Microsoft Forefront Threat Management Gateway** or **Automatic protection for ISA server** let’s you enable or disable the protection. It is enabled by default, however if you deselect the check box the disable will be disabled. When disabled, the protection will not start during system startup, for example when you restart your server.

**NOTE:** **Automatic protection** is not available on Windows Server Enterprise editions. It can only be used on Standard editions.

3.1.1.1 HTTP

Option **Enable HTTP protection** allows for this type of protection to be used in Antivirus and antispyware module of ESET Gateway Security. HTTP traffic will then be scanned for infiltrations, malicious code or spam on a specified port. This functionality is enabled by default, however, if there is a reason for it, you can disable it. Once disabled, the HTTP protection will not be available in Antivirus and antispyware.

**NOTE:** If you disable this option, HTTP protection will not be available for you to use it in Antivirus and antispyware module (this setting will be grayed out).

**NOTE:** When using different ports than standard ones, make sure these ports are defined in the Forefront TMG or ISA server, otherwise it won't work.

3.1.1.2 FTP

Option **Enable FTP protection** allows for this type of protection to be used in Antivirus and antispyware module of ESET Gateway Security. FTP traffic will then be scanned for infiltrations, malicious code or spam on a specified port. This functionality is enabled by default, however, if there is a reason for it, you can disable it. Once disabled, the FTP protection will not be available in Antivirus and antispyware.

**NOTE:** If you disable this option, FTP protection will not be available for you to use it in Antivirus and antispyware module (this setting will be grayed out).

**NOTE:** When using different ports than standard ones, make sure these ports are defined in the Forefront TMG or ISA server, otherwise it won't work.
3.1.1.3 SMTP

Option **Enable SMTP protection** allows for this type of protection to be used in a number of ESET Gateway Security modules. SMTP traffic will then be scanned for infiltrations, malicious code or spam on a specified port. This functionality is enabled by default, however, if there is a reason for it, you can disable it. Once disabled, the SMTP protection will not be available in Antivirus and antispyware nor in Antispam protection.

**NOTE:** If you disable this option, SMTP protection will not be available in any other ESET Gateway Security modules. You will not be able to use it in Antivirus and antispyware nor in Antispam protection (this setting will be grayed out).

**NOTE:** If you disable this option, SMTP protection will not be available in any other ESET Gateway Security modules. You will not be able to use it in Antivirus and antispyware nor in Antispam protection (this setting will be grayed out).

**NOTE:** When using different ports than standard ones, make sure these ports are defined in the Forefront TMG or ISA server, otherwise it won't work.

3.1.1.4 POP3

Option **Enable POP3 protection** allows for this type of protection to be used in a number of ESET Gateway Security modules. POP3 traffic will then be scanned for infiltrations, malicious code or spam on a specified port. This functionality is enabled by default, however, if there is a reason for it, you can disable it. Once disabled, the POP3 protection will not be available in Antivirus and antispyware nor in Antispam protection.

**NOTE:** If you disable this option, POP3 protection will not be available in any other ESET Gateway Security modules. You will not be able to use it in Antivirus and antispyware nor in Antispam protection (this setting will be grayed out).

**NOTE:** When using different ports than standard ones, make sure these ports are defined in the Forefront TMG or ISA server, otherwise it won't work.

3.1.1.5 IMAP

Option **Enable IMAP protection** allows for this type of protection to be used in a number of ESET Gateway Security modules. IMAP traffic will then be scanned for infiltrations, malicious code or spam on a specified port. This functionality is enabled by default, however, if there is a reason for it, you can disable it. Once disabled, the IMAP protection will not be available in Antivirus and antispyware nor in Antispam protection.

**NOTE:** If you disable this option, IMAP protection will not be available in any other ESET Gateway Security modules. You will not be able to use it in Antivirus and antispyware nor in Antispam protection (this setting will be grayed out).

**NOTE:** When using different ports than standard ones, make sure these ports are defined in the Forefront TMG or ISA server, otherwise it won't work.

3.1.1.6 Rules

The **Rules** menu item allows you to manually define your own rules for each protocol that is available. Rules feature is very useful when you want to configure what exactly should be scanned, on what ports, and what action should be taken in case the file or email message matches the rule criteria such as file name, file size or message size.

In this window, you can see a list of existing rules, provided they were previously defined (there are no rules by default). To add new rule, click on **Add...** button which will open a rule creation wizard. In case you wish to modify an existing rule, select the rule from the list and click **Edit...**, you will get the same wizard as when creating new rule. However the wizard already contain previous settings of the particular rule and allows you to modify it in the same wizard form. To delete an existing rule, simply select the rule you want to delete and click **Remove** button. To change an order in which the rules are arranged and processed, use **Move up** or **Move down** buttons.

The rules list consists of three columns:

- **Rule** - a rule name
- **Protocol** - protocol for which the rule applies
- **Count** - the number of times the rule was applied since the ESET Gateway Security was installed, or since last time the button Reset was pressed

Buttons to manage rules:
Add... - opens a wizard
Edit... - edits existing rule in a wizard form
Remove - deletes existing rule
Reset - resets the rule counter (Count column)
Move up - changes rule order in upward direction
Move down - changes rule order in downward direction

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

If Synchronized write without the use of cache is enabled, all the log entries will be immediately written in the log file without being stored in the log cache. By default, ESET Gateway Security components running in the Forefront TMG or ISA 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.

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

3.1.1.8 Performance
In this section, you can define a folder to store temporary files in, in order to improve program’s performance. If no folder is specified, ESET Gateway 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 system drive or the drive on which Forefront TMG or ISA server is installed. We strongly recommend that you avoid assigning the Temporary folder to removable media such as floppy disk, USB, DVD, etc. Also, to further increase performance, you can use logical drive located on a physical RAID array (preferably RAID O, RAID 5 or one of the nested RAID levels, such as O+1, 1+O, etc.) attached directly to the server or connected via Fibre Channel.

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

3.1.2 Antivirus and antispyware protection
Antivirus protection guards against malicious system attacks. 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.

3.1.2.1 Microsoft Forefront TMG protection
In this section, you can enable or disable Antivirus and antispyware protection for Microsoft Forefront TMG or ISA server. It is enabled by default, but if there is as reason for it and you wish to have it disabled, you do so. However, we strongly recommend you to leave it enabled.

Enable antivirus and antispyware Microsoft Forefront Threat Management Gateway protection - When enabled, you can configure ThreatSense engine settings after pressing Setup... button.
### 3.1.2.1.1 HTTP

**Enable antivirus and antispyware HTTP protection** - When enabled, you can configure ThreatSense engine settings after pressing Setup... button.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an **Action to perform on uncleaned threat** to:

- **Continue with the connection** - Let the session continue despite the fact there was a threat detected and not cleaned. However, if it the session will continue there is some possibility that the user might get an infiltration. Therefore we recommend you to use one of the following two options instead.

- **Reject connection** - It will reject connection and send a response to the user. You can press Setup... button to configure whether a Default response is used in case a connection is refused or a Custom response file (in HTML format).

- **Disconnect** - It will immediately disconnect the session without any notice.

**NOTE:** If you see this option as grayed out, you need to enable HTTP protection for the whole system first. Go to Server protection > Microsoft Forefront Threat Management Gateway > HTTP and select option Enable HTTP protection. Go back to Antivirus and antispyware section and you will be able to configure HTTP protection or change its settings.

**NOTE:** In case you use Reject connection with custom response, and the custom page is not being displayed, it might be due to the file permissions. You will need to give local user group Users read permission (at least) to your custom HTML file. If it is still not working, set the read permissions for Network Service (NT AUTHORITY\NETWORK SERVICE) account manually.

### 3.1.2.1.2 FTP

**Enable antivirus and antispyware FTP protection** - When enabled, you can configure ThreatSense engine settings after pressing Setup... button.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an **Action to perform on uncleaned threat** to:

- **Continue with the connection** - Let the session continue despite the fact there was a threat detected and not cleaned. However, if it the session will continue there is some possibility that the user might get an infiltration. Therefore we recommend you to use one of the following two options instead.

- **Reject connection** - It will reject connection and send a response to the user. You can press Setup... button to configure RFC reply code, which means what response will be sent in case a connection is refused.

- **Disconnect** - It will immediately disconnect the session without any notice.

**NOTE:** If you see this option as grayed out, you need to enable FTP protection for the whole system first. Go to Server protection > Microsoft Forefront Threat Management Gateway > FTP and select option Enable FTP protection. Go back to Antivirus and antispyware section and you will be able to configure FTP protection or change its settings.

### 3.1.2.1.3 SMTP

**Enable antivirus and antispyware SMTP protection** - When enabled, you can configure ThreatSense engine settings after pressing Setup... button.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an **Action to perform on uncleaned threat** to:

- **Continue with the connection** - Let the session continue despite the fact there was a threat detected and not cleaned. However, if it the session will continue there is some possibility that the user might get an infiltration. Therefore, we recommend you to use the other option instead.

- **Reject connection with a reply** - It will reject connection and send a response to the user. You can press Setup... button to configure RFC reply code, which means what response will be sent in case a connection is refused.

**NOTE:** If you see this option as grayed out, you need to enable SMTP protection for the whole system first. Go to Server protection > Microsoft Forefront Threat Management Gateway > SMTP and select option Enable SMTP protection. Go back to Antivirus and antispyware section and you will be able to configure SMTP protection or change its settings.
3.1.2.1.4 POP3

**Enable antivirus and antispyware POP3 protection** - When enabled, you can configure ThreatSense engine settings after pressing Setup... button.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an Action to perform on uncleaned threat to:

- **Continue with the connection** - Let the session continue despite the fact there was a threat detected and not cleaned. However, if it the session will continue there is some possibility that the user might get an infiltration. Therefore, we recommend you to use the other option instead.
- **Reject connection with a reply** - It will reject connection and send a response to the user. You can press Setup... button to configure whether a Default response is used in case a connection is refused or a Custom response (enter your text in the text box).

**NOTE**: If you see this option as grayed out, you need to enable POP3 protection for the whole system first. Go to **Server protection > Microsoft Forefront Threat Management Gateway > POP3** and select option **Enable POP3 protection**. Go back to Antivirus and antispyware section and you will be able to configure POP3 protection or change its settings.

3.1.2.1.5 IMAP

**Enable antivirus and antispyware IMAP protection** - When enabled, you can configure ThreatSense engine settings after pressing Setup... button.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an Action to perform on uncleaned threat to:

- **Continue with the connection** - Let the session continue despite the fact there was a threat detected and not cleaned. However, if it the session will continue there is some possibility that the user might get an infiltration. Therefore, we recommend you to use the other option instead.
- **Reject connection with a reply** - It will reject connection and send a response to the user. You can press Setup... button to configure whether a Default response is used in case a connection is refused or a Custom response (enter your text in the text box).

**NOTE**: If you see this option as grayed out, you need to enable IMAP protection for the whole system first. Go to **Server protection > Microsoft Forefront Threat Management Gateway > IMAP** and select option **Enable IMAP protection**. Go back to Antivirus and antispyware section and you will be able to configure IMAP protection or change its settings.

3.1.2.1.6 Actions

This functionality concerns email messages. You can set some actions when an email message has been scanned.

- **Write ID to the header of scanned messages** - If this option is enabled, then an ID is written to a header of a message after it was scanned.

- **Write information about taken action to the header of scanned messages** - If enabled, Antivirus protection engine writes an information what action was taken with the message.

3.1.2.1.7 Alerts and notifications

*Under construction*. This topic is being worked on and will be available with future releases.
3.1.2.2 Automatic exclusions

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

ESET Gateway 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 enabled (by default) by checking the appropriate box or disabled by unchecking it, with the following result:

1) If an application/operating system exclusion remains enabled, any of its critical files and folders will be added to the list of files excluded from scanning (Advanced setup > Computer protection > Antivirus and antispyware > Exclusions). Every time the server is restarted, the system performs an automatic check of exclusions and restores any exclusions that may have been deleted from the list. This is the recommended setting, if you wish to make sure the recommended Automatic exclusions are always applied.

2) If the user disables an application/operating system exclusion, its critical files and folders remain on the list of files excluded from scanning (Advanced setup > Computer protection > Antivirus and antispyware > Exclusions). However, they will not be automatically checked and renewed on the Exclusions list every time the server is restarted (see point 1 above). We recommend this setting for advanced users, who wish to remove or modify some of the standard exclusions. If you wish to have removed the exclusions from the list without restarting the server, you will need to remove them manually from the list (Advanced setup > Computer protection > Antivirus and antispyware > Exclusions).

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

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

http://support.microsoft.com/kb/822358
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166

3.1.3 Antispam protection

In the Antispam protection section, you can enable or disable spam protection for the traffic (specifically email messages) that goes to your mail server. You can configure antispam engine parameters and set other levels of protection.

NOTE: It is necessary that the Antispam database is being updated regularly in order for the Antispam module to provide the best possible protection. To allow for correct regular updates of Antispam database, you will need to make sure that ESET Gateway 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, mirrors cannot be used for Antispam database updates. For proper functioning of Antispam database updates, ESET Gateway Security needs to have access to IP addresses listed in the above mentioned KB article. Without access to these IP's, Antispam module will not be able to provide most accurate results, thus the best possible protection.
3.1.3.1 Microsoft Forefront TMG protection

In this section, you can enable or disable Antispam protection for Microsoft Forefront TMG or ISA server. It is enabled by default, but if there is a reason for it and you wish to have it disabled, you can do so. However, we strongly recommend you to leave it enabled.

Enable Microsoft Forefront Threat Management Gateway antispam protection - When enabled, you can configure Antispam engine parameters after pressing **Setup...** button.

3.1.3.1.1 Antispam engine parameter setup

3.1.3.1.1.1 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.

**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.

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

**Preffered 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.

### 3.1.3.1.1.2 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.

### 3.1.3.1.1.3 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 -

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.

Set rule file indexes which should be downloaded to disk. Use Add, Edit and Remove buttons to manage rule file indexes.

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:

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.
3.1.3.1.4 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.

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.

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.

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.

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

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.

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

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

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

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.
3.1.3.1.5 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)

**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 maxcount IP addresses) multiplied by the number of RBL servers specified in RBL list. If the value is "O" 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 |

**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 |

**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:

<table>
<thead>
<tr>
<th>Address</th>
<th>Response</th>
<th>Score</th>
</tr>
</thead>
</table>

3.1.3.1.6 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.

3.1.3.1.7 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.

3.1.3.1.8 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.
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.

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.

### 3.1.3.1.1.9 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.

### 3.1.3.1.1.10 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 disabling 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.
3.1.3.1.11 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.

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
Bulgarian bg
Catalan ca
Czech cs
Welsh cy
Danish da
German de
Greek el
English en
Esperanto eo
Spanish es
Estonian et
Basque eu
Persian fa
Finnish fi
French fr
Frisian fy
Irish ga
Gaelic gd
Hebrew he
Hindi hi
Croatian hr
Hungarian hu
Armenian hy
Indonesian id
Icelandic is
Italian it
Japanese ja
Georgian ka
Korean ko
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 Name</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFGHANISTAN</td>
<td>AF</td>
</tr>
<tr>
<td>ÁLAND ISLANDS</td>
<td>AX</td>
</tr>
<tr>
<td>ALBANIA</td>
<td>AL</td>
</tr>
<tr>
<td>ALGERIA</td>
<td>DZ</td>
</tr>
<tr>
<td>AMERICAN SAMOA</td>
<td>AS</td>
</tr>
<tr>
<td>ANDORRA</td>
<td>AD</td>
</tr>
<tr>
<td>ANGOLA</td>
<td>AO</td>
</tr>
<tr>
<td>ANGUILLA</td>
<td>AI</td>
</tr>
<tr>
<td>ANTARCTICA</td>
<td>AQ</td>
</tr>
<tr>
<td>ANTIGUA AND BARBUDA</td>
<td>AG</td>
</tr>
<tr>
<td>ARGENTINA</td>
<td>AR</td>
</tr>
<tr>
<td>ARMENIA</td>
<td>AM</td>
</tr>
<tr>
<td>ARUBA</td>
<td>AW</td>
</tr>
<tr>
<td>AUSTRALIA</td>
<td>AU</td>
</tr>
<tr>
<td>AUSTRIA</td>
<td>AT</td>
</tr>
<tr>
<td>AZERBAIJAN</td>
<td>AZ</td>
</tr>
<tr>
<td>BAHAMAS</td>
<td>BS</td>
</tr>
<tr>
<td>BAHRAIN</td>
<td>BH</td>
</tr>
<tr>
<td>BANGLADESH</td>
<td>BD</td>
</tr>
<tr>
<td>BARBADOS</td>
<td>BB</td>
</tr>
<tr>
<td>BELARUS</td>
<td>BY</td>
</tr>
<tr>
<td>BELGIUM</td>
<td>BE</td>
</tr>
<tr>
<td>BELIZE</td>
<td>BZ</td>
</tr>
<tr>
<td>BENIN</td>
<td>BJ</td>
</tr>
<tr>
<td>BERMUDA</td>
<td>BM</td>
</tr>
<tr>
<td>Country</td>
<td>Code</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>BHUTAN</td>
<td>BT</td>
</tr>
<tr>
<td>BOLIVIA</td>
<td>BO</td>
</tr>
<tr>
<td>BOSNIA AND HERZEGOVINA</td>
<td>BA</td>
</tr>
<tr>
<td>BOTSWANA</td>
<td>BW</td>
</tr>
<tr>
<td>BOUVET ISLAND</td>
<td>BV</td>
</tr>
<tr>
<td>BRAZIL</td>
<td>BR</td>
</tr>
<tr>
<td>BRITISH INDIAN OCEAN TERRITORY</td>
<td>IO</td>
</tr>
<tr>
<td>BRUNEI DARUSSALAM</td>
<td>BN</td>
</tr>
<tr>
<td>BULGARIA</td>
<td>BG</td>
</tr>
<tr>
<td>BURKINA FASO</td>
<td>BF</td>
</tr>
<tr>
<td>BURUNDI</td>
<td>BI</td>
</tr>
<tr>
<td>CAMBODIA</td>
<td>KH</td>
</tr>
<tr>
<td>CAMEROON</td>
<td>CM</td>
</tr>
<tr>
<td>CANADA</td>
<td>CA</td>
</tr>
<tr>
<td>CAPE VERDE</td>
<td>CV</td>
</tr>
<tr>
<td>CAYMAN ISLANDS</td>
<td>KY</td>
</tr>
<tr>
<td>CENTRAL AFRICAN REPUBLIC</td>
<td>CF</td>
</tr>
<tr>
<td>CHAD</td>
<td>TD</td>
</tr>
<tr>
<td>CHILE</td>
<td>CL</td>
</tr>
<tr>
<td>CHINA</td>
<td>CN</td>
</tr>
<tr>
<td>CHRISTMAS ISLAND</td>
<td>CX</td>
</tr>
<tr>
<td>Cocos (Keeling) Islands</td>
<td>CC</td>
</tr>
<tr>
<td>COLOMBIA</td>
<td>CO</td>
</tr>
<tr>
<td>COMOROS</td>
<td>KM</td>
</tr>
<tr>
<td>CONGO</td>
<td>CG</td>
</tr>
<tr>
<td>CONGO, THE DEMOCRATIC REPUBLIC</td>
<td>CD</td>
</tr>
<tr>
<td>THE</td>
<td></td>
</tr>
<tr>
<td>COOK ISLANDS</td>
<td>CK</td>
</tr>
<tr>
<td>COSTA RICA</td>
<td>CR</td>
</tr>
<tr>
<td>Côte d’IVOIRE</td>
<td>CI</td>
</tr>
<tr>
<td>CROATIA</td>
<td>HR</td>
</tr>
<tr>
<td>CUBA</td>
<td>CU</td>
</tr>
<tr>
<td>CYPRUS</td>
<td>CY</td>
</tr>
<tr>
<td>CZECH REPUBLIC</td>
<td>CZ</td>
</tr>
<tr>
<td>DENMARK</td>
<td>DK</td>
</tr>
<tr>
<td>DJIBOUTI</td>
<td>DJ</td>
</tr>
<tr>
<td>DOMINICA</td>
<td>DM</td>
</tr>
<tr>
<td>DOMINICAN REPUBLIC</td>
<td>DO</td>
</tr>
<tr>
<td>ECUADOR</td>
<td>EC</td>
</tr>
<tr>
<td>EGYPT</td>
<td>EG</td>
</tr>
<tr>
<td>EL SALVADOR</td>
<td>SV</td>
</tr>
<tr>
<td>EQUATORIAL GUINEA</td>
<td>GQ</td>
</tr>
<tr>
<td>ERITREA</td>
<td>ER</td>
</tr>
<tr>
<td>ESTONIA</td>
<td>EE</td>
</tr>
<tr>
<td>ETHIOPIA</td>
<td>ET</td>
</tr>
<tr>
<td>FALKLAND ISLANDS (MALVINAS)</td>
<td>FK</td>
</tr>
<tr>
<td>FAROE ISLANDS</td>
<td>FO</td>
</tr>
<tr>
<td>FIJI</td>
<td>FJ</td>
</tr>
<tr>
<td>FINLAND</td>
<td>FI</td>
</tr>
<tr>
<td>FRANCE</td>
<td>FR</td>
</tr>
<tr>
<td>FRENCH GUIANA</td>
<td>GF</td>
</tr>
<tr>
<td>FRENCH POLYNESIA</td>
<td>PF</td>
</tr>
<tr>
<td>FRENCH SOUTHERN TERRITORIES</td>
<td>TF</td>
</tr>
<tr>
<td>GABON</td>
<td>GA</td>
</tr>
<tr>
<td>GAMBIA</td>
<td>GM</td>
</tr>
<tr>
<td>GEORGIA</td>
<td>GE</td>
</tr>
<tr>
<td>GERMANY</td>
<td>DE</td>
</tr>
<tr>
<td>GHANA</td>
<td>GH</td>
</tr>
<tr>
<td>GIBRALTAR</td>
<td>GI</td>
</tr>
<tr>
<td>GREECE</td>
<td>GR</td>
</tr>
<tr>
<td>GREENLAND</td>
<td>GL</td>
</tr>
<tr>
<td>GRENADA</td>
<td>GD</td>
</tr>
<tr>
<td>Country</td>
<td>Code</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Guadeloupe</td>
<td>GP</td>
</tr>
<tr>
<td>Guam</td>
<td>GU</td>
</tr>
<tr>
<td>Guatemala</td>
<td>GT</td>
</tr>
<tr>
<td>Guinea</td>
<td>GN</td>
</tr>
<tr>
<td>Guinea-Bissau</td>
<td>GW</td>
</tr>
<tr>
<td>Guyana</td>
<td>GY</td>
</tr>
<tr>
<td>Haiti</td>
<td>HT</td>
</tr>
<tr>
<td>Heard Island and McDonald Islands</td>
<td>HM</td>
</tr>
<tr>
<td>Holy See (Vatican City State)</td>
<td>VA</td>
</tr>
<tr>
<td>Honduras</td>
<td>HN</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>HK</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>Iceland</td>
<td>IS</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Indonesia</td>
<td>ID</td>
</tr>
<tr>
<td>Iran, Islamic Republic of</td>
<td>IR</td>
</tr>
<tr>
<td>Iraq</td>
<td>IQ</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Italy</td>
<td>IT</td>
</tr>
<tr>
<td>Jamaica</td>
<td>JM</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Jordan</td>
<td>JO</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>KZ</td>
</tr>
<tr>
<td>Kenya</td>
<td>KE</td>
</tr>
<tr>
<td>Kiribati</td>
<td>KI</td>
</tr>
<tr>
<td>Korea, Democratic People's Republic of</td>
<td>KP</td>
</tr>
<tr>
<td>Korea, Republic of</td>
<td>KR</td>
</tr>
<tr>
<td>Kuwait</td>
<td>KW</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>KG</td>
</tr>
<tr>
<td>Lao People's Democratic Republic</td>
<td>LA</td>
</tr>
<tr>
<td>Latvia</td>
<td>LV</td>
</tr>
<tr>
<td>Lebanon</td>
<td>LB</td>
</tr>
<tr>
<td>Lesotho</td>
<td>LS</td>
</tr>
<tr>
<td>Liberia</td>
<td>LR</td>
</tr>
<tr>
<td>Libyan Arab Jamahiriya</td>
<td>LY</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>LI</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>LU</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>Country</td>
<td>Code</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------</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>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>Slovakia</td>
<td>SK</td>
</tr>
<tr>
<td>Slovenia</td>
<td>SI</td>
</tr>
<tr>
<td>Solomon Islands</td>
<td>SB</td>
</tr>
<tr>
<td>Somalia</td>
<td>SO</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Georgia and the South</td>
<td>GS</td>
</tr>
<tr>
<td>Sandwich Islands</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>LK</td>
</tr>
<tr>
<td>Sudan</td>
<td>SD</td>
</tr>
<tr>
<td>Suriname</td>
<td>SR</td>
</tr>
<tr>
<td>Svalbard and Jan Mayen</td>
<td>SJ</td>
</tr>
<tr>
<td>Swaziland</td>
<td>SZ</td>
</tr>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Country Name</td>
<td>Code</td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>SYRIAN ARAB REPUBLIC</td>
<td>SY</td>
</tr>
<tr>
<td>TAIWAN, PROVINCE OF CHINA</td>
<td>TW</td>
</tr>
<tr>
<td>TAJIKISTAN</td>
<td>TJ</td>
</tr>
<tr>
<td>TANZANIA, UNITED REPUBLIC OF</td>
<td>TZ</td>
</tr>
<tr>
<td>THAILAND</td>
<td>TH</td>
</tr>
<tr>
<td>TIMOR-LESTE</td>
<td>TL</td>
</tr>
<tr>
<td>TOGO</td>
<td>TG</td>
</tr>
<tr>
<td>TOKELAU</td>
<td>TK</td>
</tr>
<tr>
<td>TONGA</td>
<td>TO</td>
</tr>
<tr>
<td>TRINIDAD AND TOBAGO</td>
<td>TT</td>
</tr>
<tr>
<td>TUNISIA</td>
<td>TN</td>
</tr>
<tr>
<td>TURKEY</td>
<td>TR</td>
</tr>
<tr>
<td>TURKMENISTAN</td>
<td>TM</td>
</tr>
<tr>
<td>TURKS AND CAICOS ISLANDS</td>
<td>TC</td>
</tr>
<tr>
<td>TUVALU</td>
<td>TV</td>
</tr>
<tr>
<td>UGANDA</td>
<td>UG</td>
</tr>
<tr>
<td>UKRAINE</td>
<td>UA</td>
</tr>
<tr>
<td>UNITED ARAB EMIRATES</td>
<td>AE</td>
</tr>
<tr>
<td>UNITED KINGDOM</td>
<td>GB</td>
</tr>
<tr>
<td>UNITED STATES</td>
<td>US</td>
</tr>
<tr>
<td>UNITED STATES MINOR OUTLYING ISLANDS</td>
<td>UM</td>
</tr>
<tr>
<td>ISLANDS</td>
<td></td>
</tr>
<tr>
<td>URUGUAY</td>
<td>UY</td>
</tr>
<tr>
<td>UZBEKISTAN</td>
<td>UZ</td>
</tr>
<tr>
<td>VANUATU</td>
<td>VU</td>
</tr>
<tr>
<td>VATICAN CITY STATE (HOLY SEE)</td>
<td>VA</td>
</tr>
<tr>
<td>VENEZUELA</td>
<td>VE</td>
</tr>
<tr>
<td>VIET NAM</td>
<td>VN</td>
</tr>
<tr>
<td>VIRGIN ISLANDS, BRITISH</td>
<td>VG</td>
</tr>
<tr>
<td>VIRGIN ISLANDS, US</td>
<td>VI</td>
</tr>
<tr>
<td>WALLIS AND FUTUNA</td>
<td>WF</td>
</tr>
<tr>
<td>WESTERN SAHARA</td>
<td>EH</td>
</tr>
<tr>
<td>YEMEN</td>
<td>YE</td>
</tr>
<tr>
<td>ZAIRE (CONGO, THE DEMOCRATIC REPUBLIC OF THE)</td>
<td>CD</td>
</tr>
<tr>
<td>ZAMBIA</td>
<td>ZM</td>
</tr>
<tr>
<td>ZIMBABWE</td>
<td>ZW</td>
</tr>
</tbody>
</table>

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.

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.

3.1.3.1.12 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.
3.1.3.1.13 Statistics

**Turn on statistical data logging** - Logs IPs, 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.

3.1.3.1.14 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).

3.1.3.1.2 SMTP

**Enable antispam SMTP protection** - When enabled, antispam engine scans SMTP traffic and checks email messages during their transport looking for SPAM.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an Action to perform on unsolicited email to:

- **Continue with the connection and change the email subject** - Let the session continue despite the fact there was a message found which is potentially a SPAM. This means that an email which might be SPAM will be delivered to the user's mailbox. Therefore, we recommend you to use the other option instead. The only thing that will be changed is the subject of the email to notify user that this is a potential SPAM message.
- **Reject connection with a reply** - It will reject connection and send a response. You can press Setup... button to configure RFC reply code, which means what response will be sent in case a connection is refused.

**NOTE**: If you see this option as grayed out, you need to enable SMTP protection for the whole system first. Go to Server protection > Microsoft Forefront Threat Management Gateway > SMTP and select option Enable SMTP protection. Go back to Antivirus and antispyware section and you will be able to configure SMTP protection or change its settings.

3.1.3.1.3 POP3

**Enable antispam POP3 protection** - When enabled, antispam engine scans POP3 traffic and checks email messages during their transport looking for SPAM.

**Actions** - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an Action to perform on unsolicited email to:

- **Continue with the connection and change the email subject** - Let the session continue despite the fact there was a message found which is potentially a SPAM. This means that an email which might be SPAM will be delivered to the user's mailbox. Therefore, we recommend you to use the other option instead. The only thing that will be changed is the subject of the email to notify user that this is a potential SPAM message.
- **Reject connection with a reply** - It will reject connection and send a response. You can press Setup... button to configure whether a Default response is used in case a connection is refused or a Custom response (enter your text in the text box).

**NOTE**: If you see this option as grayed out, you need to enable POP3 protection for the whole system first. Go to Server protection > Microsoft Forefront Threat Management Gateway > POP3 and select option Enable POP3 protection. Go back to Antivirus and antispyware section and you will be able to configure POP3 protection or change its settings.
3.1.3.1.4 IMAP

Enable antispam IMAP protection - When enabled, antispam engine scans IMAP traffic and checks email messages during their transport looking for SPAM.

Actions - Here you can choose what should be done in case a threat is found and cannot be cleaned. You can set an Action to perform on unsolicited email to:

- **Continue with the connection and change the email subject** - Let the session continue despite the fact there was a message found which is potentially a SPAM. This means that an email which might be SPAM will be delivered to the user’s mailbox. Therefore, we recommend you to use the other option instead. The only thing that will be changed is the subject of the email to notify user that this is a potential SPAM message.

- **Reject connection with a reply** - It will reject connection and send a response. You can press Setup... button to configure whether a Default response is used in case a connection is refused or a Custom response (enter your text in the text box).

**NOTE**: If you see this option as grayed out, you need to enable IMAP protection for the whole system first. Go to Server protection > Microsoft Forefront Threat Management Gateway > IMAP and select option Enable IMAP protection. Go back to Antivirus and antispyware section and you will be able to configure IMAP protection or change its settings.

3.1.3.1.5 Alerts and notifications

*Under construction.* This topic is being worked on and will be available with future releases.

3.2 ESET Gateway Security - Computer protection

ESET Gateway Security has all of the necessary tools to ensure protection of the server as a computer. It provides significant protection for your server with following types of protection: Antivirus and Antispyware, Resident shield (Real-time protection) and Antispam protection.

3.2.1 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.

3.2.1.1 Real-time file system protection

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

3.2.1.1.1 Control setup

The Real-time file system protection checks all types of media, and control is triggered by various events. Using ThreatSense technology detection methods (as described in section ThreatSense engine parameter setup), real-time file system protection may vary for newly created files and existing files. For newly created files, it is possible to apply a deeper level of control.

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

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

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

Local drives – Controls all system hard drives

Removable media – Diskettes, USB storage devices, etc.

Network drives – Scans all mapped drives

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

3.2.1.1.2 Scan on (Event-triggered scanning)

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

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

3.2.1.1.3 Advanced scan options

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

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

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

### 3.2.1.1.2 Cleaning levels

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

- **The first level, No cleaning**, displays an alert window with available options for each infiltration found. You must choose an action for each infiltration individually. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

- **The default level** automatically chooses and performs a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a message located in the bottom right corner of the screen. Automatic actions are not performed when the infiltration is located within an archive (which also contains clean files) or when infected objects do not have a predefined action.

- **The third level, Strict cleaning**, is the most “aggressive” – all infected objects are cleaned. As this level could potentially result in the loss of valid files, we recommend that it be used only in specific situations.

![ThreatSense engine parameter setup](image)

### 3.2.1.1.3 When to modify real-time protection configuration

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

After the installation of ESET Gateway 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).

### 3.2.1.1.4 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a special harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file eicar.com is available for download at [http://www.eicar.org/download/eicar.com](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.
3.2.1.1.5 What to do if real-time protection does not work

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

**Real-time protection is disabled**

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

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

![ESET Gateway Security Setup](image)

**If Real-time protection does not detect and clean infiltrations**

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

**Real-time protection does not start**

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

If you suspect that your computer is infected (it behaves abnormally), run an On-demand computer scan to examine your computer for infiltrations. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. Regular scanning can detect infiltrations that were not detected by the real-time scanner when they were saved to the disk. This can happen if the real-time scanner was disabled at the time of infection, or if the virus signature database is not up-to-date.

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

3.2.1.2.1 Type of scan

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

3.2.1.2.1.1 Smart scan

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

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

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

3.2.1.2.2 Scan targets

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

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

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

**Local drives** – Selects all system hard drives

**Network drives** – Selects all mapped drives

**No selection** – Cancels all selections

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

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

To create a new profile, open the Advanced Setup window (F5) and click On-demand computer scan > Profiles... The Configuration profiles window has a drop-down menu of existing scan profiles as well as the option to create a new one. To help you create a scan profile to fit your needs, see section ThreatSense engine parameters setup for a description of each parameter of the scan setup.

EXAMPLE: Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you don’t want to scan runtime packers or potentially unsafe applications and you also want to apply Strict cleaning. From the Configuration profiles window, click the Add... button. Enter the name of your new profile in the Profile name field, and select Smart scan from the Copy settings from profile: drop-down menu. Then adjust the remaining parameters to meet your requirements.

3.2.1.2.4 Command Line

ESET Gateway 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` load modules from FOLDER
- `– quar-dir = FOLDER` quarantine FOLDER
- `– aind` show activity indicator

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

Cleaning:
– action = ACTION

– quarantine
– no-quarantine

Logs:
– log-file=FILE
– log-rewrite

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
disable heuristics
enable advanced heuristics
disable advanced heuristics
perform ACTION on infected objects. Available actions: none, clean, prompt
copy infected files to Quarantine (supplements ACTION)
do not copy infected files to Quarantine
log output to FILE
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.

3.2.1.3 Performance

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

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

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

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

3.2.1.4 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 Gateway Security. Please see chapter 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
Edit... – enables you to edit selected entries
Remove – removes selected entries
Default – cancels all exclusions.

To exclude an object from scanning:

• Select Add...
• Enter the path to an object or select it in the tree structure below.
3.2.1.5 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
- **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.

3.2.1.5.1 Objects setup

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

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

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

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

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

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

Self-extracting archives – Scans files which are contained in self-extracting archive files, but typically presented with an .exe file extension.
Runtime packers – Runtime packers (unlike standard archive types) decompress in memory, in addition to standard static packers (UPX, yoda, ASPack, FGS, etc.).

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

3.2.1.5.2 Options

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

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

Heuristics – Heuristics use an algorithm that analyses the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist, or was not included in the list of known viruses (virus signatures database).

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

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

Potentially unwanted applications – Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.

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

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

The cleaning settings determine the behavior of the scanner during the cleaning of infected files. There are 3 levels of cleaning:

No cleaning – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.

Standard cleaning – The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow up actions. The choice of follow-up actions will also be displayed if a predefined action could not be completed.

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

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

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

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

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

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

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

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

3.2.1.5.5 Limits

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

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

Maximum scan time for object (sec.): – Defines the maximum time value for scanning an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished.

Archive nesting level: – Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances, there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.

Maximum size of file in archive: – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If this causes scanning an archive to be prematurely terminated, the archive will remain unchecked.

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

3.2.1.5.6 Other

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

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

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

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

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

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

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

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

3.2.1.6 An infiltration is detected

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

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

- Open ESET Gateway Security and click Computer scan
- Click Smart scan (for more information, see section Smart scan[^37])
- 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 Gateway Security, suppose that an infiltration is detected by the real-time file system monitor, which uses the Default cleaning level. It will attempt to clean or delete the file. If there is no predefined action to take for the real-time protection module, you will be asked to select an option in an alert window. Usually, the options Clean, Delete and Leave are available. Selecting Leave is not recommended, since the infected file(s) would be left untouched. The exception to this is when you are sure that the file is harmless and has been detected by mistake.

Cleaning and deleting – Apply cleaning if a file has been attacked by a virus which has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.
If an infected file is “locked” or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

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

3.3 Updating the program

Regular updating of ESET Gateway 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.

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 Gateway Security.
3.3.1 Update setup

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

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

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

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

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

3.3.1.2 Advanced update setup

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

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

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

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

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

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

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

In ESET Gateway Security, proxy server setup is available in two different sections within the Advanced Setup tree. First, proxy server settings can be configured under **Miscellaneous > Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Gateway Security. Parameters here will be used by all modules requiring connection to the Internet.

To specify proxy server settings for this level, select the **Use proxy server** checkbox and then enter the address of the proxy server into the **Proxy server** field, along with the **Port** number of the proxy server. If communication with the proxy server requires authentication, select the **Proxy server requires authentication** checkbox and enter a valid **Username** and **Password** into the respective fields. Click the **Detect proxy server** button to automatically detect and insert proxy server settings. The parameters specified in Internet Explorer will be copied.

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

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

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

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified within the **Miscellaneous > Proxy server** branch of the Advanced Setup tree (as described at the top of this article).
Select the **Do not use proxy server** option to specify that no proxy server will be used to update ESET Gateway Security.

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

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

The default setting for the proxy server is **Use global proxy server settings**.
3.3.1.2.3 Connecting to the LAN

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

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

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

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

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

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

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

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

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

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

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

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

NOTE: It is not possible for Antispam database to be updated from the mirror. To read more information on how to allow for correct Antispam database updates, click here.
3.3.1.2.4.1 Updating from the Mirror

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

Accessing the Mirror using an internal HTTP server

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

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

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

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

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

Accessing the Mirror via system shares

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

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

If the shared folder is located on another computer in the network, you must specify authentication data to access the other computer. To specify authentication data, open ESET Gateway Security Advanced Setup (F5) and click the Update branch. Click the Setup... button and then click the LAN tab. This setting is the same as for updating, as described in section Connecting to LAN.
After the Mirror configuration is complete, proceed to the workstations and set `\(UNC\)\PATH` as the update server. This operation can be completed using the following steps:

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

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

### 3.3.1.2.4.2 Troubleshooting Mirror update problems

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

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

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

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

### 3.3.2 How to create update tasks

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

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

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

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

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

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

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

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

3.4.1 Purpose of scheduling tasks

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

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

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

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

From the Scheduled task: drop-down menu, select Update. Click Next and enter the name of the task into the Task name: field. Select the frequency of the task. The following options are available: Once, Repeatedly, Daily, Weekly and Event triggered. Based on the frequency selected, you will be prompted with different update parameters. Next, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

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

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

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

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

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

Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (added by user...), and number of threats (e.g., if it is an archive containing multiple infiltrations).

3.5.1 Quarantining files

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

3.5.2 Restoring from Quarantine

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

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

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

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

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

- **Detected threats** – Use this option to view all information about events related to detected infiltrations, except infiltrations detected by on-demand computer scan (these events are recorded in On-demand computer scan log).

- **Events** – This option is designed for system administrators and users to solve problems. All important actions performed by ESET Gateway Security are recorded in the Event logs.

- **On-demand computer scan** – Results of all completed scans are displayed in this window. Double-click any entry to view details of the respective On-demand scan.

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

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

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

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

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

![Log filtering window](image)

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

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

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

- Time
- Module
- Event
- User

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

- Diagnostic
- Information
- Warning
- Error
- Critical
**Time period**: - Use this option to have records filtered by time period. You can choose one of the following:

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

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

- **Match whole words only** - Shows only records that match the string as a whole word in the What text box.
- **Match case sensitive** - Shows only records that match the string with exact capitalization in the What text box.
- **Enable Smart filtering** - Use this option to let ESET Gateway Security perform filtering using its own methods.

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

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

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

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

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

**Look in columns**: - Select what columns will be taken into account when searching. You can check one or more columns to be used for searching. By default, all columns are checked:
- Time
- Module
- Event
- User
Record types: - Lets you choose what type of records to find. You can choose one particular record type, multiple types at the same time, or have all of the record types to be searched (by default):

- Diagnostic
- Information
- Warning
- Error
- Critical

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

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

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

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

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

Search up - Searches from current position upwards.

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

3.6.3 Log maintenance

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

- Delete records automatically: Log entries older than the specified number of days are automatically deleted
- Optimize log files automatically: Enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded
- Minimum logging verbosity: Specifies the logging verbosity level. Available options:
  - Diagnostic records – Logs information needed for fine-tuning of the program and all records above
  - Informative records – Records informative messages including successful update messages plus all records above
  - Warnings – Records critical errors and warning messages
  - Errors – Only “Error downloading file” messages are recorded, plus critical errors
  - Critical warnings – Logs only critical errors (error starting Antivirus protection, etc...)
3.7 ESET SysInspector

3.7.1 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). For more information see section ESET SysInspector as part of ESET Gateway Security.

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.

3.7.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the SysInspector.exe executable you downloaded from ESET's website. If you already have one of the ESET Security solutions installed, you can run ESET SysInspector directly from the Start Menu (Programs > ESET > ESET Gateway Security).

Please wait while the application inspects your system, which could take up to several minutes depending on your hardware and data to be gathered.
3.7.2 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.).

![ESET SysInspector GUI](image)

3.7.2.1 Program Controls

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

File

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

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

Tree

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

List

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

Help

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

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

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

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

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

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

Status section
Displays the current node in Navigation window.

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

3.7.2.2 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.

3.7.2.2.1 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
unknown, risk level 6-9 items are displayed
7, B  risky, risk level 7-9 items are displayed
8  risky, risk level 8-9 items are displayed
9  risky, risk level 9 items are displayed
-  decreases risk level
+  increases risk level
Ctrl+9  filtering mode, equal level or higher
Ctrl+0  filtering mode, equal level only

View

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

Other controls

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

Comparing

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

Miscellaneous

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

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

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

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

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

Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs. Items marked by a ✗ can only be found in the active log and were not present in the opened comparative log. Items marked by a + were present only in the opened log and are missing in the active one.

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

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

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

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

**Example**

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

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

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

`SysInspector.exe current.xml previous.xml`
3.7.3 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.

3.7.4 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.

3.7.4.1 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.
3.7.4.2 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 (izakmp)

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.
3.7.4.3 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.

3.7.5 FAQ

**Does ESET SysInspector require Administrator privileges to run?**

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

**Does ESET SysInspector create a log file?**

ESET SysInspector can create a log file of your computer's configuration. To save one, select **File > Save Log** from the main menu. Logs are saved in XML format. By default, files are saved to the `%USERPROFILE%\My Documents\` directory, with a file naming convention of "SysInspector-%COMPUTERNAME%-%DATE%.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 "CompanyName" 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.

3.7.6 ESET SysInspector as part of ESET Gateway Security
To open the ESET SysInspector section in ESET Gateway Security, click Tools > ESET SysInspector. The management system in the ESET SysInspector window is similar to that of computer scan logs, or scheduled tasks. All operations with system snapshots – create, view, compare, remove and export – are accessible within one or two clicks.

The ESET SysInspector window contains basic information about the created snapshots such as create time, a short comment, name of the user that created the snapshot and snapshot status.

To compare, create, or delete snapshots, use the corresponding buttons located below the list of snapshots in the ESET SysInspector window. Those options are also available from the context menu. To view the selected system snapshot, use the Show context menu option. To export the selected snapshot to a file, right-click it and select Export....
Below is a detailed description of the available options:

- **Compare** – Allows you to compare two existing logs. It is suitable if you want to track changes between the current log and an older log. For this option to take effect, you must select two snapshots to be compared.

- **Create...** – Creates a new record. Before that, you must enter a short comment about the record. To find out the snapshot creation progress (of the currently generated snapshot), see the **Status** column. All completed snapshots are marked by the **Created** status.

- **Delete/Delete all** – Removes entries from the list.

- **Export...** – Saves the selected entry in an XML file (also in a zipped version).

### 3.8 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.

#### 3.8.1 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

#### 3.8.2 How to create rescue CD

To launch the ESET SysRescue wizard, click **Start > Programs > ESET > ESET Gateway 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.
3.8.3 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.

3.8.4 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.

3.8.4.1 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.

3.8.4.2 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.

3.8.4.3 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 SPI, 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.

3.8.4.4 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.

3.8.4.5 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.

3.8.4.6 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.
3.8.5  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.

3.8.5.1  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.

3.9  User interface

The user interface configuration options in ESET Gateway 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 Gateway Security Advanced Setup tree.

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

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

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

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

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

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

To enable the use of animated icons to display the progress of various operations, select the Use animated icons for progress indication option. If you want the program to sound a warning if an important event takes place, select the Use sound signal option.
The **User interface** features also include the option to password-protect the ESET Gateway 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...**
3.9.1 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 Gateway Security.

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

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

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

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

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

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of the user** field allows you to define who will receive important notifications from ESET Gateway 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.
3.9.2 Disable GUI on Terminal Server

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

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

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

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

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

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

3.10 eShell

eShell (short for ESET Shell) is a command line interface for ESET Gateway 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 the all the commands yet. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a particular context.

- **Single command / Batch mode** - you can use this mode if you only need to execute a command without entering the interactive mode of eShell. This can be done from the Windows Command Prompt by typing in `eshell` with appropriate parameters. For example:

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

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

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

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

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

### 3.10.1 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 Gateway 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>)
GET STATUS - if you are in the context AV (command line shows eShell av>)
.. GET STATUS - if you are in the context AV OPTIONS (command line shows eShell av options>)
```
Argument
An argument an action which is performed for a particular command. For example, command `CLEANLEVEL` can be used with following arguments:

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

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

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

Examples of the short form:

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

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

eShell>a
The following command is not unique: a

The following commands are available in this context:

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

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

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

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

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

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

eShell allows you to define your own aliases.

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

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

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

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

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

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

3.10.2 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 Gateway 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 Gateway 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:

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

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

**CONTEXT PATH:**

```plaintext
root
```

**SYNTAX:**

```plaintext
[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 Gateway Security (similar to GUI).

**CONTEXT PATH:**

```plaintext
root
```

**SYNTAX:**

```plaintext
[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.

3.10.2.1 Context - AV

ANTISTEALTH
Enable Anti-Stealth.

SYNTAX:

[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:

[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:

[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

3.10.2.2 Context - AV LIMITS ARCHIVE

LEVEL
Archive nesting level.

SYNTAX:

[get] | restore level
set level <number>

OPERATIONS:

g - 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:

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

ARGUMENTS:

number - Size in kB or 0 for default settings
3.10.2.3 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

3.10.2.4 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

---

**3.10.2.5 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
3.10.2.6  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

3.10.2.7  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:
3.10.2.8 Context - AV REALTIME DISK

FLOPPY
Scan removable media.

SYNTAX:

\[ \text{[get]} \mid \text{restore floppy} \]
\[ \text{set floppy disabled} \mid \text{enabled} \]

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:

\[ \text{[get]} \mid \text{restore local} \]
\[ \text{set local disabled} \mid \text{enabled} \]

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:

\[ \text{[get]} \mid \text{restore network} \]
\[ \text{set network disabled} \mid \text{enabled} \]

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
enabled - Enables function/activates setting

3.10.2.9 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

FLOPPYACCESS
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

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
3.10.2.11  Context - AV REALTIME EXECUTABLE FROM REMOVABLE 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
all - 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.

3.10.2.12  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

3.10.2.13  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
3.10.2.14 Context - AV REALTIME OBJECTS

BOOT
Scan boot sectors.

SYNTAX:

[get] | restore boot

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

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

3.10.2.15 Context - AV REALTIME ONWRITE

ADVHEURISTICS
Enable advanced heuristics for new and modified files.

SYNTAX:

[get] | restore advheuristics

OPERATIONS:

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

ARGUMENTS:
RUNTIME
Scan new and modified runtime archives.

SYNTAX:

\[ \text{get} \mid \text{restore runtime} \]
\[ \text{set runtime disabled} \mid \text{enabled} \]

OPERATIONS:

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

ARGUMENTS:

- \text{disabled} - Disables function/deactivates setting
- \text{enabled} - Enables function/activates setting

SFX
Scan new and modified self-extracting archives.

SYNTAX:

\[ \text{get} \mid \text{restore sfx} \]
\[ \text{set sfx disabled} \mid \text{enabled} \]

OPERATIONS:

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

ARGUMENTS:

- \text{disabled} - Disables function/deactivates setting
- \text{enabled} - Enables function/activates setting

3.10.2.16  Context - AV REALTIME ONWRITE ARCHIVE
LEVEL
Archive nesting depth.

SYNTAX:

\[ \text{get} \mid \text{restore level} \]
\[ \text{set level <number>} \]

OPERATIONS:

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

ARGUMENTS:

- \text{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)

3.10.2.17  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
```

3.10.2.18  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

3.10.2.19  **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.
3.10.2.20  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

3.10.2.21  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 Gateway 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
3.10.2.22 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
3.10.2.23  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
   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

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
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

CONTEXT
Context color.

SYNTAX:

[get] | restore context

set context [black | navy | green | 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

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
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

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
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

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
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

**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
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

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
green - Grass green
ltblue - Light blue
brown - Brown
SUCCESS
Status OK color.

SYNTAX:

\[\text{[get]} \mid \text{restore success}\]

\text{set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]}

OPERATIONS:

\text{get - Returns current setting/status}\n\text{set - Sets value/status}\n\text{restore - Restores default settings/object/file}

ARGUMENTS:

\text{black - Black}\n\text{navy - Navy blue}\n\text{grass - Grass green}\n\text{ltblue - Light blue}\n\text{brown - Brown}\n\text{purple - Purple}\n\text{olive - Olive green}\n\text{ltgray - Light gray}\n\text{gray - Gray}\n\text{blue - Blue}\n\text{green - Green}\n\text{cyan - Cyan}\n\text{red - Red}\n\text{magenta - Magenta}\n\text{yellow - Yellow}\n\text{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
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

3.10.2.24 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'.

3.10.2.25  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

3.10.2.26  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:

[get] | restore hidden
set hidden 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

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:

\[\text{[get]} \mid \text{restore syntaxhint}\]
\[\text{set syntaxhint disabled} \mid \text{enabled}\]

OPERATIONS:

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

ARGUMENTS:

\text{disabled} - Disables function/deactivates setting
\text{enabled} - Enables function/activates setting

VALUESONLY

Display only values without description.

SYNTAX:

\[\text{[get]} \mid \text{restore valuesonly}\]
\[\text{set valuesonly disabled} \mid \text{enabled}\]

OPERATIONS:

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

ARGUMENTS:

\text{disabled} - Disables function/deactivates setting
\text{enabled} - Enables function/activates setting

3.10.2.27  Context - GENERAL PERFORMANCE

SCANNERS

Number of running scans.

SYNTAX:

\[\text{[get]} \mid \text{restore scanners}\]
\[\text{set scanners} \langle\text{number}\rangle\]

OPERATIONS:

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

ARGUMENTS:

\text{number} - Count (1 - 20)
3.10.2.28 Context - GENERAL PERFORMANCE SERVER TEMPORARY
PATH
Temporary files location.

SYNTAX:

    [get] | restore path
    set path [string]

OPERATIONS:

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

ARGUMENTS:

    string - Path

3.10.2.29 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
3.10.2.30  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

3.10.2.31  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
3.10.2.32  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

ENCYPT
Block uncrypted 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

3.10.2.33  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

3.10.2.34  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

3.10.2.35  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

3.10.2.36  Context - SCANNER

CLEANLEVEL

Cleaning level.

SYNTAX:

\[\text{set cleanlevel} \text{ none | normal | strict}\]

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:

\[\text{add | remove extensions <extension> | /all | /extless}\]

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:

\[\text{add profile new: <name> [copyfrom: <name>]}\]

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:

\[ \text{[get]} | \text{clear scan} \]
\[ \text{start scan [readonly]} \]
\[ \text{pause | resume | stop scan <ID> | all} \]

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:

\[ \text{[get]} target \]
\[ \text{add | remove target <path>} \]

OPERATIONS:

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

ARGUMENTS:
path - Path/Scan target

NOTE: For boot sector scan enter $Boot where 'x' is the name of scanned disk.
3.10.2.37  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

3.10.2.38  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

3.10.2.39 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

3.10.2.40  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

3.10.2.41  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:
\[ \text{get} \] | 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

3.10.2.42 Context - SERVER

AUTOEXCLUSIONS
Automatic exclusions management.

SYNTAX:
\[ \text{get} \] | restore autoexclusions
select autoexclusions <server>

OPERATIONS:
get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:
server - Server name

STATUS
Gateway server protection.

SYNTAX:
\[ \text{get} \] | 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
3.10.2.43  Context - SERVER AS

STATUS

Gateway server antispam 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

3.10.2.44  Context - SERVER AS ENGINE ANALYSIS

ATTACHMENTS

Scan message attachments.

SYNTAX:

[get] | restore attachments
set attachments 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

This option controls whether the antispam engine will scan and consider attachments when computing the spam score.

MIMEBOTH

Use both MIME sections.

SYNTAX:

[get] | restore mimeboth
set mimeboth 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.

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 analyze only one section. If this option is set to "disabled", then only one section will be analyzed.

**UNICODE**

Convert to UNICODE.

**SYNTAX:**

```
[get] | restore unicode
set unicode 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

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

### 3.10.2.45 Context - SERVER AS ENGINE ANALYSIS CACHE

**DOMAIN**

Use domain cache memory.

**SYNTAX:**

```
[get] | restore domain
set domain 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

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

**LEGITREPUTE**

Use LegitRepute cache memory.

**SYNTAX:**

```
[get] | restore legitrepute
set legitrepute 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

Enables usage of a LegitRepute cache to reduce false positives especially for newsletters.

3.10.2.46  Context - SERVER AS ENGINE ANALYSIS MEMORY
SAMPLE
Memory size for sample calculation (in bytes).

SYNTAX:
- [get] | restore sample
- set sample <number>

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

ARGUMENTS:
- number - Size

This option instructs the antispam engine not to read more than this size bytes when computing the message fingerprint. This is useful for getting consistent fingerprints.

SCORE
Memory size for score calculation (in bytes).

SYNTAX:
- [get] | restore score
- set score <number>

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

ARGUMENTS:
- number - Size

This option instructs the antispam engine not to read more than a configurable number of bytes from the message buffer when computing scores.
3.10.2.47  Context - SERVER AS ENGINE ANALYSIS SAMPLES

CACHE
Use fingerprint cache memory.

SYNTAX:

    [get] | restore cache
    set cache 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

3.10.2.48  Context - SERVER AS ENGINE ANALYSIS SAMPLES MSF

BULK
Number of messages designating a bulk message.

SYNTAX:

    [get] | restore bulk
    set bulk <number>

OPERATIONS:

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

ARGUMENTS:

    number - Number of messages

This option specifies how many similar messages are required in order to consider them a message bulk.

CLEANUP
Frequency of clearing cache memory.

SYNTAX:

    [get] | restore cleanup
    set cleanup <number>

OPERATIONS:

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

ARGUMENTS:

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

**ENTRIES**

Number of samples stored in memory.

**SYNTAX:**

\[
get | restore entries
set entries <number>
\]

**OPERATIONS:**

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

**ARGUMENTS:**

- **number** - Number samples

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.

**MATCH**

Two samples match sensitivity.

**SYNTAX:**

\[
get | restore match
set match <number>
\]

**OPERATIONS:**

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

**ARGUMENTS:**

- **number** - 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.

**USE**

Use MSF.

**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
Allows for use of an alternate fingerprinting algorithm known as MSF.

3.10.2.49  Context - SERVER AS ENGINE ANALYSIS SPAMCOMPILER

USE

Use SpamCompiler.

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

Speeds up rules processing but requires a little bit more memory.

VERSION

Preferred version.

SYNTAX:

[get] | restore version

set version auto | 5.1 | 5.2 | 6.0

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

auto - Automatic

5.1 - 5.1

5.2 - 5.2

6.0 - 6.0

 Specifies what SpamCompiler version to use. When set to "auto", the antispam engine will choose the best version to use.

NOTE: Improves accuracy and throughput.
3.10.2.50  Context - SERVER AS ENGINE ANALYSIS SPAMCOMPILER CACHE

FILELIST
List of cache memory files.

SYNTAX:

[get] | restore | clear filelist

add | remove filelist index

OPERATIONS:

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

clear - Removes all items/files

ARGUMENTS:

index - Rule file index

This option specifies which rules files are compiled on disk instead of memory.

USE
Use SpamCompiler cache memory.

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

If this option is set to enabled, SpamCompiler will store the compiled data on disk instead of memory to reduce memory usage.

3.10.2.51  Context - SERVER AS ENGINE CONFIGURATION

FILE

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

PROFILE

Automatic configuration profile.

SYNTAX:

[get] | restore profile

set profile auto | highend_desktop | lowend_desktop | highend_server | lowend_server | catch_rate | fp_rate
throughput | latency | network | cpu | memory | disk | security | reliability | privacy | reporting

OPERATIONS:

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

ARGUMENTS:

auto - Automatic
highend_desktop - High-end desktop PC
lowend_desktop - Low-end desktop PC
highend_server - High-end server
lowend_server - Low-end server
catch_rate - Focused on maximizing the success rate
fp_rate - Focused on minimizing FP
throughput - Focused on throughput
latency - Focused on latency
network - Focused on network load
cpu - Focused on CPU load
memory - Focused on memory usage
disk - Focused on Hard Disk space usage
security - Focused on security
reliability - Focused on reliability
privacy - Focused on privacy protection
reporting - Focused on reporting
3.10.2.52  Context - SERVER AS ENGINE CONNECTION

PROXY
Proxy server authentication type.

SYNTAX:

[get] | restore proxy
set proxy auto | basic | digest

OPERATIONS:

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

ARGUMENTS:

auto - Automatic
basic - Basic
digest - Digest

Specifies which type of HTTP Proxy authentication should be used.

TIMEOUT
Single SpamLabs request duration limit (in seconds).

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 - Limit (seconds)

Limit how long a single request to SpamLabs can take. The value is specified in units of integral seconds.

NOTE: that a value of “0” disables this feature and no limit will be placed.

3.10.2.53  Context - SERVER AS ENGINE CONNECTION LIVEFEED

ADDRESS
LiveFeed 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

Specifies which server to query for LiveFeed requests.

TTL

LiveFeed request lifetime (in seconds).

SYNTAX:

[get] | restore ttl

set ttl <number>

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

number - This option allows setting a minimum TTL for entries in the internal LiveFeed cache of antispam engine.

NOTE: The option is specified in units of seconds. For those LiveFeed responses whose TTL value is less than livefeed_min_ttl, the internal cache of antispam engine will instead use livefeed_min_ttl.

3.10.2.54 Context - SERVER AS ENGINE CONNECTION PROTOCOL V4

THRESHOLD

Range of v4.x protocol usage.

SYNTAX:

[get] | restore threshold

set threshold <low>:<high>

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

low - Low value

high - High value

Since networks can introduce latency and a decrease in performance, this option allows running network checks conditionally based on the score. netcheck must be yes or this option is ignored. Network is only queried if score is at or between the "low" and "high" range specified via this option.

USE

Use v.4x protocol.

SYNTAX:

[get] | restore use

set use yes | no | auto

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

ARGUMENTS:
  yes - Yes
  no - No
  auto - Automatic

Communicate with SpamLabs via old and slower v4.x protocol to determine scoring.

NOTE: "Automatic" setting allows the antispam engine to automatically use the netcheck feature as a fallback to LiveFeed queries.

3.10.2.55  Context - SERVER AS ENGINE DNS

CACHE
Use DNS cache memory.

SYNTAX:
  [get] | restore cache
  set cache 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.

Enable internal caching of DNS requests.

DIRECT
Direct DNS access.

SYNTAX:
  [get] | restore direct
  set direct yes | no | auto

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

ARGUMENTS:
  yes - Yes
  no - No
  auto - Automatic

When set to yes and if dns server is not specified, then the antispam engine will make LiveFeed requests directly to
LiveFeed servers. This option is ignored if dns server is specified as it has precedence.

**NOTE:** This option should be set to yes when direct queries are more efficient than the default DNS servers.

**ENTRIES**

Number of DNS requests stored in memory.

**SYNTAX:**

```
[get] | restore entries
set entries <number>
```

**OPERATIONS:**

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

**ARGUMENTS:**

- **number** - Request number

Limits the number of entries in internal DNS cache.

**FILECACHE**

Save cache memory to disk.

**SYNTAX:**

```
[get] | restore filecache
set filecache 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

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

**SERVER**

DNS 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
DNS servers can now be explicitly specified to override the default.

**TTL**

DNS request lifetime (in seconds).

**SYNTAX:**

```
[get] | restore ttl
set ttl <number>
```

**OPERATIONS:**

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

**ARGUMENTS:**

- `number` - Lifetime (seconds)

This option allows setting a minimum TTL for entries in the internal DNS cache of antispam engine.

**NOTE:** The option is specified in units of seconds. For those DNS responses whose TTL value is less than minimum TTL, the internal cache of antispam engine will instead use minimum TTL.

### 3.10.2.56 Context - SERVER AS ENGINE FILTERING DOMAINS

**APPROVED**

Allowed domains.

**SYNTAX:**

```
[get] | restore | clear approved
add | remove approved <ip> | <start_ip>-<end_ip> | <ip>/<mask> | <domain>
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `add` - Adds item
- `remove` - Removes item
- `restore` - Restores default settings/object/file
- `clear` - Removes all items/files

**ARGUMENTS:**

- `ip` - IP address
- `start_ip` - IP addresses range begin
- `end_ip` - IP addresses range end
- `mask` - Network mask
- `domain` - Domain

This option allows specifying body domains and IPs which should always be approved.

**BLOCKED**

Blocked domains.

**SYNTAX:**

```
[get] | restore | clear blocked
```
add | remove blocked <ip> | <start_ip>-<end_ip> | <ip>/<mask> | <domain>

OPERATIONS:
get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:
ip - IP address
start_ip - IP addresses range beginend_ip - IP addresses range end
mask - Network mask
domain - Domain

This option allows specifying body domains and IPs which should always be blocked.

IGNORED
Ignored domains.

SYNTAX:
[get] | restore | clear ignored
add | remove ignored <ip> | <start_ip>-<end_ip> | <ip>/<mask> | <domain>

OPERATIONS:
get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:
ip - IP address
start_ip - IP addresses range beginend_ip - IP addresses range end
mask - Network mask
domain - Domain

This option allows specifying body domains which should always be excluded from the DNSBL checks and ignored.
3.10.2.57 Context - SERVER AS ENGINE FILTERING IP

**APPROVED**

Allowed IP addresses.

**SYNTAX:**

```
[get] | restore | clear approved
add | remove approved <ip> | <start_ip>-<end_ip> | <ip>/<mask>
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `add` - Adds item
- `remove` - Removes item
- `restore` - Restores default settings/object/file
- `clear` - Removes all items/files

**ARGUMENTS:**

- `ip` - IP address
- `start_ip` - IP addresses range begin
- `end_ip` - IP addresses range end
- `mask` - Network mask

Set a custom list of allowed IP addresses of outgoing mail servers.

**BLOCKED**

Blocked IP addresses.

**SYNTAX:**

```
[get] | restore | clear blocked
add | remove blocked <ip> | <start_ip>-<end_ip> | <ip>/<mask>
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `add` - Adds item
- `remove` - Removes item
- `restore` - Restores default settings/object/file
- `clear` - Removes all items/files

**ARGUMENTS:**

- `ip` - IP address
- `start_ip` - IP addresses range begin
- `end_ip` - IP addresses range end
- `mask` - Network mask

Set a custom list of blocked IP addresses and domains located in the message body.

**IGNORED**

Ignored IP addresses.

**SYNTAX:**
Set a custom list of ignored IP addresses of outgoing mail servers.

3.10.2.58 Context - SERVER AS ENGINE FILTERING SENDERS

APPROVED

Allowed senders (WhiteList).

SYNTAX:

[get] | restore | clear approved

add | remove approved <email> | <domain>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

email - E-mail
domain - Domain

Set a custom list of allowed outgoing email addresses and domains.

BLOCKED

Blocked senders (BlackList).

SYNTAX:

[get] | restore | clear blocked

add | remove blocked <email> | <domain>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:
email - E-mail
domain - Domain

Set a custom list of blocked outgoing email addresses and domains.

SPOOFED
Fake senders.

SYNTAX:

[get] | restore | clear spoofed

add spoofed <server> <ip> | <start_ip>-<end_ip> | <ip>/<mask> <score>
remove spoofed <server>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:
server - Address
ip - IP address
start_ip - IP addresses range begin
domain - Domain
end_ip - IP addresses range end
mask - Network mask
score - Score

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. The offset will be applied when mail from the domain does not come from the specified IP range.

3.10.2.59  Context - SERVER AS ENGINE LOG

DETAILED

Use detailed logging.

SYNTAX:

[get] | restore detailed

set detailed disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
**FILE**

Output rerouting file.

**SYNTAX:**

```
[get] | restore file
set file [string]
```

**OPERATIONS:**

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

**ARGUMENTS:**

- **string**: Path

Redirects log output to a file in the conf directory.

---

**3.10.2.60  Context - SERVER AS ENGINE PERFORMANCE**

**STACK**

Maximum size of the used thread stack.

**SYNTAX:**

```
[get] | restore stack
set stack <number>
```

**OPERATIONS:**

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

**ARGUMENTS:**

- **number**: Size

Sets the maximum thread stack size to use. If the thread stack size is set to 64KB (e.g. FreeBSD), then this variable should be set to 100 or less. If the thread stack size is set to greater than 1MB (e.g. Linux, Solaris, and MacOSX), 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 percent.

---

**TEMPDIR**

Temporary files location.

**SYNTAX:**

```
[get] | restore tempdir
set tempdir [string]
```

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

ARGUMENTS:
string - Path

Please enter the path to the folder where temporary files will be placed.

THROUGHPUT
Required throughput (in messages per second).

SYNTAX:

[get] | restore throughput
set throughput <number>

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

ARGUMENTS:
number - Number of messages

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.

3.10.2.61 Context - SERVER AS ENGINE PERFORMANCE INCREMENTALFILES

FORCE
Download only incremental files.

SYNTAX:

[get] | restore force
set force 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

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 the incr file by setting this option to enabled.

MERGE
Join incremental files into one.

SYNTAX:

[get] | restore merge
set merge 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

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.

SIZE

Maximum size of incremental files (in bytes).

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 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.

3.10.2.62  Context - SERVER AS ENGINE REGIONAL BLOCKED

CHARSET

List of blocked charsets.

SYNTAX:
- [get] | restore | clear charset
- add charset <charset> <score>
- remove charset <charset>

OPERATIONS:
- get - Returns current setting/status
- add - Adds item
- remove - Removes item
- restore - Restores default settings/object/file
- clear - Removes all items/files

ARGUMENTS:
- charset - Charset
COUNTRY
List of blocked countries.
SYNTAX:

[get] | restore | clear country
add | remove country <code>

OPERATIONS:
get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

code - Country code

Set countries which you want to block and from which you do not want to receive messages. You can find the list of country codes in List of home countries section.

3.10.2.63 Context - SERVER AS ENGINE REGIONAL HOME
BLOCKNONHOME
Block non-home languages.
SYNTAX:

[get] | restore blocknonhome
set blocknonhome yes | no | auto

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

ARGUMENTS:

yes - Yes
no - No
auto - Automatic

This options controls whether or not languages, which are not listed in the List of Home Languages, will be blocked.

COUNTRY
List of home countries.
SYNTAX:

[get] | restore | clear country
add | remove country <code>

OPERATIONS:
get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

code - Country code

Set countries which you consider as home countries and from which you prefer to receive messages. You can find the list of country codes in List of home countries section.

LANGUAGE

List of home languages.

SYNTAX:

```
[get] | restore | clear language
add | remove language <code>
```

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

code - Language code

Set languages which you consider as home languages and in which you prefer to receive messages. You can find the list of language codes in List of home languages section.

3.10.2.64  Context - SERVER AS ENGINE RULES

CATEGORY

Category weight.

SYNTAX:

```
[get] | restore | clear category
add category spam | phish | bounce | adult | fraud | blank | forward | reply | approve | block | <score>
remove category spam | phish | bounce | adult | fraud | blank | forward | reply
```

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

spam - SPAM
phish - Phishing
bounce - Non-delivery report
adult - Mature content messages
fraud - Fraudulent messages
blank - Empty messages
forward - Forwarding messages
reply - Replying messages
approve - Approve
block - Block
score - Score

Allows the end user to adjust the weights of categories used in sc18 and in files used in custom rules list.

**NOTE:** 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**

Custom rules list.

**SYNTAX:**

```
[get] | restore | clear custom
add | remove custom path
```

**OPERATIONS:**

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

**ARGUMENTS:**

- path - Rule file path

Allows user to specify a custom list of rules (i.e. spam, ham, or phishing words/phrases).

**NOTE:** Custom rules files contain phrases in the following format on separate lines: phrase, type, confidence, case sensitivity 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 the type is SPAM, then 100 indicates a higher confidence of spamminess. If the 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 the type is SPAM, then 100 will score the message as 100. If the type is PHISH, then 100 will score the message as 100. If the type is BOUNCE, then 100 will score the message as 100. As always, any whitelist overrides any blacklist. Case sensitivity value of 1 means that the phrase will be case sensitive; 0 means that the phrase will be case insensitive.

**DOWNLOADED**

List of downloaded rule files.

**SYNTAX:**

```
[get] | restore | clear downloaded
add | remove downloaded index
```

**OPERATIONS:**

- get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:
  index - Rule file index

This option specifies which rule files are downloaded when retrieveRules() is called. If the option is blank then retrieveRules() will only download files which are necessary to support a given configuration (based on other options).

USE
Use rules.

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

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

WEIGHTS
Rule weight.

SYNTAX:
  [get] | restore | clear weights
  add weights index weight
  remove weights index

OPERATIONS:
  get - Returns current setting/status
  add - Adds item
  remove - Removes item
  restore - Restores default settings/object/file
  clear - Removes all items/files

ARGUMENTS:
  index - Rule file index
  weight - Weight

This option allows overriding weights associated with individual rules.
3.10.2.65  Context - SERVER AS ENGINE RULES EXTENSIONS

FIRST
Use rule set extension.

SYNTAX:

[get] | restore first
set first 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

Enables the extended rule set.

SECOND
Use second rule set extension.

SYNTAX:

[get] | restore second
set second 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

Enables the second extension to rule set.

3.10.2.66  Context - SERVER AS ENGINE RULES UPDATE

CLEANUP
Clear older rules after their update.

SYNTAX:

[get] | restore cleanup
set cleanup 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

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

NOTIFICATION

Show notification after successful update of rules.

SYNTAX:

[get] | restore notification
  set notification 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

3.10.2.67  Context - SERVER AS ENGINE SCORE

CLEAN

Score value up to which a message is regarded as certainly clean.

SYNTAX:

[get] | restore clean
  set clean <number>

OPERATIONS:

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

ARGUMENTS:

- number - Score (0 - 100)

Antispam protection assigns scanned messages a score from 0 to 100. Setting the score value boarders affects which messages are considered as SPAM and which are not.

NOTE: Setting incorrect values can decrease the quality of antispam engine's detection.

HISTORY

Use score history.

SYNTAX:

[get] | restore history
  set history 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

Enables tracking of historical scores for repetitive senders.

**SPAM**

Score value from which a message is regarded as SPAM.

**SYNTAX:**

```
[get] | restore spam
set spam <number>
```

**OPERATIONS:**

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

**ARGUMENTS:**

number - Score (0 - 100)

Antispam protection assigns scanned messages a score from 0 to 100. Setting the score value boarders affects which messages are considered as SPAM and which are not.

**NOTE:** Setting incorrect values can decrease the quality of antispam engine's detection.

**UNKNOWN**

Score value which sets a border when a message is regarded as a probable SPAM or probably clean.

**SYNTAX:**

```
[get] | restore unknown
set unknown <number>
```

**OPERATIONS:**

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

**ARGUMENTS:**

number - Score (0 - 100)

Antispam protection assigns scanned messages a score from 0 to 100. Setting the score value boarders affects which messages are considered as SPAM and which are not.

**NOTE:** Setting incorrect values can decrease the quality of antispam engine's detection.
3.10.2.68  Context - SERVER AS ENGINE SCORE SDK

HAM

Level of HAM score.

SYNTAX:

[get] | restore ham
set ham <number>

OPERATIONS:

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

ARGUMENTS:

number - Score (0 - 100)

This option allows you to tell the antispam engine to skip slow rule checks if the message is likely to be ham.

SPAM

Level of SPAM score.

SYNTAX:

[get] | restore spam
set spam <number>

OPERATIONS:

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

ARGUMENTS:

number - Score (0 - 100)

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.

3.10.2.69  Context - SERVER AS ENGINE SPAMBAIT

ADDRESSES

Spambait addresses.

SYNTAX:

[get] | restore | clear addresses
add | remove addresses <email>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files
ARGUMENTS:

email - E-mail
Set mail addresses which only receive SPAM.

NONEXIST
Addresses regarded as nonexistent.

SYNTAX:

[get] | restore | clear nonexist
add | remove nonexist <email>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

email - E-mail
Set mail addresses which, on the outside, appear to be nonexistent.

3.10.2.70  Context - SERVER AS ENGINE STATISTICS

ADDRESS
Analysis 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
URL where statistics files will be uploaded.

UPLOAD
Send statistical data for analysis.

SYNTAX:

[get] | restore upload
set upload 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

Launches a thread to automatically upload statistics files to analysis servers.

USE
Statistical data logging.

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

Logs IPs, Domains, URLs, suspicious words, etc. to the conf file system. Logs can be automatically uploaded to analysis servers. The logs can be converted to plain text for viewing.

3.10.2.71  Context - SERVER AS ENGINE TRAINING

COUNTRY
Use country data for training.

SYNTAX:
  [get] | restore country
  set country 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

Controls whether country routing information should be considered when training and scoring messages.

FINGERPRINT
Use training for message fingerprint score.

SYNTAX:
  [get] | restore fingerprint
  set fingerprint 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

Enables fingerprint score offset training.

FORCEUSE
Use only training data.

SYNTAX:
- [get] | restore forceuse
  - set forceuse 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

Controls whether to give full weight to training data. If this option is set to "enabled" then scoring will be based solely on training data. If this option is set to "disabled" then both rules and training data will be used.

MAXWORDS
Number of words in cache memory.

SYNTAX:
- [get] | restore maxwords
  - set maxwords <number>

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

ARGUMENTS:
- number - Word number

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. enable_word_training must be yes or this option is ignored.

MINDATA
Minimum amount of training data.

SYNTAX:
- [get] | restore mindata
set mindata <number>

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

ARGUMENTS:
  number - Data amount

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 be always ignored.

THRESHOLD
Automatic training sensitivity.

SYNTAX:
  [get] | restore threshold
  set threshold <low>:<high>

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

ARGUMENTS:
  low - Low threshold
  high - High threshold

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.

UPDATES
Use training database only for reading.

SYNTAX:
  [get] | restore updates
  set updates 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

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.

WORD

Use training for words.

SYNTAX:

[get] | restore word

set word 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

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.

WRITEBUFFER

Number of scanned messages before writing them to disk.

SYNTAX:

[get] | restore writebuffer

set writebuffer <number>

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

number - Message number

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.

Writing to disk is expensive so this number should be made as large as possible for maximum performance.

If the program is unexpectedly terminated before the buffer has been written to disk, then training performed since the last disk write will be lost. The buffer is written to disk on normal termination.
3.10.2.72  Context - SERVER AS ENGINE VERIFICATION DNSBL

COUNT
Maximum number of verified domains against DNSBL.

SYNTAX:

[get] | restore count
set count <number>

OPERATIONS:

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

ARGUMENTS:

number - Number

Allows limiting how many domains and IPs are queried against the DNS Blocklist server.

SERVERS
DNSBL (DNS Blocklists) servers.

SYNTAX:

[get] | restore | clear servers
add servers <server> <ip> <score>
remove servers <server>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

server - Server address
ip - Response IP address
score - Score

Specifies a list of DNS Blocklist (DNSBL) servers to query with domains and IPs extracted from the message body.

THRESHOLD
DNSBL verification sensitivity.

SYNTAX:

[get] | restore threshold
set threshold <low>:<high>

OPERATIONS:

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

ARGUMENTS:

low - Low value
high - High value

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.

TIMEOUT
DNSBL request execution limit (in seconds).

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 - Limit (seconds)

Allows setting a maximum timeout for finishing all DNSBL queries.

3.10.2.73 Context - SERVER AS ENGINE VERIFICATION LBL

NOTVERIFIED
IP addresses not verified against LBL (Last Blackhole Lists).

SYNTAX:

[get] | restore | clear notverified
add | remove notverified <ip>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

ip - IP address

Set the list of IP addresses which will not be verified against LBL (Last Blackhole Lists) servers.

SERVERS
LBL (Last Blackhole Lists) servers.

SYNTAX:
[get] | restore | clear servers

add servers <server> <ip> <score>

remove servers <server>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:

server - Server address
ip - Response IP address
score - Score

Set the list of LBL (Last Blackhole Lists) servers against which messages will be verified.

3.10.2.74 Context - SERVER AS ENGINE VERIFICATION RBL COUNT

Maximum number of verified addresses against RBL.

SYNTAX:

[get] | restore count

set count <number>

OPERATIONS:

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

ARGUMENTS:

number - Number

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 IPs which match against the ignored IP list option do not count towards the RBL IP addresses limit.

SERVERS

RBL (Realtime Blackhole Lists) servers.

SYNTAX:

[get] | restore | clear servers

add servers <server> <ip> <score>

remove servers <server>

OPERATIONS:

get - Returns current setting/status
add - Adds item
remove - Removes item
restore - Restores default settings/object/file
clear - Removes all items/files

ARGUMENTS:
server - Server address
ip - Response IP address
score - Score

Specifies a list of RBL (Realtime Blackhole Lists) servers to query with domains and IPs extracted from the message body.

THRESHOLD
RBL verification sensitivity.

SYNTAX:
[get] | restore threshold
set threshold <low>:<high>

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

ARGUMENTS:
low - Low value
high - High value

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.

TIMEOUT
RBL request execution limit (in seconds).

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 - Limit (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.

### 3.10.2.75 Context - SERVER AS GATEWAY

#### STATUS
Gateway server antispam 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

### 3.10.2.76 Context - SERVER AS GATEWAY IMAP

#### ACTION
Action to perform on uncleaned IMAP threat.

**SYNTAX:**

```
[get] | restore action
    set action continue | reject
```

**OPERATIONS:**

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

**ARGUMENTS:**

- **continue**: Continue with the connection
- **reject**: Reject connection with a reply

#### STATUS
Antispam IMAP 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

3.10.2.77  Context - SERVER AS GATEWAY IMAP REJECT

MESSAGE
Custom reject response message.
SYNTAX:

```
[get] | restore message
set message [<message>]
```

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

ARGUMENTS:
  - message - Message

When a connection is rejected, the client will receive a message as a response to the request. It is possible to specify a custom message.

TYPE
Reject response type.
SYNTAX:

```
[get] | restore type
set type default | custom
```

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

ARGUMENTS:
  - default - Default
  - custom - Custom

3.10.2.78  Context - SERVER AS GATEWAY POP3

ACTION
Action to perform on uncleaned POP3 threat.
SYNTAX:

```
[get] | restore action
set action continue | reject
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
ARGUMENTS:
  continue - Continue with the connection
  reject - Reject connection with a reply

STATUS
Antispam POP3 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

3.10.2.79  Context - SERVER AS GATEWAY POP3 REJECT

MESSAGE
Custom reject response message.
SYNTAX:
  [get] | restore message
  set message [<message>]

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

ARGUMENTS:
  message - Message

When a connection is rejected, the client will receive a message as a response to the request. It is possible to specify a custom message.

TYPE
Reject response type.
SYNTAX:
  [get] | restore type
  set type default | custom

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

ARGUMENTS:
  default - Default
  custom - Custom

3.10.2.80 Context - SERVER AS GATEWAY SMTP

ACTION
Action to perform on uncleaned SMTP threat.

SYNTAX:

[get] | restore action
set action continue | reject

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

ARGUMENTS:
  continue - Continue with the connection
  reject - Reject connection with a reply

STATUS
Antispam SMTP 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

3.10.2.81 Context - SERVER AS GATEWAY SMTP REJECT

CODE
Reject reply RFC code.

SYNTAX:

[get] | restore code
set code <number>

OPERATIONS:
get - Returns current setting/status
**set** - Sets value/status

**restore** - Restores default settings/object/file

**ARGUMENTS:**

- **number** - RFC code

**EXTENDED CODE**

Reject reply RFC extended code.

**SYNTAX:**

```plaintext
[get] | restore extendedcode
default extendedcode [<code>]
```

**OPERATIONS:**

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

**ARGUMENTS:**

- **code** - Extended RFC code

**TEXT**

Reject reply RFC text.

**SYNTAX:**

```plaintext
[get] | restore text
default text [<text>]
```

**OPERATIONS:**

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

**ARGUMENTS:**

- **text** - RFC text

**3.10.2.82 Context - SERVER AV**

**STATUS**

Gateway server antivirus and antispyware protection.

**SYNTAX:**

```plaintext
[get] | restore status
default 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

3.10.2.83  Context - SERVER AV FTP

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 - Adds item
- remove - Removes item
- restore - Restores default settings/object/file

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

3.10.2.84  Context - SERVER AV FTP 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:

\[\text{get} | \text{restore size}\]  
\text{set size <number>}

OPERATIONS:

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

ARGUMENTS:

number - Size in kB (1 - 3145728) or 0 for default settings

3.10.2.85 Context - SERVER AV FTP LIMITS OBJECTS

SIZE
Maximum archive size (kB).

SYNTAX:

\[\text{get} | \text{restore size}\]  
\text{set size <number>}

OPERATIONS:

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

ARGUMENTS:

number - Size in kB (1 - 3145728) or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).

SYNTAX:

\[\text{get} | \text{restore timeout}\]  
\text{set timeout <number>}

OPERATIONS:

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

ARGUMENTS:

number - Time in seconds (1 - 3600) or 0 for default settings
3.10.2.86  Context - SERVER AV FTP 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

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

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

---

### 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

3.10.2.88  Context - SERVER AV FTP 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

3.10.2.89   Context - SERVER AV GATEWAY

3.10.2.90   Context - SERVER AV GATEWAY FTP

3.10.2.91   Context - SERVER AV GATEWAY FTP REJECT

3.10.2.92   Context - SERVER AV GATEWAY HTTP

3.10.2.93   Context - SERVER AV GATEWAY HTTP REJECT

3.10.2.94   Context - SERVER AV GATEWAY IMAP

3.10.2.95   Context - SERVER AV GATEWAY IMAP REJECT

3.10.2.96   Context - SERVER AV GATEWAY POP3

3.10.2.97   Context - SERVER AV GATEWAY POP3 REJECT
3.10.2.98  Context - SERVER AV GATEWAY SMTP

3.10.2.99  Context - SERVER AV GATEWAY SMTP REJECT

3.10.2.100 Context - SERVER AV GENERAL

3.10.2.101 Context - SERVER AV GENERAL LIMITS ARCHIVE

3.10.2.102 Context - SERVER AV GENERAL LIMITS OBJECTS

3.10.2.103 Context - SERVER AV GENERAL OBJECTS

3.10.2.104 Context - SERVER AV GENERAL OPTIONS

3.10.2.105 Context - SERVER AV GENERAL OTHER

3.10.2.106 Context - SERVER AV HTTP

3.10.2.107 Context - SERVER AV HTTP LIMITS ARCHIVE

3.10.2.108 Context - SERVER AV HTTP LIMITS OBJECTS

3.10.2.109 Context - SERVER AV HTTP OBJECTS

3.10.2.110 Context - SERVER AV HTTP OPTIONS
3.10.2.111  Context - SERVER AV HTTP OTHER
3.10.2.112  Context - SERVER AV IMAP
3.10.2.113  Context - SERVER AV IMAP LIMITS ARCHIVE
3.10.2.114  Context - SERVER AV IMAP LIMITS OBJECTS
3.10.2.115  Context - SERVER AV IMAP OBJECTS
3.10.2.116  Context - SERVER AV IMAP OPTIONS
3.10.2.117  Context - SERVER AV IMAP OTHER
3.10.2.118  Context - SERVER AV POP3
3.10.2.119  Context - SERVER AV POP3 LIMITS ARCHIVE
3.10.2.120  Context - SERVER AV POP3 LIMITS OBJECTS
3.10.2.121  Context - SERVER AV POP3 OBJECTS
3.10.2.122  Context - SERVER AV POP3 OPTIONS
3.10.2.123  Context - SERVER AV POP3 OTHER
3.10.2.124  Context - SERVER AV SMTP

3.10.2.125  Context - SERVER AV SMTP LIMITS ARCHIVE

3.10.2.126  Context - SERVER AV SMTP LIMITS OBJECTS

3.10.2.127  Context - SERVER AV SMTP OBJECTS

3.10.2.128  Context - SERVER AV SMTP OPTIONS

3.10.2.129  Context - SERVER AV SMTP OTHER

3.10.2.130  Context - SERVER GATEWAY
Enter topic text here.

3.10.2.131  Context - SERVER GATEWAY FTP
Enter topic text here.

3.10.2.132  Context - SERVER GATEWAY HTTP
Enter topic text here.

3.10.2.133  Context - SERVER GATEWAY HTTP ADDRESSMGMT
Enter topic text here.

3.10.2.134  Context - SERVER GATEWAY IMAP
Enter topic text here.

3.10.2.135  Context - SERVER GATEWAY POP3
Enter topic text here.

3.10.2.136  Context - SERVER GATEWAY SMTP
Enter topic text here.
3.10.2.137  Context - SERVER RULES
Enter topic text here.

3.10.2.138  Context - SERVER RULES ACTION
Enter topic text here.

3.10.2.139  Context - SERVER RULES CONDITION
Enter topic text here.

3.10.2.140  Context - SERVER RULES REJECT
Enter topic text here.

3.10.2.141  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
send - Sends item/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)

3.10.2.142  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

3.10.2.143  Context - TOOLS ACTIVITY GATEWAY
PERFORMANCE
Gateway server protection performance.
SYNTAX:
[get] performance [<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
3.10.2.144  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
ers - 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:

```bash
[get] | restore verbosity
```

```bash
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
3.10.2.145  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

3.10.2.146  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)
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

3.10.2.147  Context - TOOLS LOG SERVER

SYNCHRONIZED

Synchronized write without the use of cache.

SYNTAX:

[get] | restore synchronized

set synchronized 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

3.10.2.148  Context - TOOLS LOG SERVER EVENT

ANTISPAM

Log spam score.

SYNTAX:

[get] | restore antispam

set antispam 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

DIAGNOSTIC
Log diagnostic information.

SYNTAX:

[get] | restore diagnostic
set diagnostic 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

PERFORMANCE
Log performance.

SYNTAX:

[get] | restore performance
set performance 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

RULE
Log rule application.

SYNTAX:

[get] | restore rule
set rule 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

3.10.2.149  Context - TOOLS NOTIFICATION

VERBOSITY

Minimum verbosity for notifications.

SYNTAX:

\[ \text{get} \] | \text{restore verbosity}

\text{set} \ \text{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

3.10.2.150  Context - TOOLS NOTIFICATION EMAIL

FROM

Senders email address.

SYNTAX:

\[ \text{get} \] | \text{restore from}

\text{set from} [\text{<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:

\[ \text{get} \] | \text{restore login}

\text{set login} [\text{<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:
   [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

3.10.2.151 Context - TOOLS NOTIFICATION MESSAGE
ENCODING
Warning messages encoding.

SYNTAX:
   [get] | restore encoding
   set encoding nolocal | localcharset | localencoding | ISO-2022-JP

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

ARGUMENTS:
   nolocal - Do not use national alphabet characters
   localcharset - Use national alphabet characters
   localencoding - Use national alphabet characters and encoding
   ISO - Use ISO-2022-JP encoding (For japanese version only)

3.10.2.152 Context - TOOLS NOTIFICATION MESSAGE FORMAT
DETECTION
Format of threat warning messages.

SYNTAX:
   [get] | restore detection
   set detection [<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
%ErrorDescription% - Error description

For message format, you need to replace key words (listed here between percent sign "%") with the corresponding values.

NOTE: ESET Gateway 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 message format, you need to replace key words (listed here between percent sign "%") with the corresponding values.

NOTE: ESET Gateway 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.
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
3.10.2.154  Context - TOOLS SCHEDULER

**ACTION**

Scheduled task action.

**SYNTAX:**

```
[get] action
```

**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

3.10.2.155 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
genrveupdate - Virus signature update
appupdate - Program component update
logon - User logon
detection - Threat detection
3.10.2.156  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)

3.10.2.157  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

3.10.2.158 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

3.10.2.159  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

3.10.2.160  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

3.10.2.161  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)

3.10.2.162 Context - TOOLS SCHEDULER STARTUP

DATE
Task will be run on the selected date.
SYNTAX:

[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:

[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:
[get] time
set time <hour>:<minute>:<second>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
hour - Hour
minute - Minute
second - Second

3.10.2.163  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
always - 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**

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

3.10.2.164  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

### 3.10.2.165 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:**
**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
3.10.2.166  Context - UPDATE MIRROR 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

3.10.2.167  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

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

3.10.2.168  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:
 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.

### 3.10.2.169  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
```

---

220
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

3.10.2.170  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

3.11 Import and export settings

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

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

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

1. You can decide not to enable the ThreatSense.Net Early Warning System. You will not lose any functionality in the software, and you will still receive the best protection that we offer.

2. You can configure the ThreatSense.Net Early Warning System to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

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

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

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

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

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

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

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

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

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

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

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

The ThreatSense.Net Early Warning System collects anonymous information about your computer related to newly detected threats. This information may include the name of the infiltration, the date and time it was detected, the ESET security product version, your operating system version and the location setting. The statistics are typically delivered to ESET’s servers once or twice a day.

Below is an example of a statistical package submitted:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4ed4d4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1463[1].exe
```

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

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

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

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

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

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

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

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

- **Server address:** Network address of the server where the ERA Server is installed.

- **Port:** This field contains a predefined server port used for connection. We recommend that you leave the default port setting of 2222.

- **Remote Administrator server requires authentication:** Allows you to enter a password to connect to the ERA Server, if required.

Click OK to confirm changes and apply the settings. ESET Gateway Security will use these settings to connect to the ERA Server.
3.14 Licenses

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

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

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

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

4.1 Types of infiltration

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

4.1.1 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.

4.1.2 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.

4.1.3 Trojan horses

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

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

- **Downloader** – A malicious program with the ability to download other infiltrations from the Internet
- **Dropper** – A type of trojan horse designed to drop other types of malware onto compromised computers
• **Backdoor** – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it

• **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers

• **Dialer** – Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

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

### 4.1.4 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 Gateway Security users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

### 4.1.5 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.

### 4.1.6 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.

4.1.7 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 Gateway 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.

4.1.8 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

4.2 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
4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 Recognizing spam scams

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

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

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

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

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

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

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