ESET Mail Security 4

for Microsoft Exchange Server

User Guide

Microsoft® Windows® 2000 / 2003 / 2008

ESET Mail Security 4
for Microsoft Exchange Server

Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

REV.20091029-001

Content

1. Introduction

ESET Mail Security 4 for Microsoft Exchange Server (EMSX) is an integrated solution protecting user mailboxes from various types of malware content (most often they are email attachments infected by worms or trojans, documents containing harmful scripts, phishing, spam etc.). EMSX filters the malicious content on the mailserver level, before it arrives in the addressee's email client inbox. The administrator can set the following message filtering criteria in EMSX: target mail folder, recipient, sender, message subject, message body, attachment name and size. An action to be performed on the filtered message can be set for each condition.

EMSX supports Microsoft Exchange versions 5.5 and later, in addition to Microsoft Exchange in a cluster environment. In newer versions (Microsoft Exchange 2007 and later), specific roles (mailbox, hub, edge) are also supported.

You can remotely manage EMSX in larger networks with the help of ESET Remote Administrator.

Where functionality is concerned, EMSX is almost identical to ESET NOD32 Antivirus 4.0. It has all the tools necessary to ensure protection of the server-as-client (resident shield, web-access protection, email client protection and antispam), while providing Microsoft Exchange Server protection. We will concentrate, however, on the Microsoft Exchange Server protection in this manual., We recommend reading the ESET NOD32 Antivirus manual for a comprehensive description and guide to all other EMSX modules.

1.1 System requirements

Supported Operating Systems:

- Microsoft Windows 2000 Server
- Microsoft Windows 2003 Server (x86 and x64)
- Microsoft Windows 2008 Server (x86 and x64)

Supported Microsoft Exchange Server versions:

Microsoft Exchange Server 5.5 SP3, SP4	
Microsoft Exchange Server 2000 SP1, SP2, SP3	min. requirements: Windows 2000 Server, Intel Pentium 166MHz or compatible, 128MB RAM, 700MB free disk space
Microsoft Exchange Server 2003 SP1, SP2	min. requirements: Windows 2000 Server, 133MHz or higher processor, 256MB RAM, 700MB free disk space
Microsoft Exchange Server 2007 SP1	min. requirements: Windows Server 2003, Intel Pentium 800MHz or compatible, 2GB RAM, 1.9GB free disk space
Microsoft Exchange Server 2010 Beta	min. requirements: Windows Server 2008, Intel 64 architecture or AMD64 platform processor, 4GB RAM, 1.9GB free disk space

Hardware requirements depend on the version of Microsoft Exchange employed, as well as the operating system version used. We recommend reading the Microsoft Exchange product documentation for more detailed information on hardware requirements.

1.2 Methods Used

Two independent methods are used to scan email messages:

1.2.1 Mailbox scanning via VSAPI

The mailbox scanning process is triggered and controlled by the Microsoft Exchange Server. Depending on the version of the Microsoft Exchange Server (consequently, the VSAPI interface version) and on the user-defined settings, the scanning process can be triggered in any of the following situations:

- When the user accesses email (e.g. in an email client)
- In the background, when use of the Microsoft Echange Server is low
- Proactively (based on the Microsoft Exchange Server's inner algorithm)

The VSAPI interface is currently used for antivirus scan and rule-based protection.

1.2.2 Message filtering on the SMTP server level

SMTP server level filtering is secured by a specialized plugin. In Microsoft Exchange Server 2000 and 2003, the plugin in question (Event Sink) is registered on the SMTP server as a part of Internet Information Services (IIS). In Microsoft Exchange Server 2007, the plugin is registered as a transport agent on the Edge or the Hub roles of the Microsoft Exchange Server.

The filtering plugin performs a scan during the processing of the SMTP END_OF_DATA command on Microsoft Exchange Server 2000, Microsoft Exchange Server 2003 and Microsoft Exchange Server 2007 in the Edge role. The exception to this rule is the Greylisting technique bound to the processing of the SMTP RCPT_TO command.

When Microsoft Exchange Server 2007 is in the Hub role, the transport agent processes messages while they are queuing.

SMTP server-level filtering by a transport agent provides protection in the form of antivirus, antispam and user-defined rules.

1.3 Types of protection

There are three types of protection:

1.3.1 Antivirus protection

Antivirus protection is one of the basic functions of the EMSX product. The same properties and parameters apply to antivirus protection in EMSX as antivirus protection in ESET Smart Security and ESET NOD32 Antivirus.

1.3.2 Antispam protection

Antispam protection integrates several technologies (SPF, RBL, whitelisting, rules, etc.) to ensure maximum detection of email threats. The antispam scanning core's output is the spam probability value of the given email message expressed as a percentage (0 to 100). Values of 90 and above are considered sufficient for the EMSX to classify an email as spam.

Another component of the antispam protection is the Greylisting technique. The technique relies on the assumption that legitimate mail agents will 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 within the database of verified connections on the second attempt, allowing any email with relevant characteristics to be delivered from then on.

1.3.3 Application of user-defined rules

Protection based on user-defined rules is available for scanning with both the VSAPI and the filtering agent. You can use the EMSX user interface to create individual rules that may also be combined. If one rule uses multiple conditions, the conditions will be linked using the logical operator AND. Consequently, the rule will be executed only if all its conditions are fullfilled. If multiple rules are created, the logical operator OR will be applied, meaning the program will run the first rule whose conditions are met.

In the scanning sequence, the first technique used is greylisting - if it is enabled. Consequent procedures will always execute the following sequence of techniques: protection based on user-defined rules, followed by an antivirus scan and, lastly, an antispam scan.

1.4 User interface

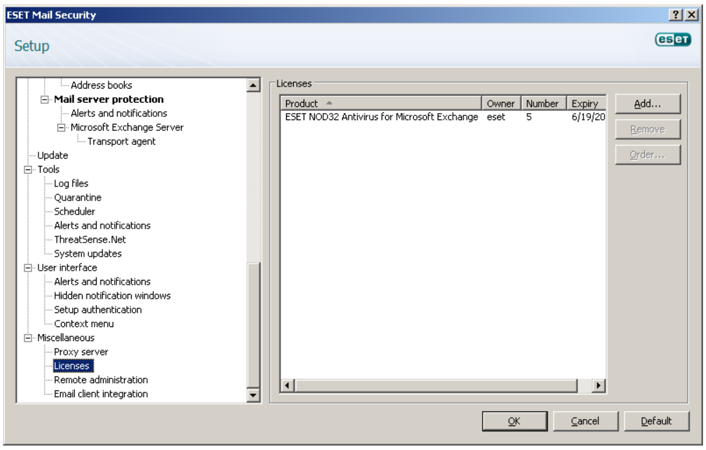
The similarity in design and functionality between EMSX and ESET NOD32 Antivirus/ESET Smart Security enables an intuitive user interface. You will only notice differences deep within the main menu and the advanced settings menu tree.

All items that contain Mail Server Protection in the title are assigned to MS Exchange Server protection.

We will discuss these items in this manual.

1.5 Installation

The installation process for EMSX is similar to that of other ESET security products. To begin, run the .msi installation file for ESET NOD32 Antivirus for Microsoft Exchange, downloadable from the ESET website. A very important step is to enter the license file for ESET NOD32 Antivirus for Microsoft Exchange. Without it, email protection on the Microsoft Exchange Server will not work properly. If you do not add the license file during installation, you can do so later in the advanced settings, under **Miscellaneous > Licenses**.



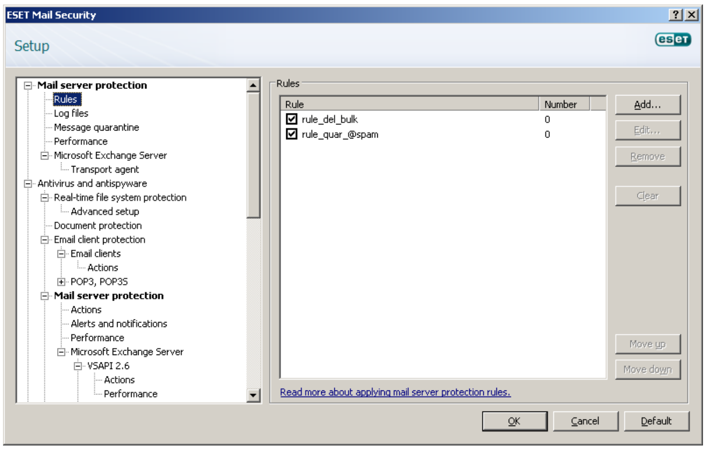
Product	Owner	Number	Expiry
ESET NOD32 Antivirus for Microsoft Exchange	eset	5	6/19/20

2. General settings

This section describes how to administer rules, log files, message quarantine and performance parameters.

2.1 Rules

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

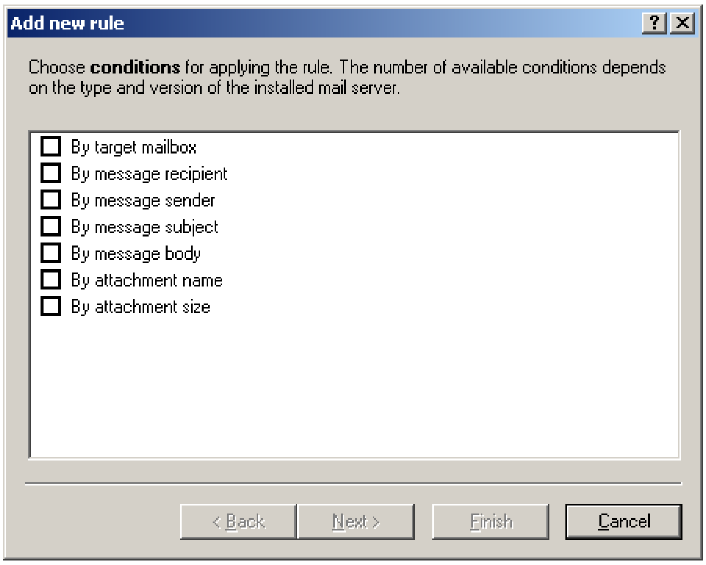


Rule	Number
☑ rule_del_bulk	0
☑ rule_quar_@spam	0

NOTE: You can also use system variables to apply Rules (for example: %PATHEXT%).

2.1.1 Adding new rules

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



Choose **conditions** for applying the rule. The number of available conditions depends on the type and version of the installed mail server.

- ☐ By target mailbox
- ☐ By message recipient
- ☐ By message sender
- ☐ By message subject
- ☐ By message body
- ☐ By attachment name
- ☐ By attachment size

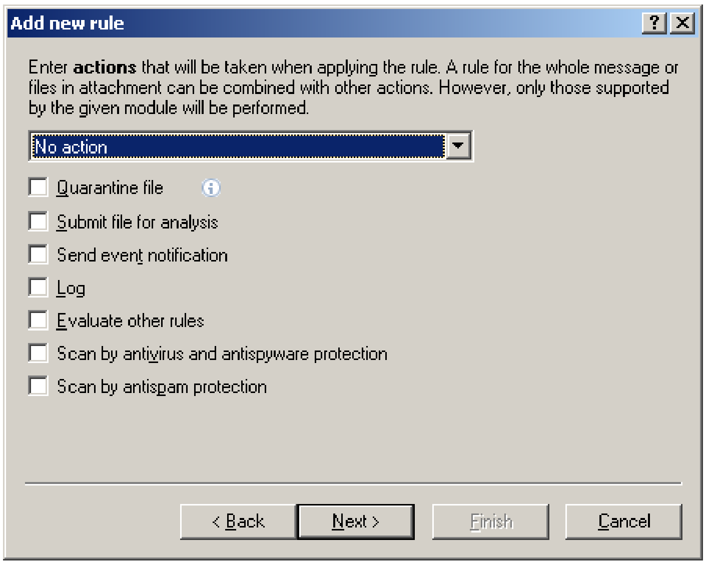
- **By target mailbox** applies to the name of a mailbox
- **By message recipient** applies to a message sent to a specified recipient
- **By message sender** applies to a message sent by a specified sender
- **By message subject** applies to a message with a specified subject line
- **By message body** applies to a message with specific text in the message body
- **By attachment name** applies to a message with a specific attachment name
- **By attachment size** applies to a message with an attachment exceeding a defined size

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

Examples:
By email sender: spam@spam.*
By email body: ("free" OR "lottery") AND ("win" OR "buy")

2.1.2 Actions

This section allows you to select actions to take with messages and/or attachments matching conditions defined in rules. You can take no action, block the message, move it to quarantine or delete it.



Enter **actions** that will be taken when applying the rule. A rule for the whole message or files in attachment can be combined with other actions. However, only those supported by the given module will be performed.

No action

- ☐ Quarantine file
- ☐ Submit file for analysis
- ☐ Send event notification
- ☐ Log
- ☐ Evaluate other rules
- ☐ Scan by antivirus and antispyware protection
- ☐ Scan by antispam protection

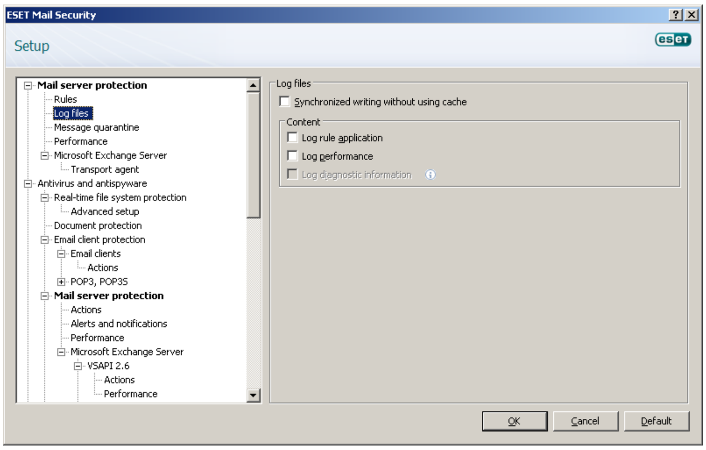
- **Quarantine file** saves an attached file to the quarantine mailbox
- **Submit file** for analysis sends suspicious attachments to ESET's Threat Lab for analysis
- **Send event notification** sends a notification to the administrator (based on settings in Tools > Alerts and notifications)
- **Log** writes information about the applied rule in the program log
- **Evaluate other rules** allows the evaluation of other rules, enabling the user to define multiple sets of conditions and multiple actions to take, given the conditions
- **Scan by antivirus and antispyware protection** scans the message and its attachment
- **Scan by antispam module** scans the message using the antispam module

The last step in the new rule creation wizard is to name each created rule. You can also add a Rule comment. This information will be stored in the Exchange server log.

2.2 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 server performance.



Log files

☐ Synchronized writing without using cache

Content

☐ Log rule application

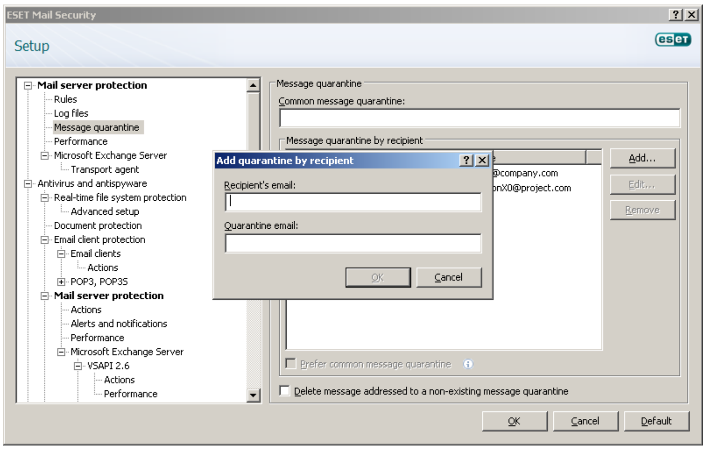
☐ Log performance

☐ Log diagnostic information

Select the Synchronized writing without cache use option to disable storage of log entries in the log cache. You can specify the type of information stored in the log files in the **Content** menu.

2.3 Message quarantine

The **Message quarantine** mailbox is a special mailbox defined by the system administrator to store potentially infected messages and SPAM. Messages stored in quarantine are harmless to the system. They can be analyzed and cleaned later using a newer virus signature database. The quarantine mailbox should have a dedicated database and separate Active Directory user.



Message quarantine

Common message quarantine:

Message quarantine by recipient

@company.com

onX0@project.com

Add quarantine by recipient

Recipient's email:

Quarantine email:

OK Cancel

☐ Prefer common message quarantine

☐ Delete message addressed to a non-existing message quarantine

You can specify the message quarantine address in the Common message quarantine (e.g. main_quarantine@company.com).

In the Message quarantine by recipient field, you can define message quarantine mailboxes for multiple recipients. Every quarantine rule can be enabled or disabled by selecting or deselecting the check box in its row.

NOTE: You can also use system variables in Message Quarantine administration (for example: %PATH%).

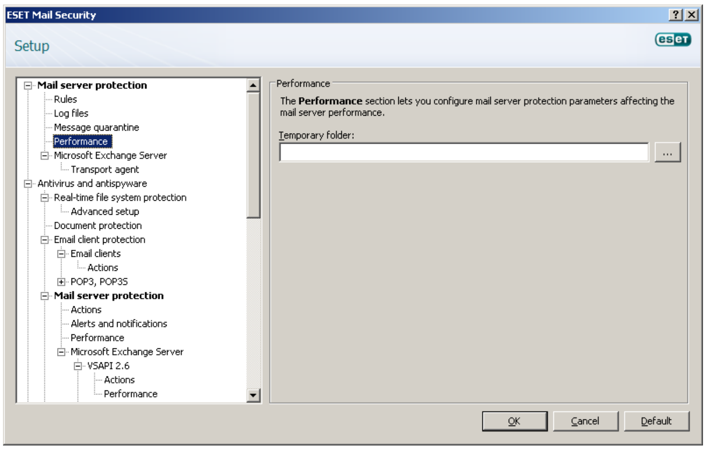
2.3.1 Adding a new quarantine rule

Enter the desired Recipient's email address and the desired Quarantine email address into the appropriate fields.

If you want to delete an email message addressed to a recipient who does not have a quarantine rule applied, you can select the **Delete message addressed to a non-existing message quarantine** option.

2.4 Performance

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



Performance

The **Performance** section lets you configure mail server protection parameters affecting the mail server performance.

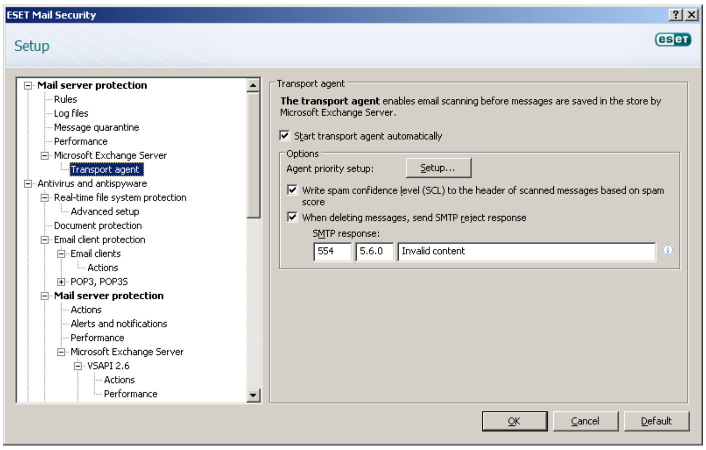
Temporary folder:

NOTE: You can also use system variables in the Performance settings (for example: %SystemRoot%\TEMP).

Warning: In order to reduce potential I/O and fragmentation impact, we recommended placing the Temporary folder on a different hard drive than the one on which Microsoft Exchange is installed.

2.5 Transport Agent

In this section, you can set up automatic startup of the transport agent as well as the agent loading priority. It is only possible to install a transport agent if the server is in one of two roles: Edge Transport or Hub Transport.



Transport agent

The transport agent enables email scanning before messages are saved in the store by Microsoft Exchange Server.

☑ Start transport agent automatically

Options

Agent priority setup:

☑ Write spam confidence level (SCL) to the header of scanned messages based on spam score

☑ When deleting messages, send SMTP reject response

SMTP response: 554 5.6.0 Invalid content

NOTE: Transport agent is not available in Microsoft Exchange 5.5 (VSAPI 1.0).

In the **Agent priority setup** menu, you can set the priority of ESET Mail Security agents started after the Microsoft Exchange startup. The agent priority can have a value between 0 and 32767 (the lower the number, the higher the priority).

Write spam confidence level (SCL) to the header of scanned messages based on spam score – SCL is a normalized value assigned to a message that indicates the likelihood of the message being spam (based on the characteristics of the message header, its subject, content, etc.).

The **When deleting messages, send SMTP reject response** option:

- If unchecked, the server sends an OK SMTP response to the sender's Mail Transfer Agent (MTA) in the format '*250 2.5.0 – Requested mail action okay, completed*' and then performs a silent drop

- If checked, an SMTP reject response is sent back to the sender's MTA. You can type a response message in the following format:

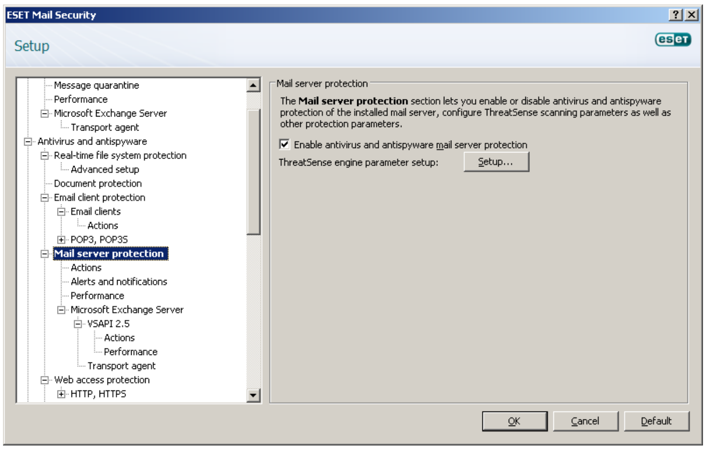
Primary response code	**Enhanced status code**	**Description**
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted: local error in processing
550	5.5.0	Requested action not taken: mailbox unavailable

Warning: Incorrect syntax of the SMTP response codes can lead to malfunctioning of program components and decrease effectiveness.

NOTE: You can also use system variables when configuring SMTP Reject Responses.

3. Antivirus and antispyware settings

You can enable antivirus and antispyware mail server protection by selecting the **Enable antivirus and antispyware mail server protection** option.



Mail server protection

The **Mail server protection** section lets you enable or disable antivirus and antispyware protection of the installed mail server, configure ThreatSense scanning parameters as well as other protection parameters.

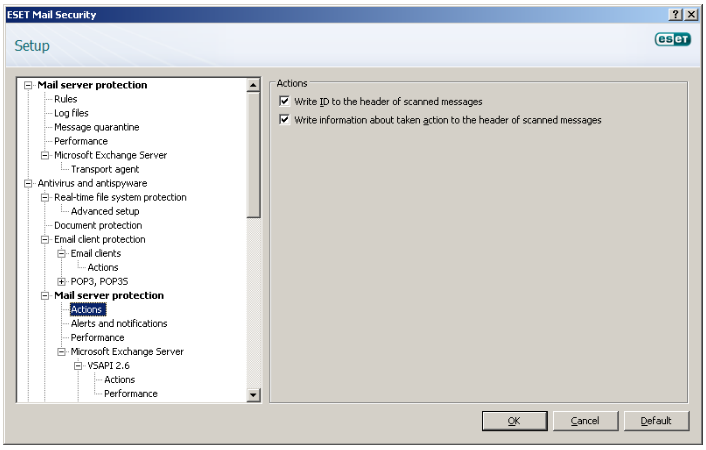
☑ Enable antivirus and antispyware mail server protection

ThreatSense engine parameter setup: Setup...

3.1 ThreatSense engine parameter setup

3.2 Actions

In this section you can choose to attach a scan task ID and additional information to the header of scanned messages.



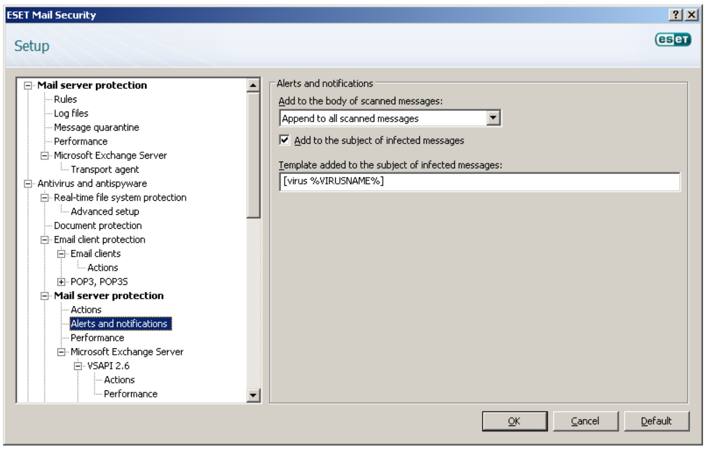
Actions

☑ Write ID to the header of scanned messages

☑ Write information about taken action to the header of scanned messages

3.3 Alerts and notifications

ESET Mail Security allows you to append text to the original subject or body of infected messages.



Alerts and notifications

Add to the body of scanned messages: Append to all scanned messages

☑ Add to the subject of infected messages

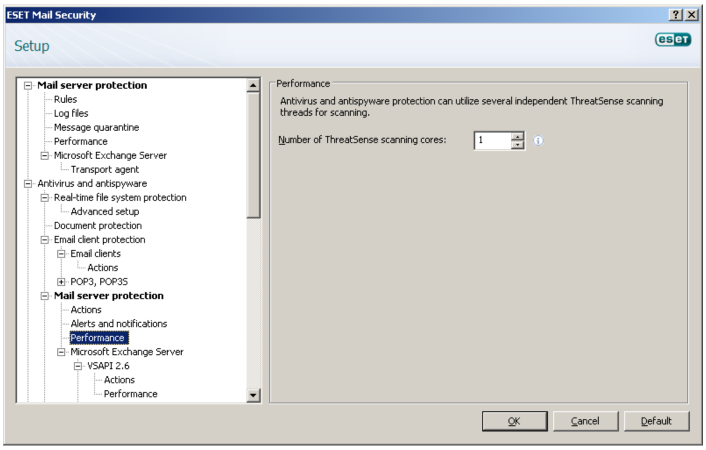
Template added to the subject of infected messages: [virus %VIRUSNAME%]

By enabling **Add to the subject of infected messages**, ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template added to the subject of infected messages** text field (by default [virus %VIRUSNAME%]).

NOTE: You can also use system variables when adding a template to the message subject.

3.4 Performance

In this section, you can set the number of ThreatSense scanning cores that should be used for virus scanning. More threads on multiprocessor machines can increase the scan rate.



Performance

Antivirus and antispyware protection can utilize several independent ThreatSense scanning threads for scanning.

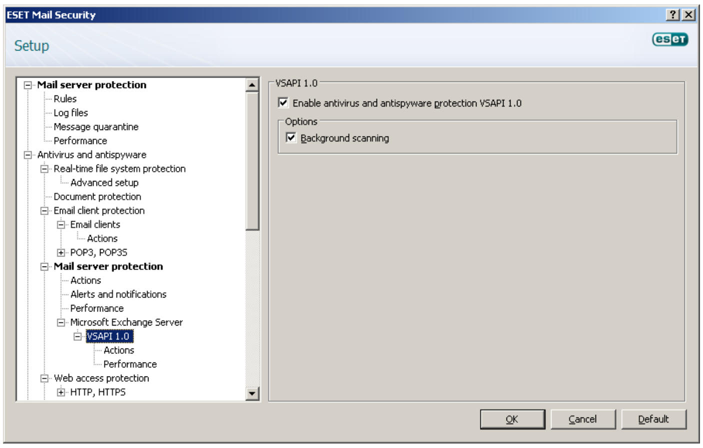
Number of ThreatSense scanning cores: 1

3.5 Virus-Scanning Application Programming Interface (VSAPI)

Exchange provides a mechanism to make sure that every message component is scanned against the current virus signature database. If a message component is not scanned, its corresponding component is submitted to the scanner before the message is released to the client. Every supported version of Microsoft Exchange (5.5/2000/2003/2007) offers a different version of VSAPI.

3.5.1 Microsoft Exchange 5.5

This version of Microsoft Exchange includes VSAPI version 1.0. The user can specify what **Actions** should be taken with an infected message that cannot be cleaned.



VSAPI 1.0

☑ Enable antivirus and antispyware protection VSAPI 1.0

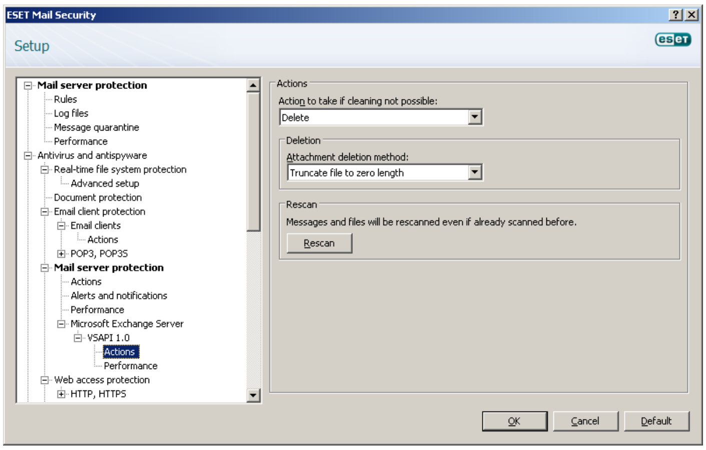
Options

☑ Background scanning

The **Background scanning** option allows scanning of all messages in the system background. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message not scanned by the most current virus signature database, Exchange sends the message to ESET Mail Security to scan it before opening the message in your e-mail client. Background scanning can affect system load (scanning is performed after each virus signature database update).

3.5.1.1 Actions

In this section you can specify the actions to be performed when a message and/or attachment is evaluated as infected.



Actions

Action to take if cleaning not possible: Delete

Deletion

Attachment deletion method: Truncate file to zero length

Rescan

Messages and files will be rescanned even if already scanned before.

Rescan

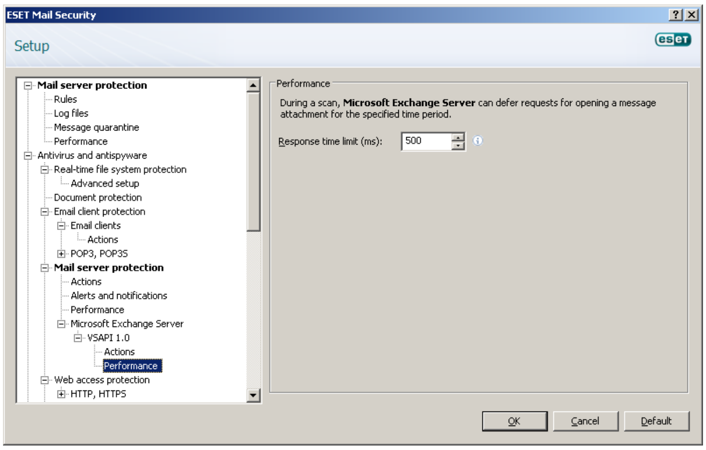
The **Actions to take if cleaning not possible** field allows you to block infected content or delete the message. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup > Cleaning**) did not clean the message.

The **Deletion** option allows you to truncate a file attachment to zero size or replace an infected file with a virus protocol or rule description.

By activating **Rescan**, you can scan messages and files that have already been scanned again.

3.5.1.2 Performance

During a scan, Microsoft Exchange Server allows you to limit a time for opening message attachments. This time is set in the **Response time limit (ms)** field.



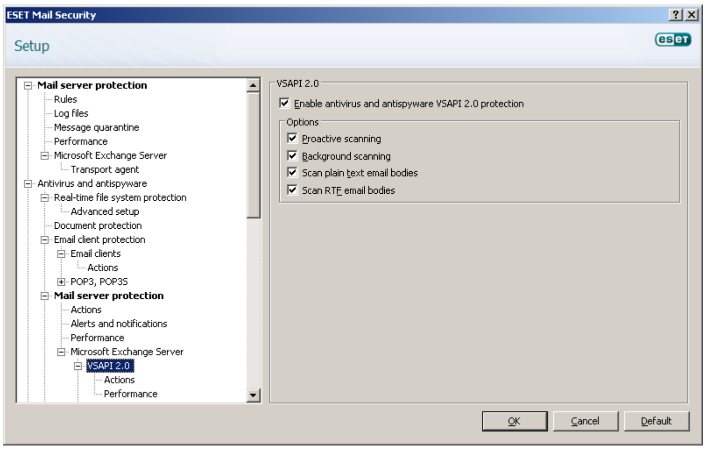
Performance

During a scan, **Microsoft Exchange Server** can defer requests for opening a message attachment for the specified time period.

Response time limit (ms): 500

3.5.2 Microsoft Exchange 2000

This version of Microsoft Exchange includes VSAPI version 2.0. The user can specify what **Actions** should be taken with an infected message that cannot be cleaned.



VSAPI 2.0

☑ Enable antivirus and antispyware VSAPI 2.0 protection

Options

☑ Proactive scanning

☑ Background scanning

☑ Scan plain text email bodies

☑ Scan RTF email bodies

If the **Proactive scanning** option is enabled, new inbound messages will be scanned in the same order in which they were received.

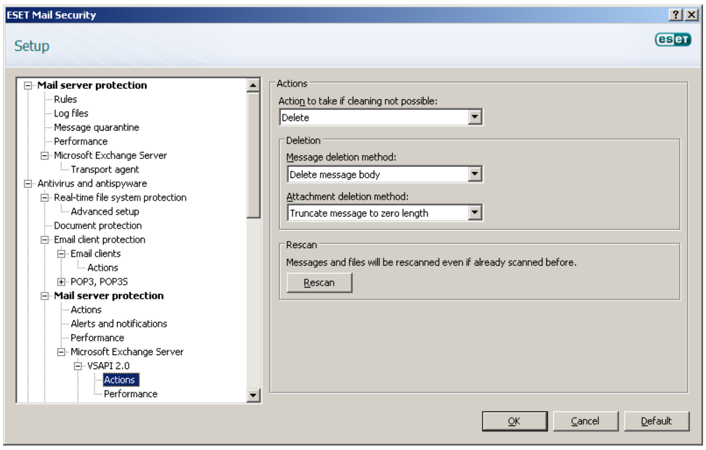
The **Background scanning** option allows the scanning of all messages in the background. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used.

If you want to scan plain text messages, select the **Scan plain text email bodies** option.

Enabling the **Scan RTF email bodies** option activates scanning of RTF message bodies.

3.5.2.1 Actions

In this section you can specify the actions to be performed when a message and/or attachment is evaluated as infected.



Actions

Action to take if cleaning not possible: Delete

Deletion

Message deletion method: Delete message body

Attachment deletion method: Truncate message to zero length

Rescan

Messages and files will be rescanned even if already scanned before.

Rescan

The **Actions to take if cleaning not possible** field allows you to block infected content or delete the message. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup > Cleaning**) did not clean the message.

The **Message deletion method** option offers the choice to either delete the message body or rewrite the message body with action information.

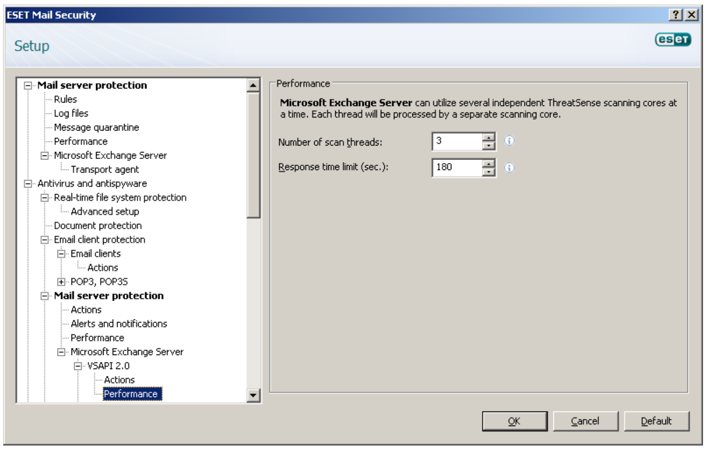
Attachment deletion method lets you decide to delete the message, truncate file attachment to zero size or replace the infected file with action information.

By activating **Rescan**, you can scan messages and files that have already been scanned again.

3.5.2.2 Performance

In this section you can set the number of independent scan threads used at a single time and also set the time during which

Microsoft Exchange Server can defer requests for opening message attachments. This time is set in the **Response time limit (sec.)** input field. More threads on multiprocessor machines can increase the scan rate. For the best program performance we advise using an equal number of ThreatSense scanning cores and scanning threads.



Performance

Microsoft Exchange Server can utilize several independent ThreatSense scanning cores at a time. Each thread will be processed by a separate scanning core.

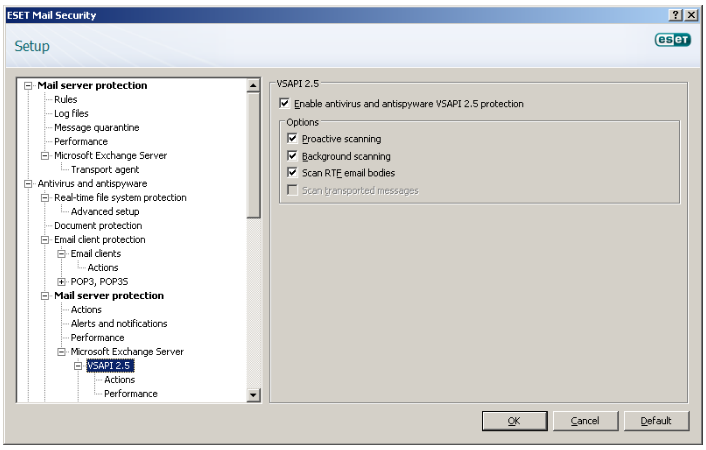
Number of scan threads: 3

Response time limit (sec.): 180

NOTE: To determine the **Number of scan threads** the Microsoft Exchange provider recommends, use the following formula: [number of physical processors] x 2 + 1.

3.5.3 Microsoft Exchange 2003

This version of Microsoft Exchange includes VSAPI version 2.5. The user can specify what **Actions** should be taken with an infected message that cannot be cleaned.



VSAPI 2.5

☑ Enable antivirus and antispyware VSAPI 2.5 protection

Options

☑ Proactive scanning

☑ Background scanning

☑ Scan RTF email bodies

□ Scan transported messages

If the **Proactive scanning** option is checked, new inbound messages will be scanned in the same order in which they were received.

The **Background scanning** option allows the scanning of all messages in the background. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used.

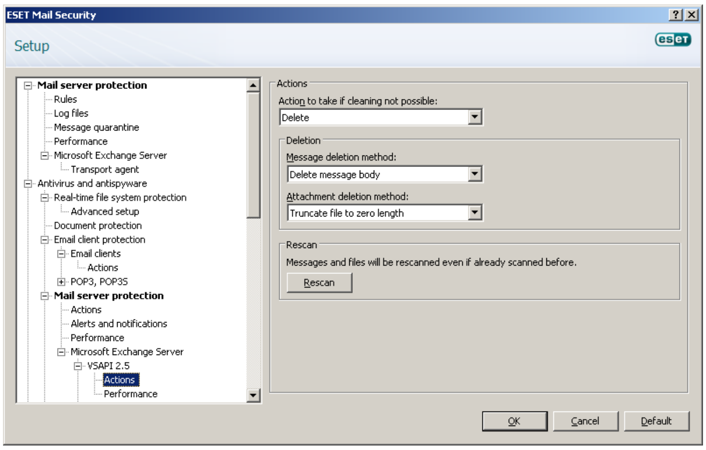
If you want to scan plain text messages, select the **Scan plain text email bodies** option.

Enabling the **Scan RTF email bodies** option activates scanning of RTF message bodies. RTF message bodies may contain macro viruses.

The **Scan transported messages** option enables scanning for messages that are not stored on the local Microsoft Exchange server and are delivered to other e-mail servers through the local Exchange server. If scanning for transported messages is enabled, XMON also scans these messages. This option is only available when the transport agent is disabled.

3.5.3.1 Actions

In this section you can specify the actions to be performed if a message and/or attachment is evaluated as infected.



Actions

Action to take if cleaning not possible: Delete

Deletion

Message deletion method: Delete message body

Attachment deletion method: Truncate file to zero length

Rescan

Messages and files will be rescanned even if already scanned before.

The **Actions to take if cleaning not possible** field allows you to block infected content or delete the message. This action will be applied only if the automatic cleaning (in **ThreatSense engine parameter setup > Cleaning**) did not clean the message.

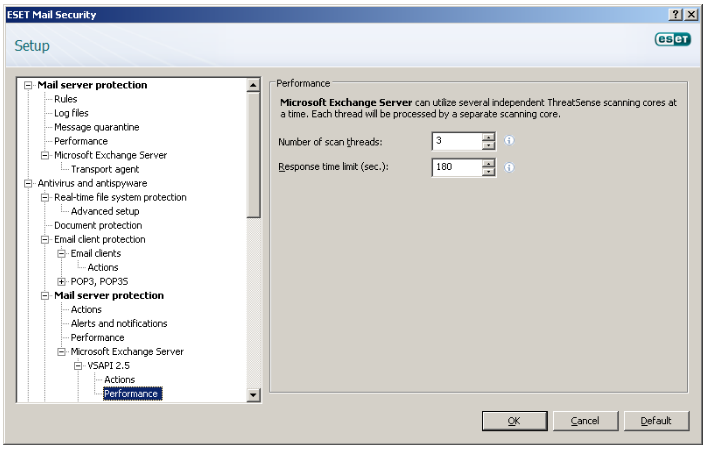
The **Message deletion method** option offers the choice to either delete the message body or rewrite the message body with action information.

Attachment deletion method lets you decide to delete the message, truncate file attachment to zero size or replace the infected file with action information.

By activating **Rescan**, you can scan the messages and files that have already been scanned again.

3.5.3.2 Performance

In this section, you can set the number of independent scan threads used at a single time and a time limit during which the Exchange Server can defer requests for opening message attachments. This time is set in the **Response time limit (sec.)** input field. More threads on multiprocessor machines can increase the scan rate. For the best program performance, we advise using an equal number of ThreatSense scanning cores and scanning threads.



Performance

Microsoft Exchange Server can utilize several independent ThreatSense scanning cores at a time. Each thread will be processed by a separate scanning core.

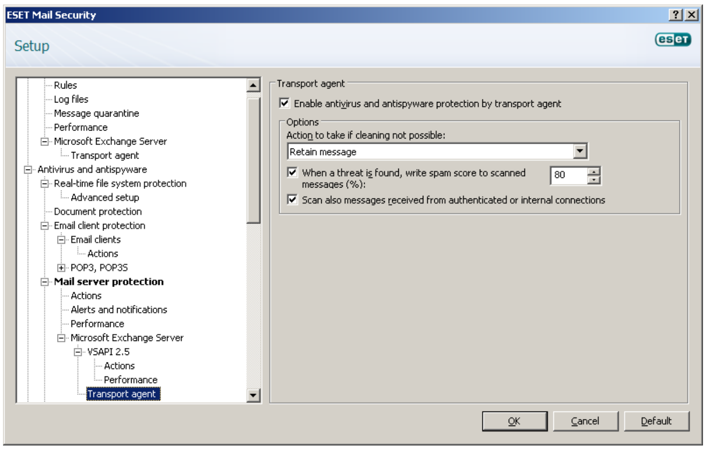
Number of scan threads: 3

Response time limit (sec.): 180

NOTE: To determine the **Number of scan threads** the Microsoft Exchange provider recommends, use the following formula: [number of physical processors] x 2 + 1.

3.5.3.3 Transport Agent

In this section, you can enable antivirus and antispyware protection by the transport agent.



Transport agent

☑ Enable antivirus and antispyware protection by transport agent

Options

Action to take if cleaning not possible: Retain message

☑ When a threat is found, write spam score to scanned messages (%): 80

☑ Scan also messages received from authenticated or internal connections

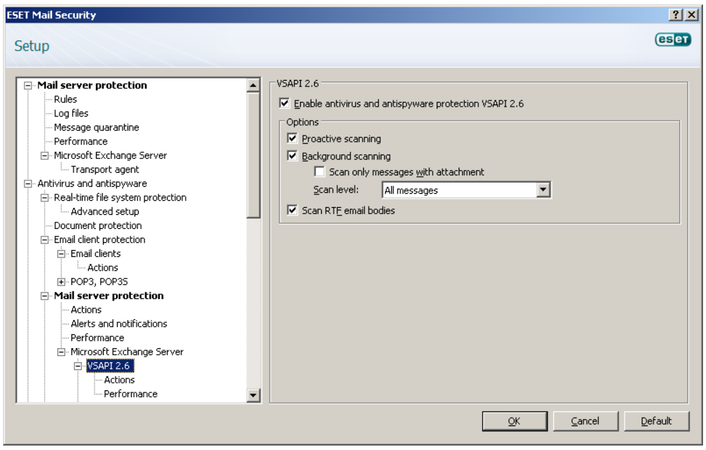
If a message cannot be cleaned, you can delete it, send it to the quarantine mailbox or retain it.

If a threat is found, you can choose to write a spam score to the scanned message and specify the value (in %).

You can also choose to scan messages received from authenticated or local servers.

3.5.4 Microsoft Exchange 2007

This version of Microsoft Exchange includes VSAPI version 2.6. The user can specify what **Actions** should be taken with an infected message that cannot be cleaned.



VSAPI 2.6

☑ Enable antivirus and antispyware protection VSAPI 2.6

Options

☑ Proactive scanning

☑ Background scanning

□ Scan only messages with attachment

Scan level: All messages

☑ Scan RTF email bodies

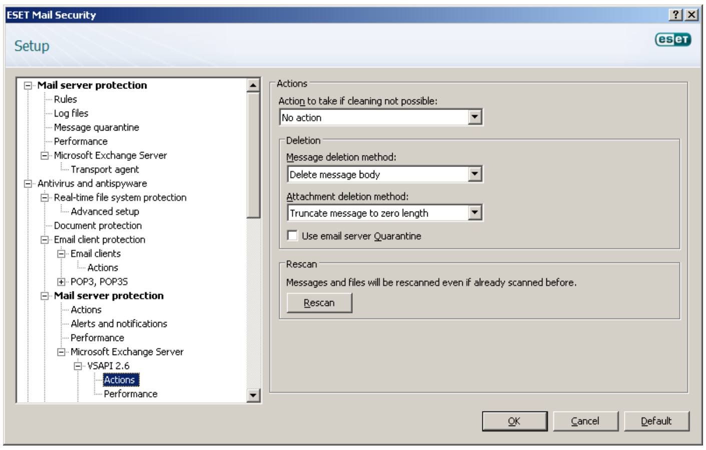
If the **Proactive scanning** option is enabled, new inbound messages will be scanned in the same order in which they were received.

The **Background scanning** option allows the scanning of all messages in the background. Microsoft Exchange Server keeps a record of scanned messages and the version of the virus signature database used. You can choose to **Scan only messages with attachment** and filter based on time received.

Enabling the **Scan RTF email bodies** option activates scanning of RTF message bodies. RTF message bodies may contain macro viruses.

3.5.4.1 Actions

In this section you can specify the actions to take if a message and/or attachment is evaluated as infected.



Actions

Action to take if cleaning not possible: No action

Deletion

Message deletion method: Delete message body

Attachment deletion method: Truncate message to zero length

□ Use email server Quarantine

Rescan

Messages and files will be rescanned even if already scanned before.

Rescan

The **Actions to take if cleaning not possible** field allows you to block infected content or delete the message. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup > Cleaning**) did not clean the message.

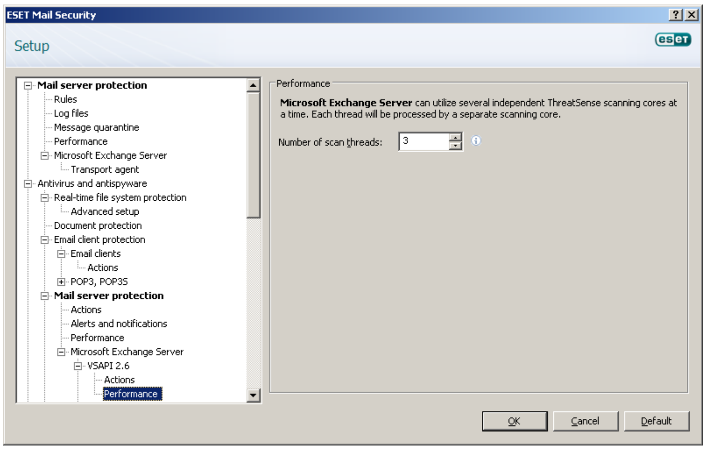
The **Message deletion method** option offers the choice to either delete the message body or rewrite the message body with action information.

Attachment deletion method lets you decide to delete the message, truncate file attachment to zero size or replace the infected file with action information.

By activating **Rescan**, you can scan messages and files that have already been scanned again.

3.5.4.2 Performance

In this section you can set the number of independent scan threads used at a single time and a time limit during which the Exchange Server can defer requests for opening message attachments. This time is set in the **Response time limit (sec.)** input field. More threads on multiprocessor machines can increase the scan rate. For the best program performance, we advise using an equal number of ThreatSense scanning cores and scanning threads.



Performance

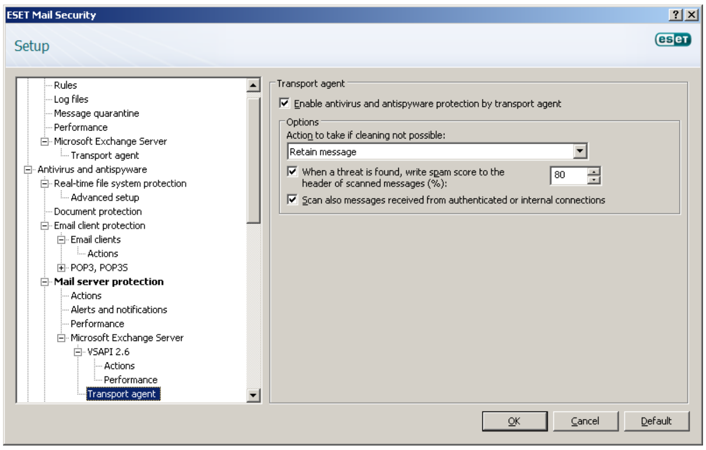
Microsoft Exchange Server can utilize several independent ThreatSense scanning cores at a time. Each thread will be processed by a separate scanning core.

Number of scan threads: 3

NOTE: To determine the **Number of scan threads** the Microsoft Exchange provider recommends, use the following formula: [number of physical processors] x 2 + 1.

3.5.4.3 Transport Agent

In this section you can enable or disable antivirus and antispyware protection by the transport agent. It is only possible to install a transport agent if the server is in one of two roles: Edge Transport or Hub Transport.



Transport agent

☑ Enable antivirus and antispyware protection by transport agent

Options

Action to take if cleaning not possible: Retain message

☑ When a threat is found, write spam score to the header of scanned messages (%): 80

☑ Scan also messages received from authenticated or internal connections

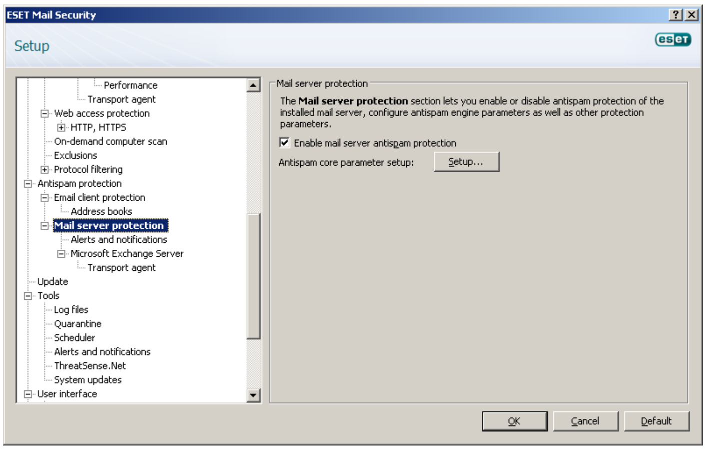
If the message cannot be cleaned, you can delete it, send it to the quarantine mailbox or retain it.

If a threat is found, you can choose to write a spam score to the scanned message and specify the value (in %).

You can also choose to scan messages received from authenticated or local servers.

4. Antispam settings

In the Mail server protection section you can enable spam protection for the installed mail server, configure antispam core parameters and set other levels of protection.



Mail server protection

The **Mail server protection** section lets you enable or disable antispam protection of the installed mail server, configure antispam engine parameters as well as other protection parameters.

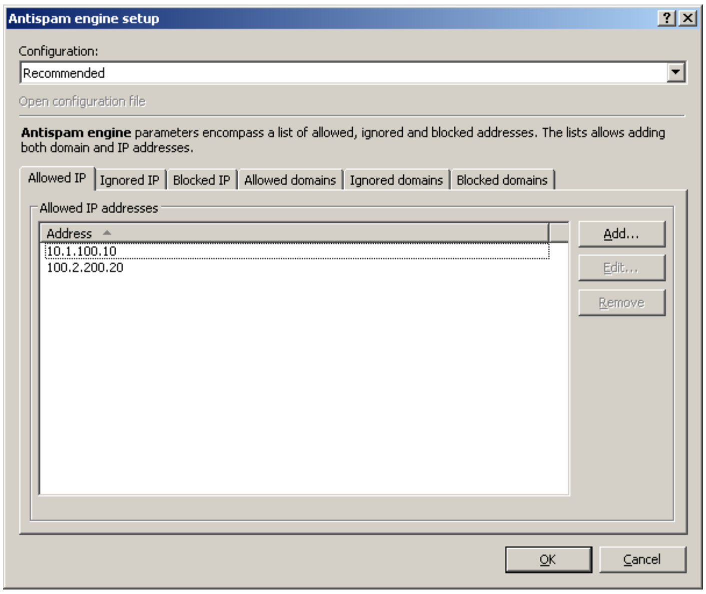
☑ Enable mail server antispam protection

Antispam core parameter setup: Setup...

4.1 Antispam core parameter setup

In this section you can choose from a set of preconfigured profiles that may match your needs. The list of profiles is loaded from the antispam module.

You can also define allowed, ignored and blocked email addresses.



Configuration: Recommended

Open configuration file

Antispam engine parameters encompass a list of allowed, ignored and blocked addresses. The lists allows adding both domain and IP addresses.

Allowed IP addresses

Address
10.1.100.10
100.2.200.20

The **Recommended** profile is comprised of the recommended settings, striking a balance between security and impact on system performance.

The **Most accurate** profile is focused solely on mail server security. This profile requires more system resources than the **Recommended** profile.

The **Fastest** profile is preconfigured for minimal usage of system resources, achieved through the disabling of some scanning features.

Custom > Open configuration file allows a user to edit the *spamcatcher.conf* file. This option is recommended for advanced users only.

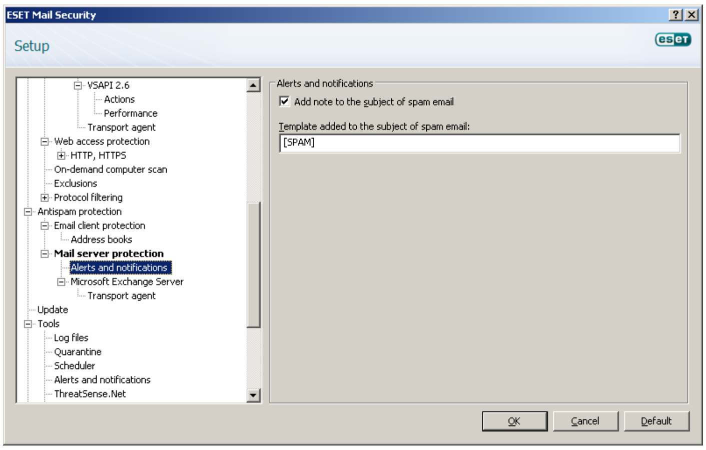
In the **Allowed IP** and **Allowed domains** you can specify IP and domain addresses from which the server will always allow message delivery.

In the **Ignored IP** and **Ignored domains** you can specify IP and domain addresses that will not be examined through the blocked list.

In the **Blocked IP** and **Blocked domains** you can specify IP and domain addresses from which the server will always block the message.

4.2 Alerts and notifications

Each email scanned by ESET Mail Security and evaluated as spam can be marked by appending a tag message to the email subject. Apart from the default [SPAM] tag, you can define your own string.



Alerts and notifications

☑ Add note to the subject of spam email

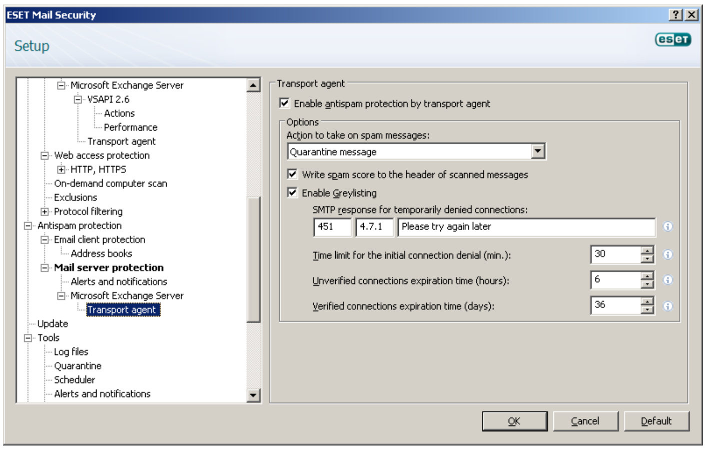
Template added to the subject of spam email: [SPAM]

NOTE: You can also use system variables when adding a template to the message subject.

4.3 Transport agent

In this section you can set up options for spam protection using the transport agent.

NOTE: The transport agent is not available in Microsoft Exchange 5.5.



Transport agent

☑ Enable antispam protection by transport agent

Options

Action to take on spam messages: Quarantine message

☑ Write spam score to the header of scanned messages

☑ Enable Greylisting

SMTP response for temporarily denied connections: 451 4.7.1 Please try again later

Time limit for the initial connection denial (min.): 30

Unverified connections expiration time (hours): 6

Verified connections expiration time (days): 36

You can take any of the following actions with spam messages:

- Retain the message even if it is marked as spam
- Send the message to the quarantine mailbox
- Delete the message

If you want to include information about a message's spam score in its header, enable the **Write spam score to scanned messages** option.

The **Enable Greylisting** function activates a feature that protects users from spam. The transport agent will send a "*temporarily reject*" SMTP return value (default is 451/4.7.1) for any received email that is not from a recognized sender. A legitimate server will try to resend the message after a delay. Spam servers will typically not attempt to resend the message, as they usually go through thousands of email addresses and do not waste time resending.

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

Example of SMTP response message:

Primary response code	**Enhanced status code**	**Description**
451	4.7.1	Requested action aborted: local error in processing

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

Time limit for the initial connection denial (min.) defines a time period during which the message will be refused. After the specified delay, the message will be successfully received.

Unverified connections expiration time (hours) defines the time during which the triplet data will be stored. A valid server must resend the requested message during this period.

Verified connections expiration time (days) defines the number of days during which the triplet information will be stored. Emails from this sender will be received without any delay.

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