we protect digital worlds

NOD32
antivirus system

ESET NOD32 Antivirus for MS Exchange Server

Installation

ESET, spol. s r. o.
Svoradova 1, 811 03 Bratislava, Slovak Republic

http://www.eset.sk/en

Technical Support Worldwide:
http://www.eset.com/support
Technical Support for Europe:
http://www.eset.eu/support

REV.20071114-002

1. Introduction

ESET NOD32 Antivirus for MS Exchange Server is ESET NOD32 Antivirus version designed for scanning e-mail traffic routed by the MS Exchange Servers.

The major differences between the ESET NOD32 Antivirus 2.7 and the ESET NOD32 Antivirus for MS Exchange Server include a module XMON and the absence of IMON and EMON modules.

This document describes the XMON module. Before reading this document, please read the ESET NOD32 Antivirus 2.7 user guide first.

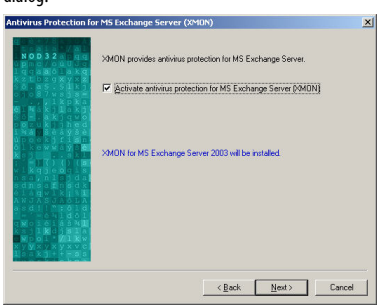
As of version 2.71, the XMON module provides antivirus protection for MS Exchange Server in two flavors – a 32-bit for MS Exchange Server 5.5 SP3 and higher, 2000 SP 1 and higher and 2003 (xmon.dll), and a 64-bit for MS Exchange Server 2007 (xmon64.dll).

The XMON module checks the MS Exchange Server e-mail communication via its antivirus interface VSAPI or external Control Center scanning core.

2. Installation

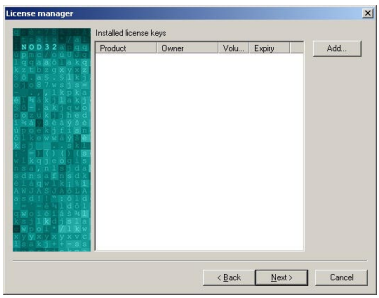
If you are running any previous version of the ESET NOD32 Antivirus for Exchange Server, the new one can be installed over (if it is version 2.0 or higher).

The installation wizard will help you to install the NOD32 for MS Exchange Server. It displays the following dialog:



If you want to install XMON, check the Activate antivirus protection for MS Exchange Server (XMON) checkbox. To activate the XMON service, you need the license file provided by the provider or distributor upon purchase of the program.

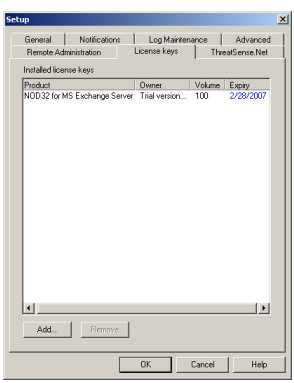
The license file is entered in the next step. If your License file is valid, click *Add* and list the license file.



This screen is present in all installation scenarios.

Additional Activation of XMON:

If you have not activated the antivirus protection for MS Exchange server, you can do it additionally by adding the license file in the License manager. For License manager click on ESET NOD32 Antivirus system tools in the ESET NOD32 Antivirus Control Center and choose ESET NOD32 Antivirus system setup/ setup. After adding the license file, XMON will be activated.

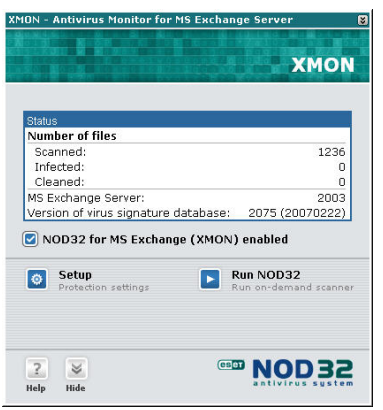


3. XMON

The Main Window

To open the XMON main window, click on the XMON icon in the Control Center window. If the XMON is displayed in grey color, the MS Exchange Server is not present on the local computer or the MS Exchange server version is not supported by XMON. XMON is displayed in grey color also if the XMON module is not activated (it is not set, or the license file has expired). In these cases XMON cannot scan e-mails. If the XMON is displayed in red color; the XMON module is not active. To activate the XMON, check the Activate Control checkbox in the main window.

The main XMON window shows the number of scanned, infected and cleaned files (a file is each e-mail message and its attachments). The main window also displays MS Exchange version running on the local server and the virus signature database version (with the date of the last update in the parentheses).



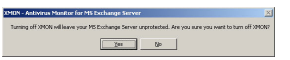
• **Active control** – check box for XMON activation. To activate the XMON, mark the check box. To disable it, uncheck it. Before XMON deactivation you will be requested to confirm its shutdown.

• **Settings** – enables you to alter the default XMON settings

• **Run NOD32** – activates the NOD32 on–demand scanner

Before XMON deactivation you will be requested to confirm its shutdown. If you really want to turn off XMON, press Yes.

Note: MS Exchange Server communicates with the antivirus scan using the system database registry, which is being checked in approximately one minute intervals. Turning XMON on and off, as well as any change in the settings will take about a minute to take effect.

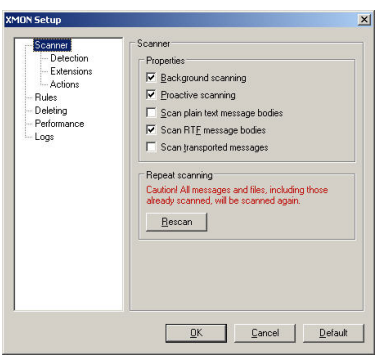


SETTINGS

The left part of the XMON Settings window shows eight possible setting areas of XMON. The setting parameters in each setting area are shown in the right part of the window.

The MS Exchange server checks the settings of the XMON module each minute, so the new XMON settings come into effect after a few seconds.

Scanner



The Scanner page shows the following properties:

• **Background scanning** – if checked, all the messages are scanned in the background. XMON keeps track of what messages it scanned and the version of virus database it used. If you are opening a message not scanned by the most current virus database, XMON scans it before opening it in your e-mail client. The background testing means that XMON keeps scanning all the messages from

the Exchange server, so when you are about to open the message, it has already been scanned. Background scanning can influence system load (scanning is done by each virus signature database update). When scanning the store database in the day mode, the system might be slowed down. In this case we recommend using scheduled scanning outside working hours. By scheduled scanning, the option has to be disabled.

• **Proactive scanning** – new inbound messages are scanned in the order they are received. If this checkbox is marked and a user opens a message that has not been scanned yet, this message is scanned before the other messages waiting in the scanning queue.

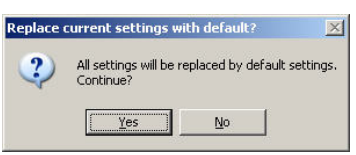
• **Scan plain text message bodies** – enables scanning plain text messages

• **Scan RTF message bodies** – enables scanning RTF message bodies. The RTF message bodies may contain macroviruses

• **Scan transported messages** – When checked, XMON scans also messages that are not stored on the local MS Exchange server and are delivered to other e-mail servers through the local Exchange server. The MS Exchange Server can be set as a gateway and used just to deliver messages to the other e-mail servers. If Scan of the transported messages is turned on, XMON scans also these messages.

• **Repeat scanning button** – By clicking the Repeat scanning button all the messages stored on the local MS Exchange server are scanned again. Upon each virus database update the XMON scans all the messages stored on the Exchange server again as well. It is useful for example after changing the rules.

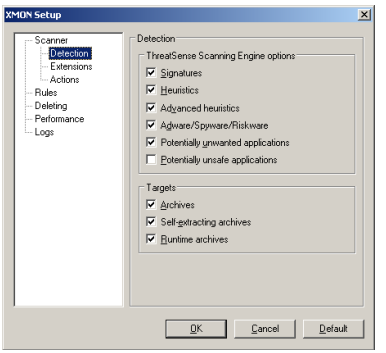
• **Default button** – By clicking the Default button, all the properties on Scanner page are set to default (factory settings).



When clicking the Default button, a confirmation window will allow you to confirm or reject your selection. By clicking Yes, you will activate the default settings.

Detection

The Detection page contains the settings of detection methods.



The ThreatSense Scanning Engine options section allows you to set the methods for detection of infiltrations used in XMON module. For highest security level check all of them.

• **Signatures** – when checked, XMON uses the signature based infiltration detection

• **Heuristics** – when checked, XMON uses heuristic method based infiltration detection (analysis of file content)

• **Advanced Heuristics** – when checked, XMON uses Advanced Heuristics based infiltration detection. Advanced Heuristics is a new unique set of ESET NOD32 Antivirus system, among others capable of effective detecting internet worms.

• **Adware/Spyware/Riskware** – when checked, XMON detects also this kind of bothering malware

• **Potentially unsafe applications** - this classification is used for commercial legitimate software. It includes programs such as remote access tools, password-cracking applications, and keyloggers (programs recording all keystrokes).

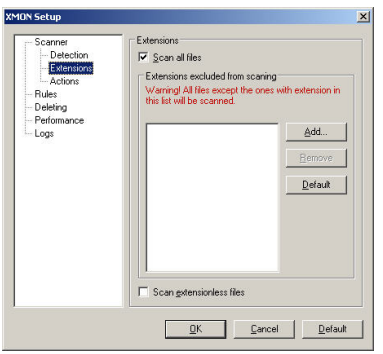
• **Potentially unwanted applications** - Potentially unwanted applications are not necessarily intended

to be malicious, but they may affect the performance of your computer. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (when compared to the state before their installation).

In the Target section check the types of attachments to be scanned (**Archives, Self-extracting archives, Runtime archives**). When scanning archives the scanning procedure is more time consuming, because the archive must be opened for scanning.

Extensions

The Extensions page enables you to set which file types should be included in virus scanning.



• **Scan all files** – marking this check box, XMON will scan all files types found in message attachments. The file types list will show file types excluded from scanning instead of files included in scanning.

• **Add** – enables you to add a new file extension to the file extension list. It displays Add new extension window. To add a new extension use alphanumerical characters and wildcards such as "?" (represents random character) and "*" (represents random order of characters).

• **Remove** – removes the selected file extension from the list

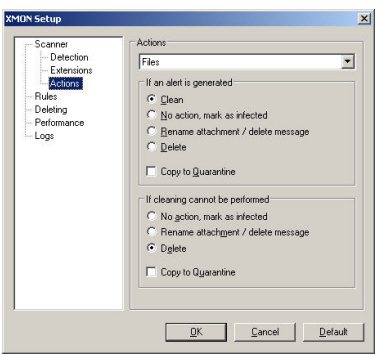
• **Default** – restores the default extension list setting

• **Scan extension–less files** - adds scanning files without extensions

Add a new extension (you can also use wildcards "?" and "*") and click **OK**.

Actions

The Actions page lets you select what actions should be taken upon virus detection. When scan archives option in Detection in the Targets section is activated, this pane contains separate settings for archives and files. The type can be chosen in the pull-down menu.



The When virus is found settings let you select what action should be taken upon virus detection.

• **Clean** – XMON attempts to clean the virus from the infected file. When the attempt fails, the action selected in the When virus cannot be cleaned settings is executed.

• **No action, mark as infected** – when selected the Exchange server is notified about the infection and the user cannot open the infected message attachment.

• **Rename attachment/ delete message** – XMON changes the attachment extension, so that it cannot be opened or run. If the message body contains a virus, the message will be deleted.

• **Delete** – XMON deletes the infected message or the attachment if only the attachment is infected. The

deletion process can be adjusted in the Deleting setting page.

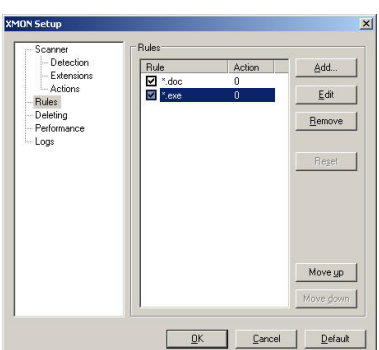
• **Quarantine** – when checked, the infected messages will be stored in Quarantine, where it is harmless. Messages stored in Quarantine can be analyzed and cleaned later using a newer virus signature database.

When virus cannot be cleaned setting is executed, if Clean option in previous menu is set. Some of the infections cannot be cleaned, because the XMON does not have a cleaning procedure for them, or because they do not contain any useful content except virus (currently the most common case). The When virus cannot be cleaned settings lets you select what action should be taken when attempt to clean an infected message fails. (**No action, Mark as infected, Rename attachment/ Delete message, Delete, Quarantine**)

Rules

The Rules settings let you select detailed rules for handling file types. If there is more than one rule for a single file type, the first rule in the list is applied.

Rules are prior to extensions set in Extensions settings, meaning that the each file is at first compared to existing rules. It will be scanned only if no rule is applied (or if the respective rule says that it has to be scanned). The number of rules applied is displayed in the Number column.



• **Add**– enables you to add a new rule

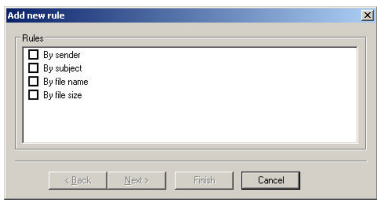
• **Modify**– modifies the selected rule

• **Remove**– removes the selected rule

• **Move up** – moves up the selected rule and increases its priority

• **Move down** – moves down the selected rule and decreases its priority

Adding a new rule will open a wizard, which guides you through the process.



• **Mailbox** – the rule applies to the name of a mailbox

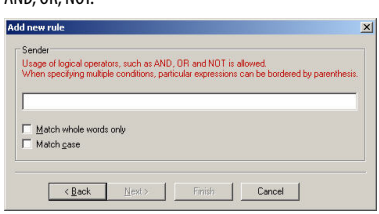
• **Sender of message** – the rule applies to a message sent by the selected sender.

• **Subject of message** – the rule applies to a message with the selected subject line

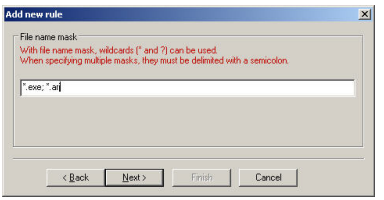
• **File name mask** – File name mask enables you to select a certain file selection

• **File size** – File size enables you to select files from certain size

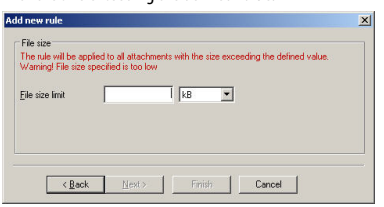
In the strings in the Sender of message and Subject of message it is enough to fill in only a part of a text (if the Match whole words only option is not checked); capital letters are not differentiated (if the option Differentiate capital letters is not checked). When using other than alphanumerical characters, use parentheses and quotes. You can also create conditions using logical operators AND, OR, NOT.



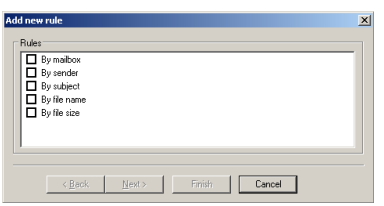
File name mask enables you to select a certain file selection using a mask created from alphanumerical characters and wildcards "?" and "*", e.g. "*.VBS". The rule is applied to files matching this mask. To use more than one mask, separate them by a semicolon.



File size limit enables you to select certain size of attachments. The rule will be applied to all attachments with the size exceeding the defined value.

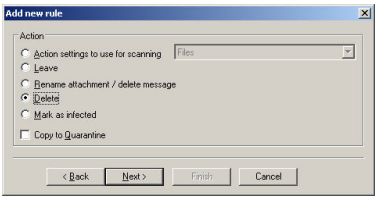


Rule applies to a name of a mailbox and all other procedures connected with its usage are the same as with the other rules.



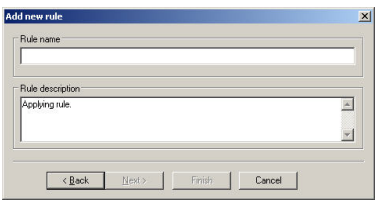
The Action section lets you select what actions should be taken with files matching the above mentioned search criteria.

- **Scan for viruses as** – XMON will scan for viruses in selected file
- **No action** – XMON declares the message to be clean
- **Rename attachment/ delete message** – XMON alters the file extension so that it cannot be opened or run



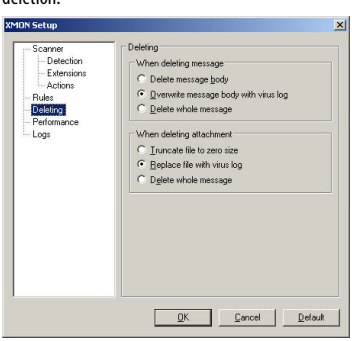
- **Delete** – XMON deletes the selected message
- **Mark as infected** – XMON marks the selected message as infected
- **Quarantine** – The selected message will be stored in Quarantine

Finally, add the rule name and description to be saved in the Exchange server log when the rule is applied.



Deleting

The Deleting page lets you select what action should be made when a message or attached file is selected for deletion.



When deleting message settings lets you select what actions should be taken when the whole message is marked for deletion.

- **Delete message body** – XMON deletes the body of the infected message. The recipient will receive the empty message and also non–infected attachments
- **Overwrite message body with virus protocol** – XMON overwrites the message body with a virus protocol or a rule description.
- **Delete whole message** – XMON deletes the whole message including all attachments

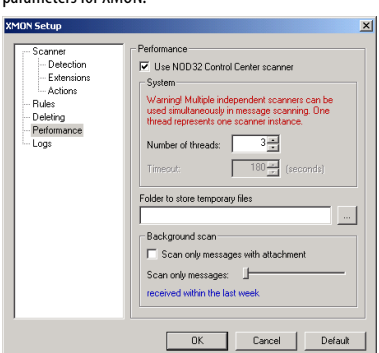
When deleting attachments settings lets you select what action should be taken when a message is marked for deletion.

- **Truncate file to zero size** – XMON truncates the attachment to zero size and lets the recipient see the attachment file name and type.
- **Replace file with virus protocol** – XMON replaces the infected file with a virus protocol or rule description
- **Delete whole message** – XMON deletes the whole message along with all its attachments

Note: If you can not open the Deleting selection (it is displayed in grey), it is not supported by your MS Exchange Server version.

Performance

The Performance page lets you select performance parameters for XMON.



- **Use NOD32 Control Center scanner** - Unlike all the previous versions that would explicitly use the internal scanning core for antivirus scanning, version 2.71 brings an option to utilize external Control Center scanning core as well. With 32-bit versions of MS Exchange Server this feature is optional and it is possible to select it in the Performance section of the XMON setup. With the 64-bit version of MS Exchange Server it is only possible to utilize the external Control Center scanning core. Therefore this option is automatically selected and grayed out.
- **Number of threads** – this parameter lets you select how many threads should be used for virus scanning. More threads on multiprocessor machines can increase the scanning rate. MS Exchange server provider recommends using the following formula to determine the number of threads used: Number of physical processors times 2 plus 1 = number of threads used.
- **Time limit** (for Exchange 5.5) – sets the time interval for running the virus scanner
- **Time limit** (for Exchange 2000 and higher) – a time limit for scanning an individual file
- **Folder to store temporary files** - For the best performance, we recommend that you configure XMON to store temporary files on a physical drive other than the one with the Exchange store. If no folder is specified, XMON will create temporary files in the system temporary folder.

Background scan scope option

MS Exchange Server 2007 provides a way to actively affect antivirus scanning in the background. Therefore the 64-bit XMON module version offers an option to configure the progress and scope of background scanning. However, this option is not available in 32-bit versions of MS Exchange Server and the XMON module; therefore the appropriate controls are inactive and grayed out

Selecting Scan only messages with attachment will limit the background scanning scope only to messages with an attachment. This will also decrease the overall server load while scanning in the background.

Please note that not all infected messages necessarily come with an attachment. However, this will, not decrease protection of the messages in the MS Exchange

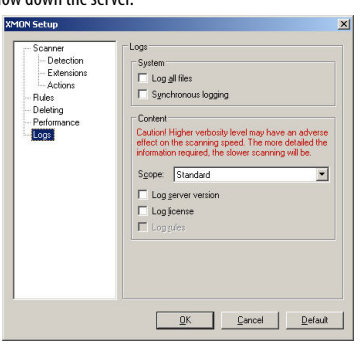
Server store, as messages are also checked when accessed by the user.

Another way to reduce the overall system load is provided by the Scan level option. When enabled, only messages from the specified time interval determined by the date of message receipt will be scanned on the background. It is possible to choose between scanning of all messages regardless the date of receipt, messages received within the last year, 6 months, 3 months, one month or week. Choosing the appropriate background scan level will enable administrators of MS Exchange Server 2007 to tune up the system performance to their needs. Also in this case messages not falling into the specified time interval are not left without antivirus protection, yet they are checked when accessed by the user.

Given the high detection efficiency provided by the ESET NOD32 Antivirus for MS Exchange Server scanning core, we recommend the following: After the initial installation of ESET NOD32 Antivirus for MS Exchange Server, let the scanning run in the background with no restrictions. After certain time (1 - 2 days) tune up background scanning according to the estimated frequency of users accessing older messages and the volume of messages received within the specified time interval.

Protocol

The Protocol settings page lets you select how the virus scanning protocol/log should be assembled. More detailed protocol can contains more information, but it can slow down the server.



• **Log all files** – when checked, all scanned files are listed in the scanning log, including non–infected files

• **Synchronous logging** – when checked, all the log entries are immediately written into the log file without storing them in the log cache

• **Scope** – This setting lets you select what the scope of logging activities. The more detailed the scope, the more activities are written into the log file

• **Log server version** – when checked, XMON writes the server version into the log file

• **Log license** – when checked, XMON writes the XMON license into the log file

• **Log rules** – when checked, XMON writes the list of currently enabled rules into the log file (only in detailed one)

4.Recommended settings:

• Excluding Exchange files from resident protection scanning

XMON scans e-mail messages stored in the MS Exchange Server storage. This storage is saved on the server file system as a single file and using non-standard settings in AMON (on-access scanner) while running on the same server, might lead to a collision between XMON and AMON. To avoid the collision make sure that the AMON module is not set to scan .EDB, .TMP and .EML file types. By default, the mentioned extensions are excluded from scanning. It is also recommended to exclude from scanning directories containing following files and directories:

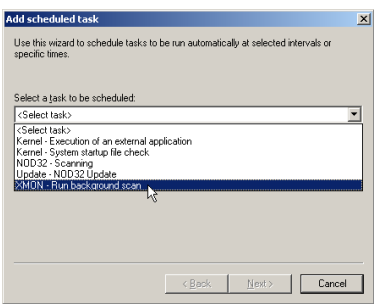
%ProgramFiles%\Exchsrvr\MDBData\
%ProgramFiles%\Exchsrvr\Mtadata\
%ProgramFiles%\Exchsrvr\Server_Name.log
%ProgramFiles%\Exchsrvr\Mailroot
%ProgramFiles%\Exchsrvr\Srsdata
%SystemRoot%\System32\Inetsrv
%ProgramFiles%\Exchsrvr\IMCData

To exclude these file and directories in AMON module, follow these steps:

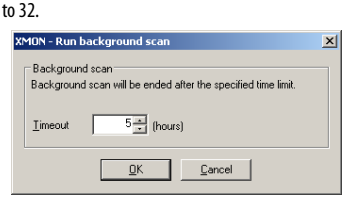
- Click on the Setup button in AMON module
- Click on the Exclusions tab and then on the Add button
- In displayed window click on the Folder or File button (depends on what you want to exclude) and browse for required items.

• Setting the background scanning in the scheduled time

Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When scheduling a Background scanning task you can set the launch time, the number of repetitions as well as other parameters available in the Scheduler/Planner.



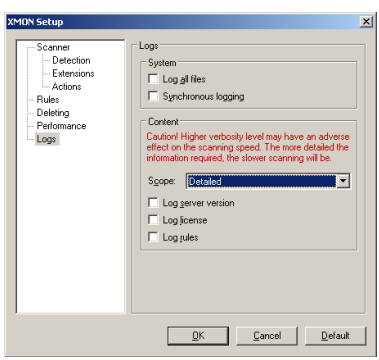
The Background scan task requires one mandatory parameter that specifies the timeout for background scanning. The interval is in hours, within the range from 1 to 32.



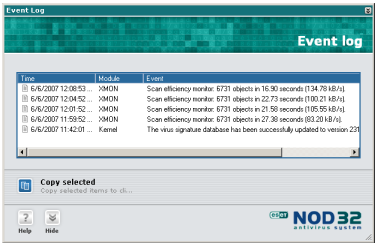
After the task has been scheduled, it will appear in the list of scheduled tasks and as with the other tasks, you can modify its parameters, delete or temporary deactivate the task. If the task is run at the specified time, XMON will allow MS Exchange Server to run background scanning. After the specified timeout has elapsed, XMON will stop MS Exchange Server from scanning in the background. In this interval, it is up to MS Exchange Server to decide whether a background scan will run or not, based on various factors, such as the current system load, the number of active users, etc.

• Performance monitoring

With transition to 64-bit systems, the XMON module has started to support an external Control Center scanning core. This extension applies also to 32-bit version, where the option to utilize the internal scanning core remains. Both approaches to way of utilizing the scanning core have their pros and cons, depending on the systems where they are installed. One of the factors that administrators will consider when choosing between these approaches is the speed of antivirus scanning. Therefore, as of version 2.71 the XMON module can calculate the current performance and report it in the module event log. To log this information, the logging scope must be set to **Detailed**.



XMON will log performance information such as number of scanned objects (messages and attachments), scan time in seconds, scanning speed in kB per seconds, etc. in 5-minute intervals.



Likewise logging results, the monitoring results are also written in a 5-minute interval. They are not accumulated and each benchmark is performed from scratch once the results have been logged.

- **Rename infected files**

It is not recommended to set the default settings for infected files to "rename" while using the option to scan all files (default settings). All infected files with .EXE or .DOC extension would after renaming have the extensions .VEXE or VDOC, so the Server in MS Windows would not be executed after clicking, but the antivirus system at each scan would recognize the files by their content and rename them further (.VVEXE or .VVDOC, etc.). All messages are scanned in the MS Exchange Server storage upon each virus signature database update, the consequent renaming would slow down your computer. It is recommended to exclude from testing at least files with . VV* extensions (not .V extensions – this would include also Visual Basic Script.)