AVG 8.5 Email Server Edition

User Manual

Document revision 85.4 (30.4.2009)

Contents

1. Introduction

This user manual provides comprehensive documentation for **AVG 8.5 Email Server Edition**.

Congratulations on your purchase of AVG 8.5 Email Server Edition!

AVG 8.5 Email Server Edition is one of a range of award winning AVG products designed to provide you with peace of mind and total security for your PC. As with all AVG products **AVG 8.5 Email Server Edition** has been completely re-designed, from the ground up, to deliver AVG's renowned and accredited security protection in a new, more user friendly and efficient way.

AVG has been designed and developed to protect your computing and networking activity. Enjoy the experience of full protection from AVG.

2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG 8.5 Email Server Edition is intended to protect e-mail servers running under the following operating systems:

- Windows 2008 Server Edition (x86 and x64)
- Windows 2003 Server (x86, x64 and Itanium) SP1
- Windows 2000 Server SP4 + Update Rollup 1

(and possibly higher service packs for specific email servers)

2.2. Email Servers Supported

The following e-mail servers are supported:

- ***MS Exchange 2000 Server (with Service Pack 1 or higher) version***

  Note: for Exchange 2000 Server - Service Pack 1 (or higher) needs to be applied before you can use the AVG engine; **AVG for MS Exchange 2000/2003 Server** uses the VSAPI 2.0 (or 2.5 with Exchange 2003 Server) application interface which is covered in this Service Pack.

- ***MS Exchange 2003 Server version***
- ***MS Exchange 2007 Server version***
- ***AVG for Kerio MailServer*** – version 5.x/6.x and higher

2.3. Minimum Hardware Requirements

Minimum hardware requirements for **AVG 8.5 Email Server Edition** are:

- Intel Pentium CPU 1.2 GHz
- 250 MB of free hard drive space (for installation purposes)
- 256 MB of RAM memory

2.4. Uninstall Previous Versions

If you have an older version of AVG Email Server installed, you will need to uninstall it manually before installing **AVG 8.5 Email Server Edition**. You must manually perform the uninstallation of the previous version, using the standard windows functionality.

- From the start menu ***Start/Settings/Control Panel/Add or Remove Programs*** select the correct program from the list of installed software. Be careful to select the correct AVG program for uninstallation. You need to uninstall the Email Server Edition before uninstalling the AVG File Server Edition.

- Once you have uninstalled the Email Server Edition, you can proceed to uninstall your previous version of AVG File Server Edition. This can be done easily from the start menu ***Start/All Programs/AVG/Uninstall AVG***

2.5. MS Exchange Service Packs

Since **AVG for MS Exchange 2000/2003 Server** uses the VSAPI 2.0/2.5 virus scanning interface, you must have the Service Pack 1 (or higher) for MS Exchange 2000 Server applied on your system. Follow the link below to get the latest Service Pack for MS Exchange 2000 Server:

Service Pack for MS Exchange 2000 Server:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

For MS Exchange 2003 Server no additional service pack is needed; however, it is recommended to keep your system as up to date with the latest service packs and hotfixes as possible in order to obtain maximal available security.

Service Pack for MS Exchange 2003 Server (optional):

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

At the beginning of the setup, all system libraries versions will be examined. If it is necessary to install newer libraries, the installer will rename the old ones with a .delete extension. They will be deleted after the system restart.

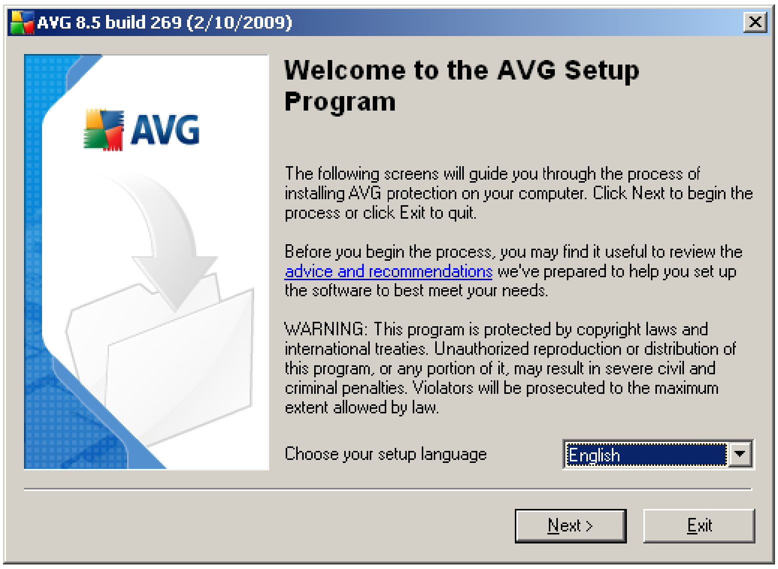
3. AVG Installation Process

To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from the AVG website (at http://www.avg.com/download?prd=msw).

During the installation process you will be asked for your license/sales number. Please make sure you have it available before starting the installation. The sales number can be found on the CD packaging. If you purchased your copy of AVG on-line, your license number will have been delivered to you via e-mail.

Once you have downloaded and saved the installation file on your hard disk, you can launch the installation process. The installation is a sequence of dialog windows with a brief description of what do at each step. In the following, we offer an explanation for each dialog window:

3.1. Installation Launch



AVG 8.5 build 269 (2/10/2009)

Welcome to the AVG Setup Program

The following screens will guide you through the process of installing AVG protection on your computer. Click Next to begin the process or click Exit to quit.

Before you begin the process, you may find it useful to review the advice and recommendations we've prepared to help you set up the software to best meet your needs.

WARNING: This program is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent allowed by law.

Choose your setup language: English

The installation process starts with the ***Welcome*** window. In here you select the language used for the installation process. In the lower part of the dialog window find the ***Choose your setup language*** item, and select the desired language from the drop down menu. Then press the ***Next*** button to confirm and continue to the next dialog.

***Attention:** Here you are choosing the language for the installation process only. You are not selecting the language for the AVG application - that can be specified later on during the installation process!*

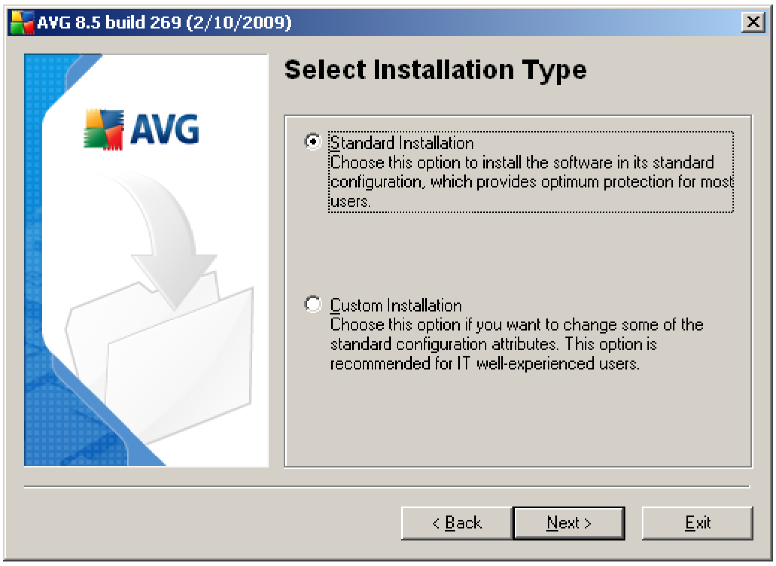
3.2. License Agreement

The ***License Agreement*** dialog provides the full wording of the AVG license agreement. Please read it carefully and confirm that you have read, understood and accept the agreement by pressing the ***Accept*** button. If you do not agree with the license agreement press the ***Don't accept*** button, and the installation process will be terminated immediately.

3.3. Checking System Status

Having confirmed the license agreement you will be redirected to the ***Checking System Status*** dialog. This dialog does not require any intervention; your system is being checked before the AVG installation can start. Please wait until the process has finished, then continue automatically to the following dialog.

3.4. Select Installation Type



Select Installation Type

● Standard Installation
Choose this option to install the software in its standard configuration, which provides optimum protection for most users.

○ Custom Installation
Choose this option if you want to change some of the standard configuration attributes. This option is recommended for IT well-experienced users.

The ***Select Installation Type*** dialog offers the choice of two installation options: ***standard*** and ***custom*** installation.

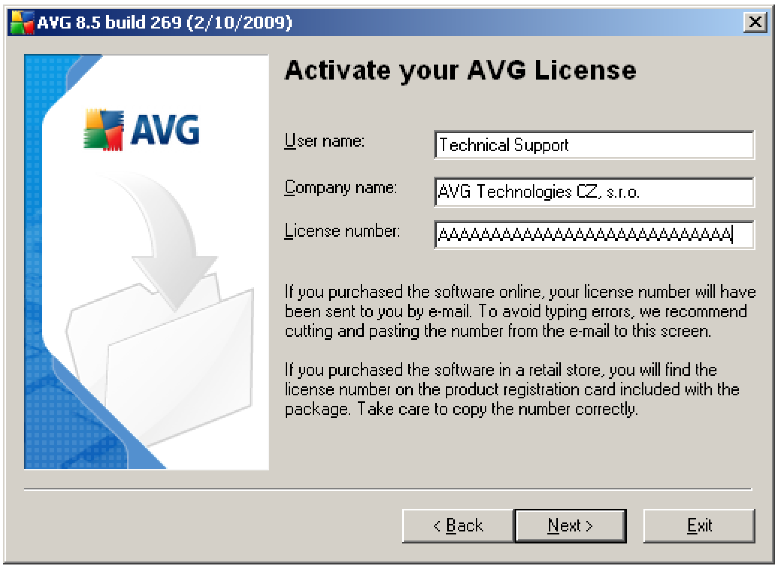
For most users, it is highly recommended to keep to the ***standard installation*** that installs AVG in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of resources. In the future, if the need arises to change the configuration, you will always have the possibility to do so directly in the AVG application.

Custom installation should only be used by experienced users who have a valid reason to install AVG with non-standard settings. E.g. to fit specific system requirements.

3.5. Activate AVG

In the ***Activate your AVG License*** dialog you have to fill in your registration data. Type in your name (***User Name*** field) and the name of your organization (***Company Name*** field).

Then enter your license/sales number into the ***License Number*** text field. The license number will be in the confirmation email that you received after purchasing your AVG on-line. You must type in the number exactly as shown. If the digital form of the license number is available (in the email), it is recommended to use the copy and paste method to insert it.



Activate your AVG License

User name: Technical Support

Company name: AVG Technologies CZ, s.r.o.

License number: AAAAAAAAAAAAAAAAAAAAAAAAAAAAA

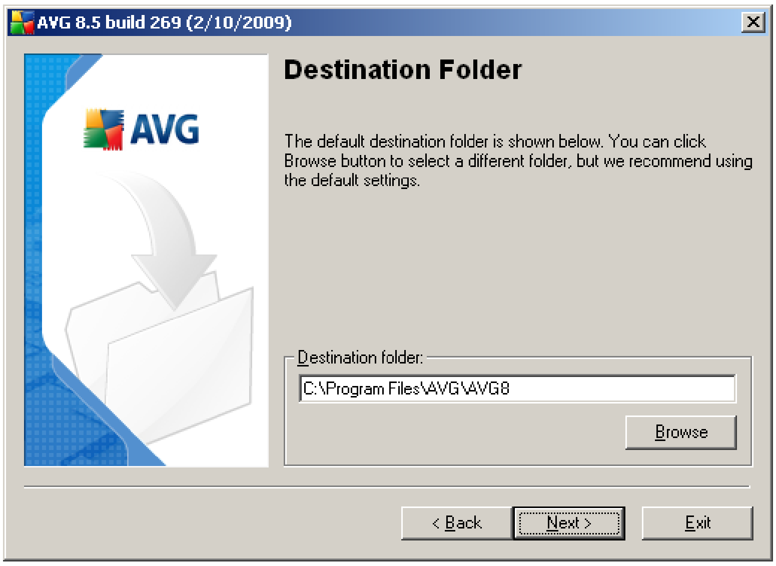
If you purchased the software online, your license number will have been sent to you by e-mail. To avoid typing errors, we recommend cutting and pasting the number from the e-mail to this screen.

If you purchased the software in a retail store, you will find the license number on the product registration card included with the package. Take care to copy the number correctly.

Press the ***Next*** button to continue the installation process.

If in the previous step you have selected the standard installation, you will be redirected directly to the ***Setup Summary*** dialog. If custom installation was selected you will continue with the ***Destination Folder*** dialog.

3.6. Custom Installation - Destination Folder



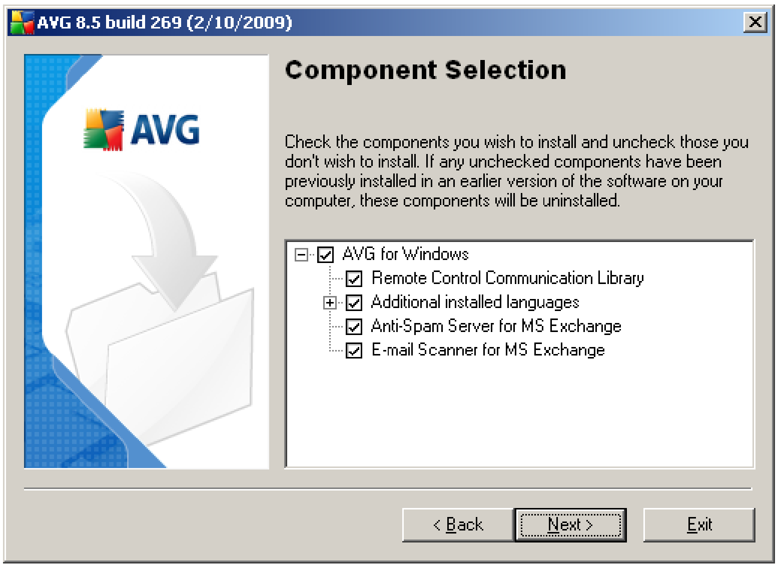
Destination Folder

The default destination folder is shown below. You can click Browse button to select a different folder, but we recommend using the default settings.

Destination folder: C:\Program Files\AVG\AVG8

The ***Destination folder*** dialog allows you to specify the location where AVG should be installed. By default, AVG will be installed to the program files folder located on drive C:. If you want to change this location, use the ***Browse*** button to display the drive structure, and select the respective folder. Press the ***Next*** button to confirm.

3.7. Custom Installation - Component Selection



Component Selection

Check the components you wish to install and uncheck those you don't wish to install. If any unchecked components have been previously installed in an earlier version of the software on your computer, these components will be uninstalled.

- ☑ AVG for Windows
  - ☑ Remote Control Communication Library
  - ☑ Additional installed languages
  - ☑ Anti-Spam Server for MS Exchange
  - ☑ E-mail Scanner for MS Exchange

The ***Component Selection*** dialog displays an overview of all AVG components that can be installed. If the default settings do not suit you, you can remove/add specific components.

However, you can only select from components that are included in your purchased AVG edition. Only those components will be offered to be installed within the Component Selection dialog!

- ***Remote Control Communication Library*** - if you intend to connect AVG to an AVG DataCenter (AVG Network Editions), then you need to select this option.

  Note: *Not all e-mail servers can be managed remotely!*

- ***Additional Installed Languages*** - you can define which language(s) AVG should be installed in. Check the ***Additional installed languages*** item and then select the desired languages from the respective menu.

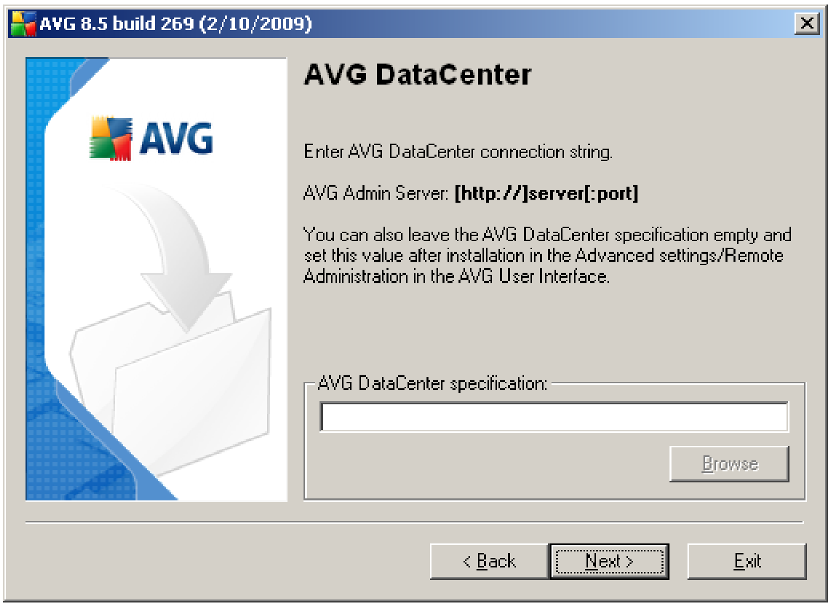
- ***Anti-Spam Server (for e-mail server)*** - select if you wish to install Anti-Spam protection for your e-mail server.

- ***Email Scanner (for e-mail server)*** - select if you wish to install anti-virus/anti-malware protection for your e-mail server.

Continue by pressing the ***Next*** button.

3.8. Custom Installation - DataCenter

If you selected the ***Remote Control Communication Library*** module during module selection, then in this screen you can define the connection string for connecting to your AVG DataCenter.



AVG 8.5 build 269 (2/10/2009)

AVG DataCenter

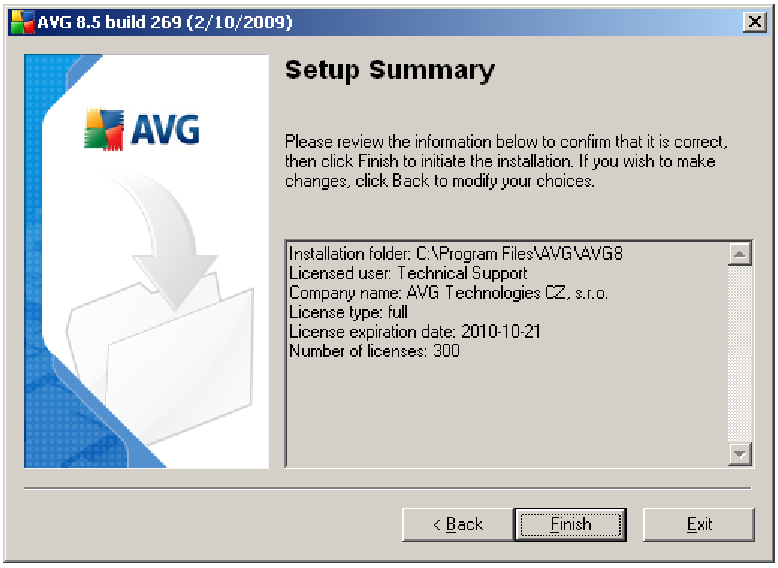
Enter AVG DataCenter connection string.

AVG Admin Server: **[http://]server[:port]**

You can also leave the AVG DataCenter specification empty and set this value after installation in the Advanced settings/Remote Administration in the AVG User Interface.

AVG DataCenter specification:

3.9. Setup Summary



Setup Summary

Please review the information below to confirm that it is correct, then click Finish to initiate the installation. If you wish to make changes, click Back to modify your choices.

Installation folder: C:\Program Files\AVG\AVG8
Licensed user: Technical Support
Company name: AVG Technologies CZ, s.r.o.
License type: full
License expiration date: 2010-10-21
Number of licenses: 300

The ***Setup Summary*** dialog provides an overview of all parameters of the installation process. Please make sure all the information is correct. If so, press the ***Finish*** button to continue. Otherwise, you can use the ***Back*** button to return to the respective dialog and correct the information.

3.10.Installing

The ***Installing*** dialog shows the progress of the installation process, and does not require any intervention. Please wait until the installation is complete, then you will be redirected to the ***Installation Complete*** dialog.

3.11.Installation Complete

The ***Installation Complete*** dialog is the last step of the AVG installation process. AVG is now installed on your computer and fully functional. The program is running in the background in fully automatic mode.

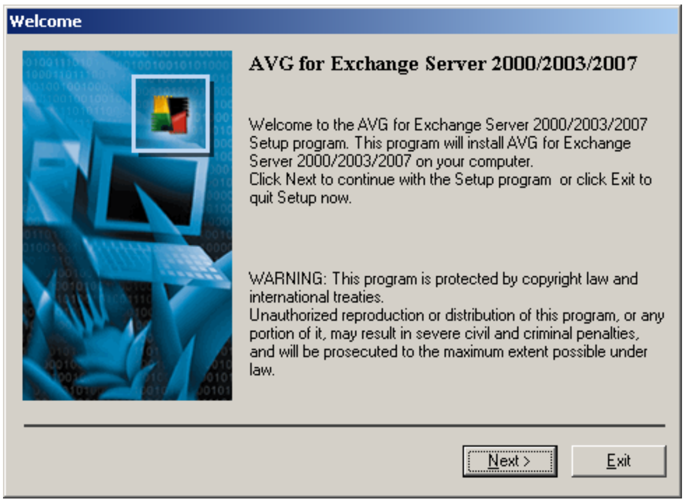
Depending on the e-mail server installed, you will experience other installation dialogs (see below).

4. AVG E-mail Servers Installation Options

Once you successfully complete installation of AVG, the installation of individual e-mail servers will begin.

Note: *The anti-virus protection mechanism for Kerio MailServer is integrated directly in the Kerio application. More information to be found in the [AVG for Kerio MailServer]() chapter.*

4.1. Installation Launch



Welcome

AVG for Exchange Server 2000/2003/2007

Welcome to the AVG for Exchange Server 2000/2003/2007 Setup program. This program will install AVG for Exchange Server 2000/2003/2007 on your computer.
Click Next to continue with the Setup program or click Exit to quit Setup now.

WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

The installation process starts with the ***Welcome*** window. Click on the ***Next*** button to continue to the next dialog.

4.2. License Agreement

This dialog provides the full wording of the AVG license agreement. Please read it carefully and confirm that you have read, understood and accept the agreement by pressing the ***Yes*** button. If you do not agree with the license agreement press the ***No*** button, and the installation process will be terminated immediately.

4.3. Location

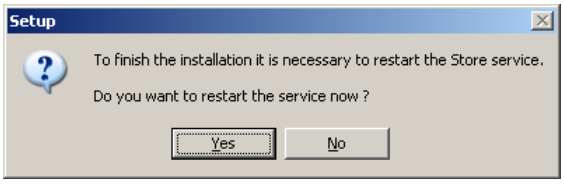
In the next window you will be prompted to select the target installation folder. Press the Browse button to select other location than the default one. If you do not have an actual reason to change the default settings, it is recommended to keep the preset location. Click on the ***Next*** button to continue.

4.4. Start Copying Files

Setup prompts you to trigger copying of the installation files before the installation will be completed. Accept it by clicking on the ***Next*** button.

4.5. Restarting the Store Service

During the installation process, or after closing the setup dialog, you will be prompted to restart the Exchange Server Store service:



Setup

To finish the installation it is necessary to restart the Store service.

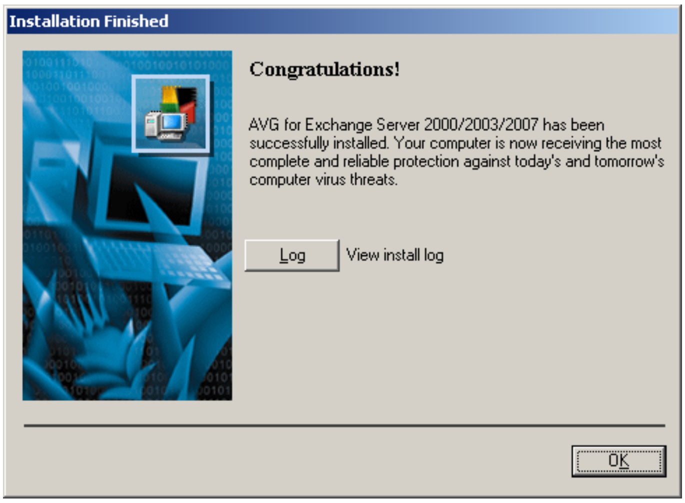
Do you want to restart the service now ?

Press the ***Yes*** button to restart the Store service with all **AVG for MS Exchange** components included.

Note: *Restarting the service will make your server unreachable for some time! You should warn your users before restarting the service because all users online will be automatically disconnected during the restart.*

4.6. Installation Finished

Once the installation wizard has copied all necessary files to your hard drive, the installation will be completed.



Installation Finished

Congratulations!

AVG for Exchange Server 2000/2003/2007 has been successfully installed. Your computer is now receiving the most complete and reliable protection against today's and tomorrow's computer virus threats.

You can view the installation log file by pressing the ***Log*** button.

You can also view the setup log later as the setup.log file in your system temporary folder.

Press the ***OK*** button in the ***Installation Finished*** window to close the setup dialog.

After the installation, AVG Basic Configuration Wizard will be launched automatically and in a few steps will lead you through the **AVG 8.5 Email Server Edition** elementary configuration. Despite the fact the AVG configuration is accessible any time during AVG run, we deeply recommend to use this option and set up the basic configuration with the wizard's help.

To individually setup protection for your e-mail server, follow the appropriate chapter:

- ***AVG for MS Exchange Server 2007***
- ***AVG for MS Exchange Server 2000/2003***
- ***AVG for Kerio MailServer***

5. AVG For MS Exchange Server 2007

5.1. Configuration

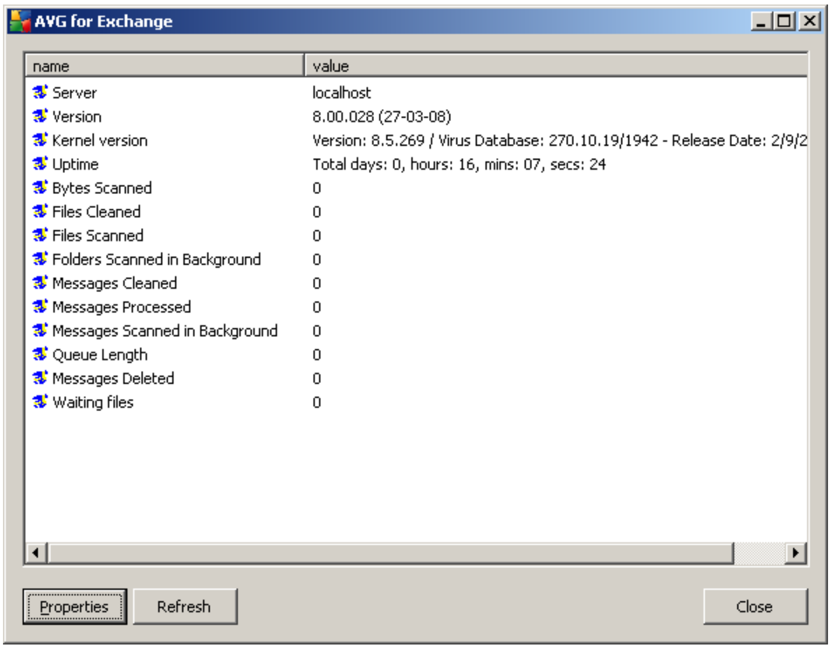
When the Exchange 2007 Server Store service is restarted after AVG for MS Exchange 2007 Server has been installed, no further actions are needed to be taken to launch it.

5.1.1. Status

To view the status or configuration of **AVG**, you need to launch the AVG for Exchange administration application first. It is located under the installation directory, by default:

C:\AVG4ES2K

Navigate to this directory and launch ***avg4es2kadm.exe***. A new window will open with information window showing various data to be overviewed.



name	value
Server	localhost
Version	8.00.028 (27-03-08)
Kernel version	Version: 8.5.269 / Virus Database: 270.10.19/1942 - Release Date: 2/9/2
Uptime	Total days: 0, hours: 16, mins: 07, secs: 24
Bytes Scanned	0
Files Cleaned	0
Files Scanned	0
Folders Scanned in Background	0
Messages Cleaned	0
Messages Processed	0
Messages Scanned in Background	0
Queue Length	0
Messages Deleted	0
Waiting files	0

The information displayed in the window include server name, application version, database version, kernel version, and the total time of program run since the last restart. Also, items informing about anti-virus performance are displayed here *(performance monitor counters)*.

AVG for MS Exchange 2007 Server scans all messages in the databases of private and public folders. If a virus is found, AVG for MS Exchange 2007 Server writes a message into the AVG log file and also into the Event Log.

5.1.2. VSAPI 2.0

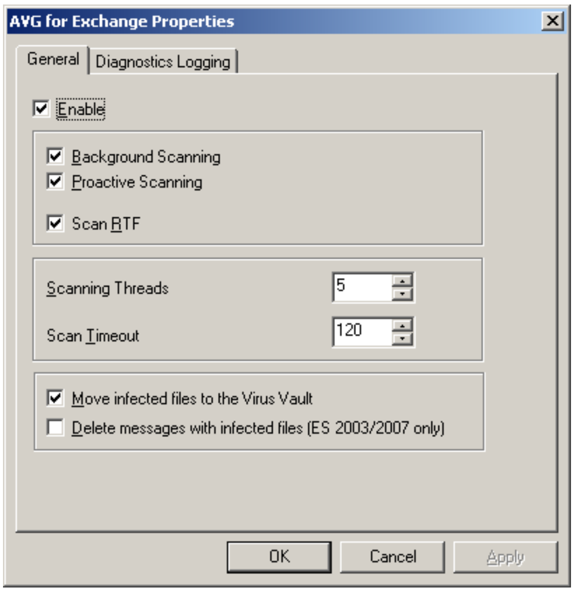
Virus Scanning **API 2.5** *(VSAPI 2.5 as provided in MS Exchange 2003 Server)* allows deletion of infected messages. This feature can be set up in the ***Properties*** dialog (see below).

5.1.3. General Properties

The AVG for Exchange 2007 Server configuration window can be opened by clicking the ***Properties*** button.

The ***AVG for Exchange Properties*** configuration window consists of two tabs. You can change the e-mail virus scanning settings and the logging behavior here.

General Tab



AVG for Exchange Properties

General | Diagnostics Logging

☑ Enable

☑ Background Scanning
☑ Proactive Scanning

☑ Scan RTF

Scanning Threads: 5

Scan Timeout: 120

☑ Move infected files to the Virus Vault
☐ Delete messages with infected files (ES 2003/2007 only)

On the ***General*** tab you will find several preset options related to the AVG for MS Exchange 2007 Server e-mail virus scanning performance:

- ***Enable*** – you can enable or disable mail scanning here.
- ***Background Scanning*** – you can enable or disable the background scanning process here. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging Databases. Whenever an item that has not been scanned before is encountered in the users' mailbox folders, it is submitted to AVG for Exchange 2007 Server to be scanned. Scanning and searching for the not examined objects runs in parallel.

  A specific low priority thread is used for each database, which guarantees other tasks (e.g. e-mail messages storage in the Microsoft Exchange database) are always carried out preferentially.

- ***Proactive Scanning*** – you can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. The proactive scanning lies in dynamical priority management of items in scanning queue. The lower priority items are not being scanned unless all the higher priority ones (most frequently supplied on demand in the queue) have been scanned. However, the priority of an item rises if a client tries to use it, so the precedence of the item changes according to users' activity.
- ***Scan RTF*** – you can specify here, whether the RTF file type should be scanned or not.
- ***Scanning Threads*** – the scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. You can change the threads count here. The default number of threads is computed as 2 times the 'number_of_processors' + 1.
- ***Scan Timeout*** field – the maximum continuous interval (in seconds) for one thread to access the message that is being scanned.
- ***Move infected files to the Virus Vault*** – if checked on, every infected e-mail message file will be moved into AVG **Virus Vault** quarantine environment.
- ***Delete messages with infected files (ES 2003/2007 only)*** – after checking this item on, a message where a virus is detected will be deleted. When this item is checked off, the infected e-mail is delivered to recipient, but infected attachment is replaced with a text file containing information on the virus detected. This option is available only in VSAPI 2.5 in Exchange 2007 Server.

Generally, all the features on this tab are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI 2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

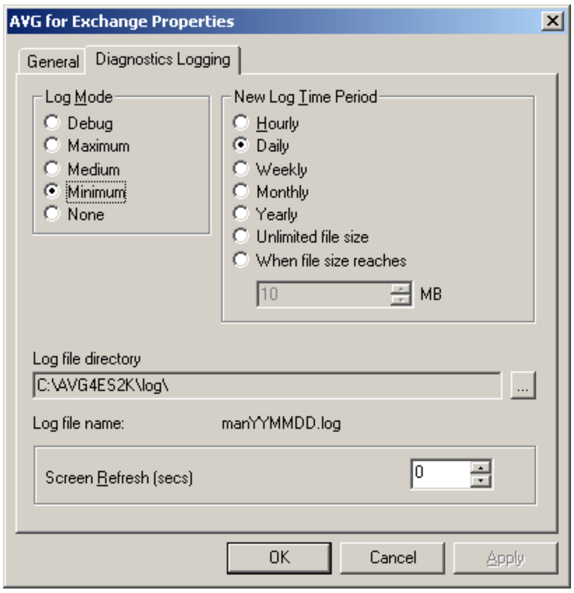
- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP for general info on the VSAPI 2.0 in Exchange 2000 Server Service Pack 1

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - for information on Exchange and antivirus software interaction

- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 for information on additional VSAPI 2.5 features in Exchange 2003 Server application.

Note: *The scanning behavior is controlled from the AVG Application. From the application's main menu select Tools/Advanced Settings. (See the E-mail Scanner chapter).*

5.1.4. Diagnostics Logging



AVG for Exchange Properties

General | Diagnostics Logging

Log Mode
○ Debug
○ Maximum
○ Medium
● Minimum
○ None

New Log Time Period
○ Hourly
● Daily
○ Weekly
○ Monthly
○ Yearly
○ Unlimited file size
○ When file size reaches
10 MB

Log file directory
C:\AVG4ES2K\log\

Log file name: manYYMMDD.log

Screen Refresh (secs) 0

On this tab you can define the virus scanning logging frequency and general behavior here. Several fields are preset on the Diagnostics Logging tab:

- ***Log Mode*** – you can adjust the amount of information to be logged here.

- ***New Log Time Period*** – you can define the period of new log file creation, and possibly the log file size here.

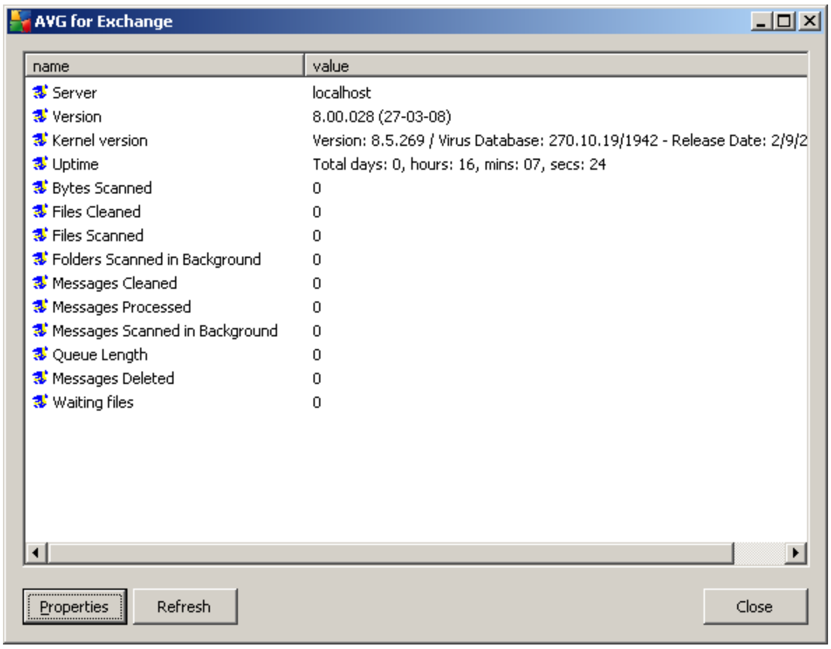
- ***Log file directory*** – you can change the default log file location here.

- ***Log file name*** – you can see the default log filename here.

- ***Screen Refresh (secs)*** – you can specify how often the online monitoring screen (shown on the AVG for Exchange Server information window) should be refreshed.

5.2. Server Monitoring

5.2.1. Online Monitoring



name	value
Server	localhost
Version	8.00.028 (27-03-08)
Kernel version	Version: 8.5.269 / Virus Database: 270.10.19/1942 - Release Date: 2/9/2
Uptime	Total days: 0, hours: 16, mins: 07, secs: 24
Bytes Scanned	0
Files Cleaned	0
Files Scanned	0
Folders Scanned in Background	0
Messages Cleaned	0
Messages Processed	0
Messages Scanned in Background	0
Queue Length	0
Messages Deleted	0
Waiting files	0

In the AVG for Exchange Server information window (*Refer to the Configuration/Status section to see how to get there.*), there are several fields displayed:

The first four items provide general information on the server and AVG for Exchange 2007 Server status:

- ***Server*** – server name

- ***Version*** – version of AVG for Exchange 2007 Server

- ***Kernel version*** – version of the Anti-Virus kernel, and its internal virus database

- ***Uptime*** – total time since the last Exchange server restart

The other items represent particular VSAPI 2.0/2.5 performance monitor counters related to virus scanning of Exchange 2007 Server. Counters are described as follows:

- ***Bytes Scanned*** – total number of bytes in all files processed by the virus scanner
- ***Files Cleaned*** – total number of separate files cleaned by the virus scanner
- ***Files scanned*** – total number of files scanned by the virus scanner
- ***Folders Scanned in Background*** – total number of folders processed by background scanning
- ***Messages Cleaned*** – total number of top-level messages cleaned by the virus scanner
- ***Messages Processed*** – cumulative value of the total number of top-level messages processed by the virus scanner
- ***Messages Scanned in Background*** – total number of messages processed by background scanning
- ***Queue Length*** – current number of outstanding requests that are queued for virus scanning
- ***Messages Deleted*** – total number of suspect messages deleted by virus scanner (available only in VSAPI 2.5)
- ***Waiting Files*** – count of files waiting to be scanned

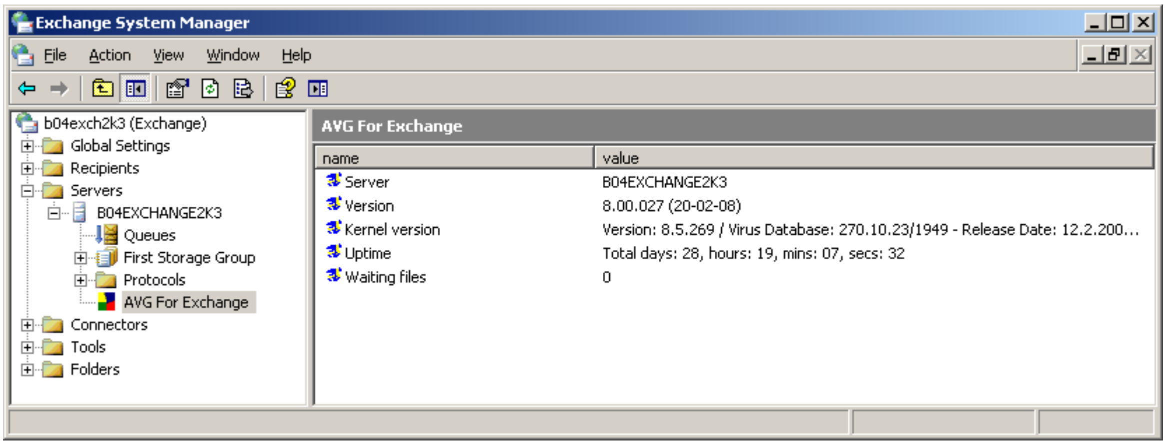
6. AVG For MS Exchange Server 2000/2003

6.1. Configuration

When the Exchange 2000/2003 Server Store service is restarted after **AVG for MS Exchange 2000/2003 Server** has been installed, no further actions are needed to be taken to launch it.

6.1.1. Status

To view the status of **AVG**, launch the MS Exchange System Manager application. In the Servers branch of the control tree *(on the left side of the main window)* select the particular server. There is the AVG for Exchange branch in the server's sub-tree. Selecting this branch will open the information window showing various data to be overviewed.



AVG For Exchange

name	value
Server	B04EXCHANGE2K3
Version	8.00.027 (20-02-08)
Kernel version	Version: 8.5.269 / Virus Database: 270.10.23/1949 - Release Date: 12.2.200...
Uptime	Total days: 28, hours: 19, mins: 07, secs: 32
Waiting files	0

The information displayed in the window include server name, application version, database version, kernel version, and the total time of program run since the last restart. Also, items informing about anti-virus performance are displayed here *(performance monitor counters)*.

AVG for MS Exchange 2000/2003 Server scans all messages in the databases of private and public folders. If a virus is found, AVG for MS Exchange 2000/2003 Server writes a message into the AVG log file and also into the Event Log.

6.1.2. VSAPI 2.0

Virus Scanning **API 2.0** (VSAPI 2.0 as provided in MS Exchange 2000 Server) does not allow the deletion of infected e-mail files. Since the virus infected e-mail message attachment cannot be deleted, its filename is changed: AVG for Exchange 2000/2003 Server appends the .virusinfo.txt extension to the original filename. The file content is overwritten with a message about the known virus. If a virus is found directly in the message, the whole body of the message is overwritten with a note saying a virus was found inside this message.

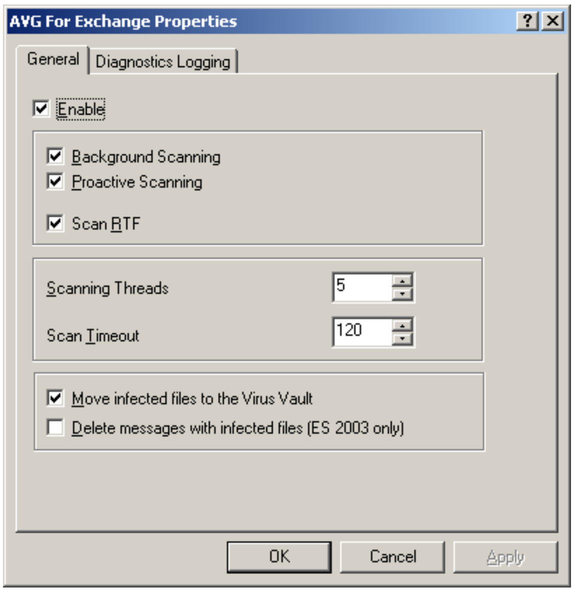
Virus Scanning **API 2.5** *(VSAPI 2.5 as provided in MS Exchange 2003 Server)* also allows deletion of infected messages. This feature can be set up in AVG for MS Exchange 2000/2003 Server configuration dialog.

6.1.3. General Properties

The AVG for Exchange 2000/2003 Server configuration window can be opened by right clicking on the ***AVG for Exchange*** branch, and selecting the ***Properties*** item. Alternatively, you can open the window using the ***Action*** button from the upper menu.

The ***AVG for Exchange Properties*** configuration window consists of two tabs. You can change the e-mail virus scanning settings and the logging behavior here.

General Tab



☑ Enable

☑ Background Scanning
☑ Proactive Scanning
☑ Scan RTF

Scanning Threads 5

Scan Timeout 120

☑ Move infected files to the Virus Vault
☐ Delete messages with infected files (ES 2003 only)

On the ***General*** tab you will find several preset options related to the AVG for MS Exchange 2000/2003 Server e-mail virus scanning performance:

- ***Enable*** – you can enable or disable mail scanning here.
- ***Background Scanning*** – you can enable or disable the background scanning process here. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging Databases. Whenever an item that has not been scanned before is encountered in the users' mailbox folders, it is submitted to AVG for Exchange 2000/2003 Server to be scanned. Scanning and searching for the not examined objects runs in parallel.

  A specific low priority thread is used for each database, which guarantees other tasks (e.g. e-mail messages storage in the Microsoft Exchange database) are always carried out preferentially.

- ***Proactive Scanning*** – you can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. The proactive scanning lies in dynamical priority management of items in scanning queue. The lower priority items are not being scanned unless all the higher priority ones (most frequently supplied on demand in the queue) have been scanned. However, the priority of an item rises if a client tries to use it, so the precedence of the item changes according to users' activity.
- ***Scan RTF*** – you can specify here, whether the RTF file type should be scanned or not.
- ***Scanning Threads*** – the scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. You can change the threads count here. The default number of threads is computed as 2 times the 'number_of_processors' + 1.
- ***Scan Timeout*** field – the maximum continuous interval (in seconds) for one thread to access the message that is being scanned.
- ***Move infected files to the Virus Vault*** – if checked on, every infected e-mail message file will be moved into **AVG Virus Vault** quarantine environment.
- ***Delete messages with infected files (ES 2003 only)*** – after checking this item on, a message where a virus is detected will be deleted. When this item is checked off, the infected e-mail is delivered to recipient, but infected attachment is replaced with a text file containing information on the virus detected. This option is available only in VSAPI 2.5 in Exchange 2003 Server.

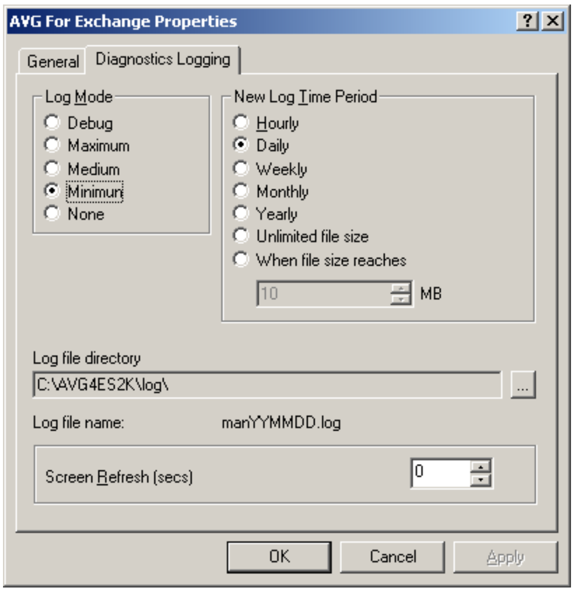
Generally, all the features on this tab are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI

2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP for general info on the VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - for information on Exchange and antivirus software interaction
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 for information on additional VSAPI 2.5 features in Exchange 2003 Server application.

Note: *The scanning behavior is controlled from the AVG E-Mail Server Application. From the application's main menu select Tools/Advanced Settings. (See the E-mail Scanner chapter).*

6.1.4. Diagnostics Logging


AVG For Exchange Properties

General | Diagnostics Logging

Log Mode
○ Debug
○ Maximum
○ Medium
● Minimum
○ None

New Log Time Period
○ Hourly
● Daily
○ Weekly
○ Monthly
○ Yearly
○ Unlimited file size
○ When file size reaches
10 MB

Log file directory: C:\AVG4ES2K\log\

Log file name: manYYMMDD.log

Screen Refresh (secs): 0

On this tab you can define the virus scanning logging frequency and general behavior here. Several fields are preset on the Diagnostics Logging tab:

- ***Log Mode*** – you can adjust the amount of information to be logged here.
- ***New Log Time Period*** – you can define the period of new log file creation, and possibly the log file size here.

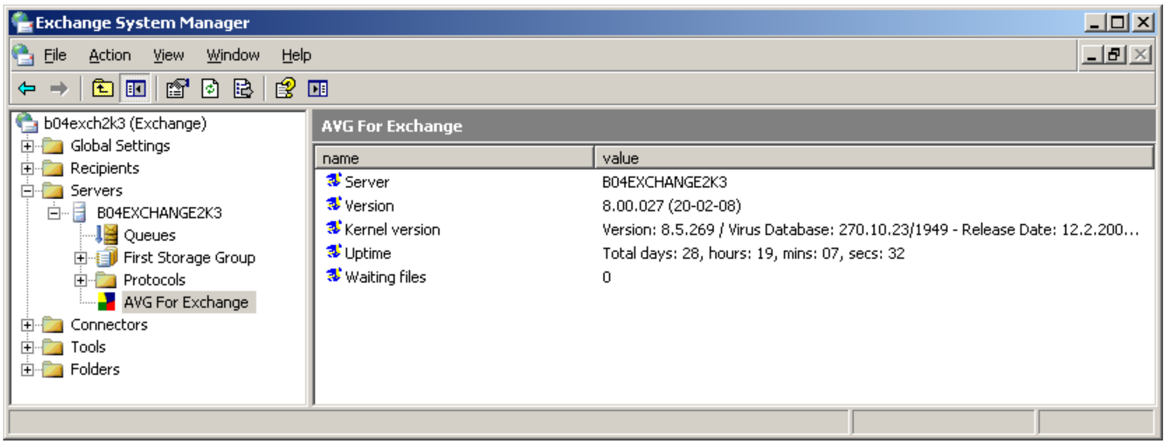
- ***Log file directory*** – you can change the default log file location here.

- ***Log file name*** – you can see the default log filename here.

- ***Screen Refresh (secs)*** – you can specify how often the online monitoring screen (shown on the AVG for Exchange 2000/2003 Server information window) should be refreshed.

6.2. Server Monitoring

6.2.1. Online Monitoring



AVG For Exchange

name	value
Server	B04EXCHANGE2K3
Version	8.00.027 (20-02-08)
Kernel version	Version: 8.5.269 / Virus Database: 270.10.23/1949 - Release Date: 12.2.200...
Uptime	Total days: 28, hours: 19, mins: 07, secs: 32
Waiting files	0

In the AVG for MS Exchange 2000/2003 Server information window (*Refer to the Configuration/Status section to see how to get there.*), there are several fields displayed:

The first four items provide general information on the server and AVG for Exchange 2000/2003 Server status:

- ***Server*** – server name

- ***Version*** – version of AVG for Exchange 2000/2003 Server

- ***Kernel version*** – version of the Anti-Virus kernel, and its internal virus database

- ***Uptime*** – total time since the last Exchange Server restart

- ***Waiting Files*** – count of files waiting to be scanned

The other items represent particular VSAPI 2.0/2.5 performance monitor counters related to virus scanning of Exchange 2000/2003 Server and may not be visible all the time. Counters are described as follows:

- ***Bytes Scanned*** – total number of bytes in all files processed by the virus scanner
- ***Files Cleaned*** – total number of separate files cleaned by the virus scanner
- ***Files Cleaned/sec*** – rate at which separate files are cleaned by the virus scanner
- ***Files Quarantined*** – total number of separate files moved to quarantine by the virus scanner
- ***Files Quarantined/sec*** – rate at which separate files are put into quarantine by the virus scanner
- ***Folders Scanned in Background*** – total number of folders processed by background scanning
- ***Messages Cleaned*** – total number of top-level messages cleaned by the virus scanner
- ***Messages Cleaned/sec*** – rate at which top-level messages are cleaned by the virus scanner
- ***Messages Quarantined*** – total number of top-level messages moved to quarantine by the virus scanner
- ***Messages Quarantined/sec*** – rate at which top-level messages are put into quarantine by the virus scanner
- ***Messages Processed*** – cumulative value of the total number of top-level messages processed by the virus scanner
- ***Messages Processed/sec*** – rate at which top-level messages are processed by the virus scanner
- ***Messages Scanned in Background*** – total number of messages processed by background scanning

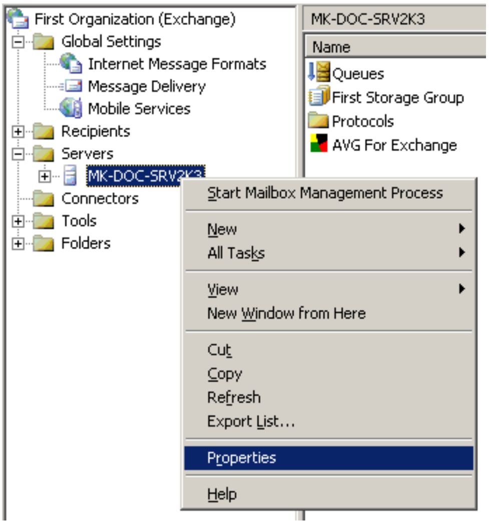
- ***Messages Deleted*** – total number of suspect messages deleted by virus scanner (available only in VSAPI 2.5)
- ***Messages Deleted/sec*** – rate at which suspect messages are deleted by virus scanner (available only in VSAPI 2.5)
- ***Queue Length*** – current number of outstanding requests that are queued for virus scanning

6.2.2. Event Log

Except for the online monitoring of AVG for MS Exchange 2000/2003 Server you can also setup the virus scanner related events logging within the **Event Log**. Available events cover many issues, such as program libraries loading notes, virus-found events, troubleshooting warnings, etc.

You can set up the logging level of Exchange VSAPI 2.0/2.5 in the Exchange System Manager's main window *(as shown in the Configuration/Diagnostics Logging section)*.

- Double-click the ***Servers*** branch in the control tree
- Select the particular server (see an example server name highlighted in the picture below)
- Right-click the server name, and select the ***Properties*** item from the context menu



- The ***Properties*** window appears.

- Switch to the ***Diagnostics Logging*** tab

- From the ***Services*** tree select the MSExchangeIS / System folder

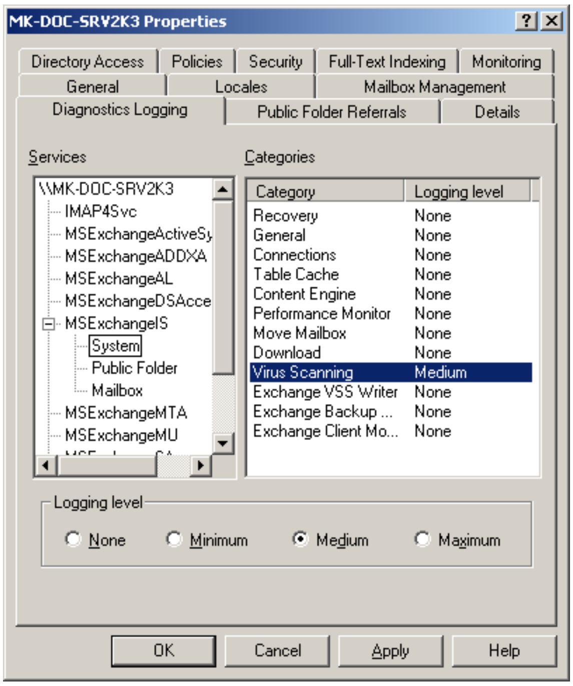
- From the opened ***Categories*** list select the ***Virus Scanning*** item, and choose the desired logging level for the operating system Event Log component. The following levels are offered:

    - ***None***

    - ***Minimum***

    - ***Medium***

    - ***Maximum***



MK-DOC-SRV2K3 Properties

Services

\\MK-DOC-SRV2K3
- IMAP4Svc
- MSExchangeActiveSy
- MSExchangeADDXA
- MSExchangeAL
- MSExchangeDSAcce
- MSExchangeIS
    - System
    - Public Folder
    - Mailbox
- MSExchangeMTA
- MSExchangeMU

Categories

Category	Logging level
Recovery	None
General	None
Connections	None
Table Cache	None
Content Engine	None
Performance Monitor	None
Move Mailbox	None
Download	None
Virus Scanning	Medium
Exchange VSS Writer	None
Exchange Backup ...	None
Exchange Client Mo...	None

Logging level

○ None ○ Minimum ● Medium ○ Maximum

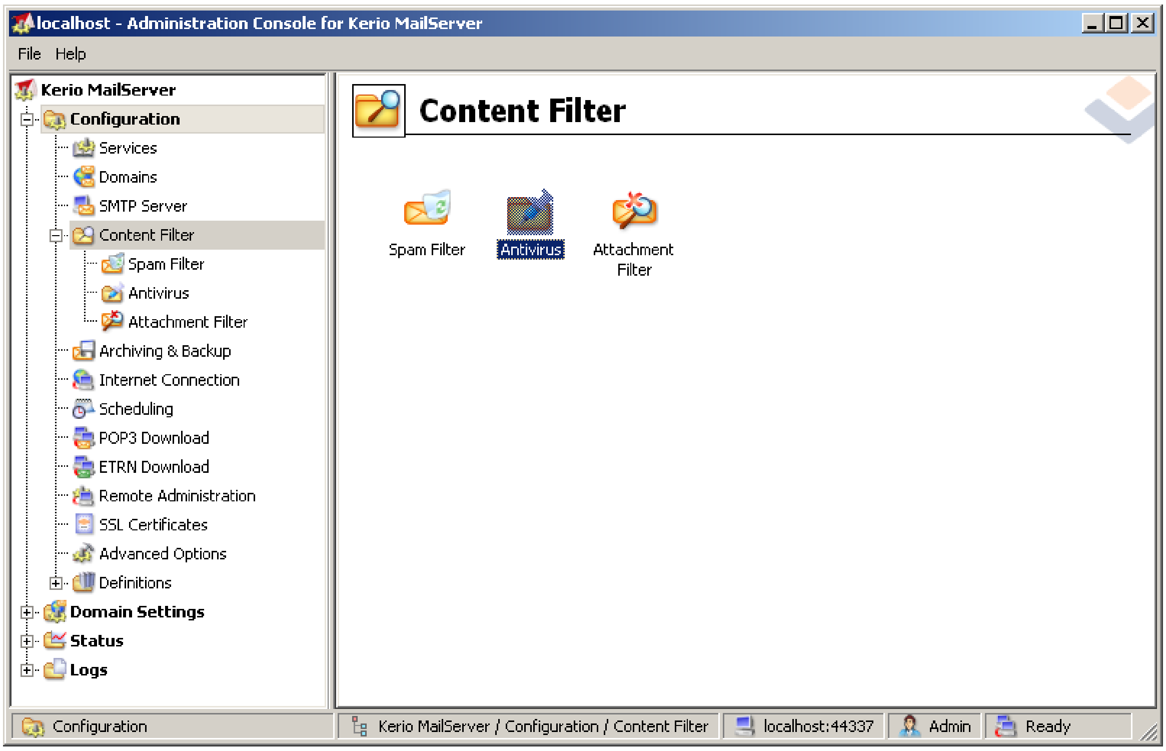
Note: *You will find the complete description of the VSAPI 2.0/2.5 events on this link:*

[*http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336*](http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336).

7. AVG for Kerio MailServer

7.1. Configuration

The anti-virus protection mechanism is integrated directly into the Kerio MailServer application. In order to activate e-mail protection of Kerio MailServer by the AVG scanning engine, launch the Kerio Administration Console application. In the control tree on the left side of the application window choose the Content Filter sub-branch in the Configuration branch:

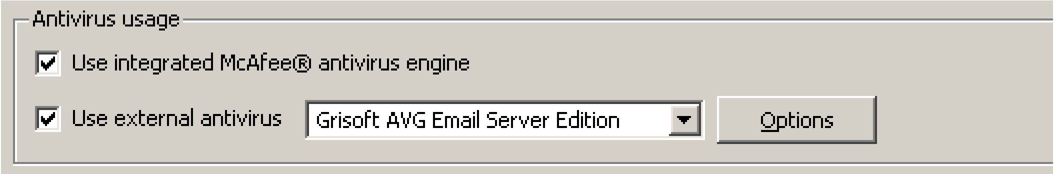


Clicking the Content Filter item will display a dialog with three items:

- ***Spam Filter***
- ***Antivirus*** (see section ***Antivirus***)
- ***Attachment Filter*** (see section ***Attachment Filter***)

7.1.1. Antivirus

To activate AVG for Kerio MailServer, select the Use external antivirus checkbox and choose the AVG Email Server Edition item from the external software menu in the Antivirus usage frame of the configuration window:



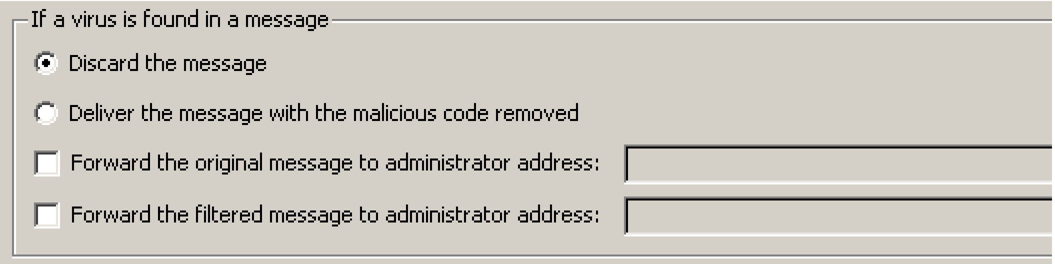
Antivirus usage

☑ Use integrated McAfee® antivirus engine

☑ Use external antivirus Grisoft AVG Email Server Edition

In the following section you can specify what to do with an infected or filtered message:

- ***If a virus is found in a message***



If a virus is found in a message

● Discard the message

○ Deliver the message with the malicious code removed

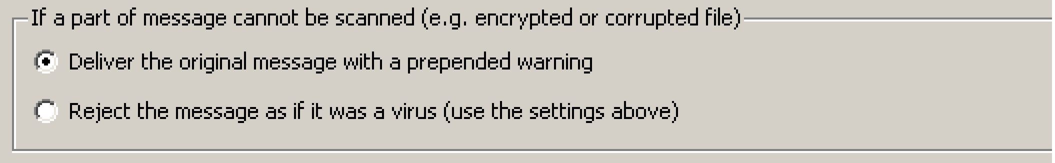
□ Forward the original message to administrator address:

□ Forward the filtered message to administrator address:

This frame specifies the action to be carried out when a virus is detected in a message, or when a message is filtered by an attachment filter:

- ***Discard the message*** – when selected, the infected or filtered message will be deleted.
- ***Deliver the message with the malicious code removed*** – when selected, the message will be delivered to the recipient, but without the possibly harmful attachment.
- ***Forward the original message to administrator address*** – when selected, the virus infected message is forwarded to the address specified in the address text field
- ***Forward the filtered message to administrator address*** - when selected, the filtered message is forwarded to the address specified in the address text field

- ***If a part of message cannot be scanned (e.g. encrypted or corrupted file)***



If a part of message cannot be scanned (e.g. encrypted or corrupted file)

● Deliver the original message with a prepended warning

○ Reject the message as if it was a virus (use the settings above)

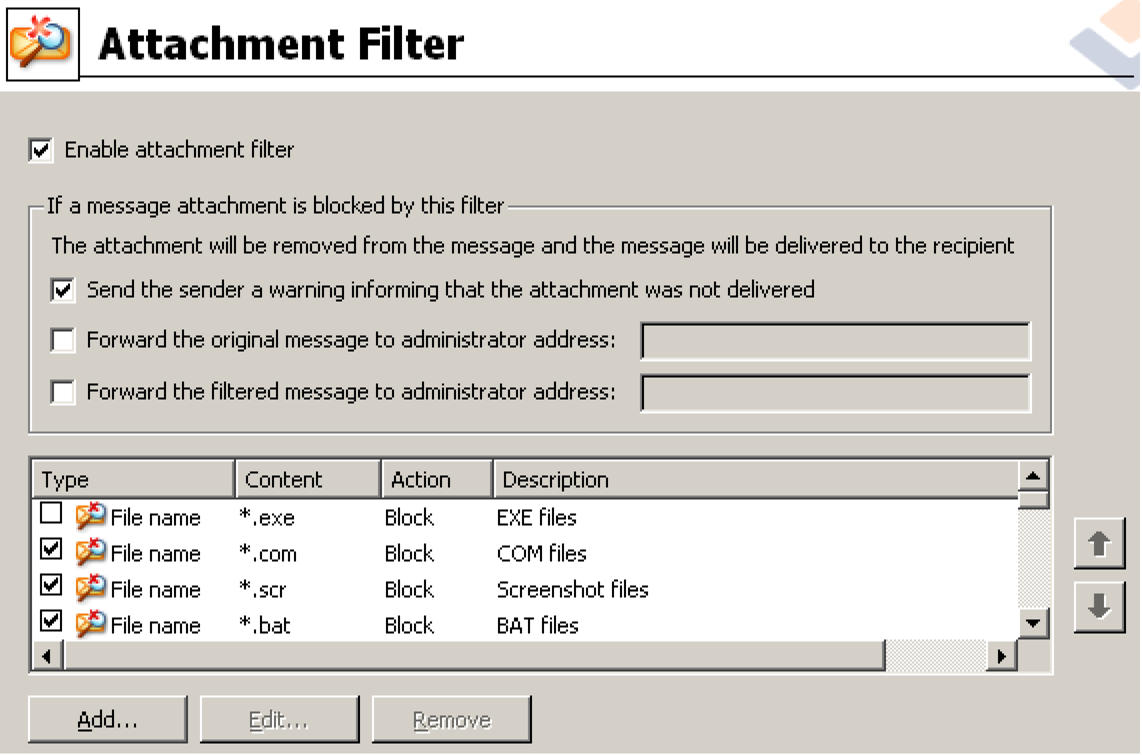
This frame specifies the action to be taken when part of the message or attachment cannot be scanned:

- ***Deliver the original message with a prepared warning*** – the message (or attachment) will be delivered unchecked. The user will be warned that the message may still contain viruses.
- ***Reject the message as if it was virus*** – the system will react the same way as when a virus was detected (i.e. the message will be delivered without any attachment or rejected). This option is safe, but sending password protected archives will be virtually impossible.

Note: *The scanning behavior is controlled from the AVG E-mail Server Application. From the application's main menu select Tools/Advanced Settings. (See the E-mail Scanner chapter).*

7.1.2. Attachment Filter

In the Attachment Filter menu there is a list of various attachment definitions:



Attachment Filter

☑ Enable attachment filter

If a message attachment is blocked by this filter

The attachment will be removed from the message and the message will be delivered to the recipient

☑ Send the sender a warning informing that the attachment was not delivered

□ Forward the original message to administrator address:

□ Forward the filtered message to administrator address:

	Type	Content	Action	Description
□	File name	*.exe	Block	EXE files
☑	File name	*.com	Block	COM files
☑	File name	*.scr	Block	Screenshot files
☑	File name	*.bat	Block	BAT files

You can enable/disable filtering of mail attachments by selecting the Enable attachment filter checkbox. Optionally you can change the following settings:

- ***Send a warning to sender that the attachment was not delivered***

  The sender will receive a warning from Kerio MailServer, that he/she has sent a message with a virus or blocked attachment.

- ***Forward the original message to administrator address***

  The message will be forwarded (as it is — with the infected or forbidden attachment) to a defined email address, regardless of whether it is a local or an external address.

- ***Forward the filtered message to administrator address***

The message without its infected or prohibited attachment will be (apart from the actions selected below) forwarded to the specified e-mail address. This can be used to verify the correct functioning of the antivirus and/or attachment filter.

In the list of extensions, each item has four fields:

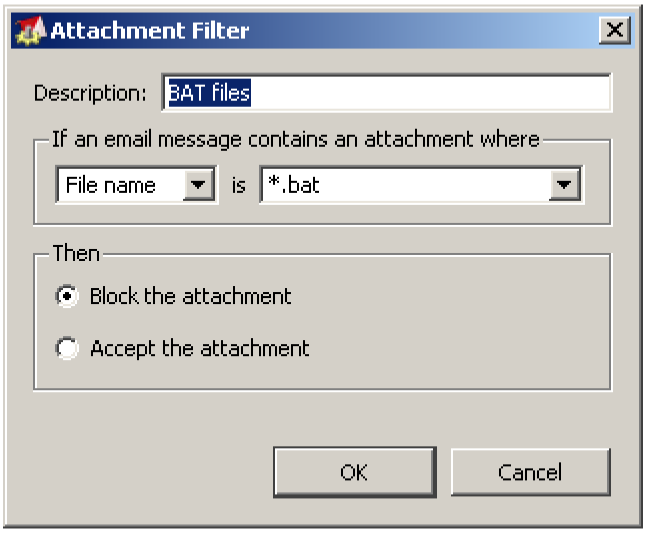
- ***Type*** – specification of the kind of attachment determined by the extension given in the Content field. Possible types are File name or MIME type. You can select the respective box in this field to include/exclude the item from attachment filtering.

- ***Content*** – an extension to be filtered can be specified here. You can use operation system wildcards here (for example the string '*.doc.*' stands for any file with the .doc extension, and any other extension following).

- ***Action*** – define action to be performed with the particular attachment. Possible actions are Accept (accept the attachment), and Block (block the attachment as defined in the Action tab dialog).

- ***Description*** – description of the attachment is defined in this field.

An item is removed from the list by pressing the Remove button. You can add another item to the list by pressing the ***Add...*** button. Or, you can edit an existing record by pressing the ***Edit...*** button. The following window then appears:



Description: BAT files

If an email message contains an attachment where

File name is *.bat

Then

● Block the attachment

○ Accept the attachment

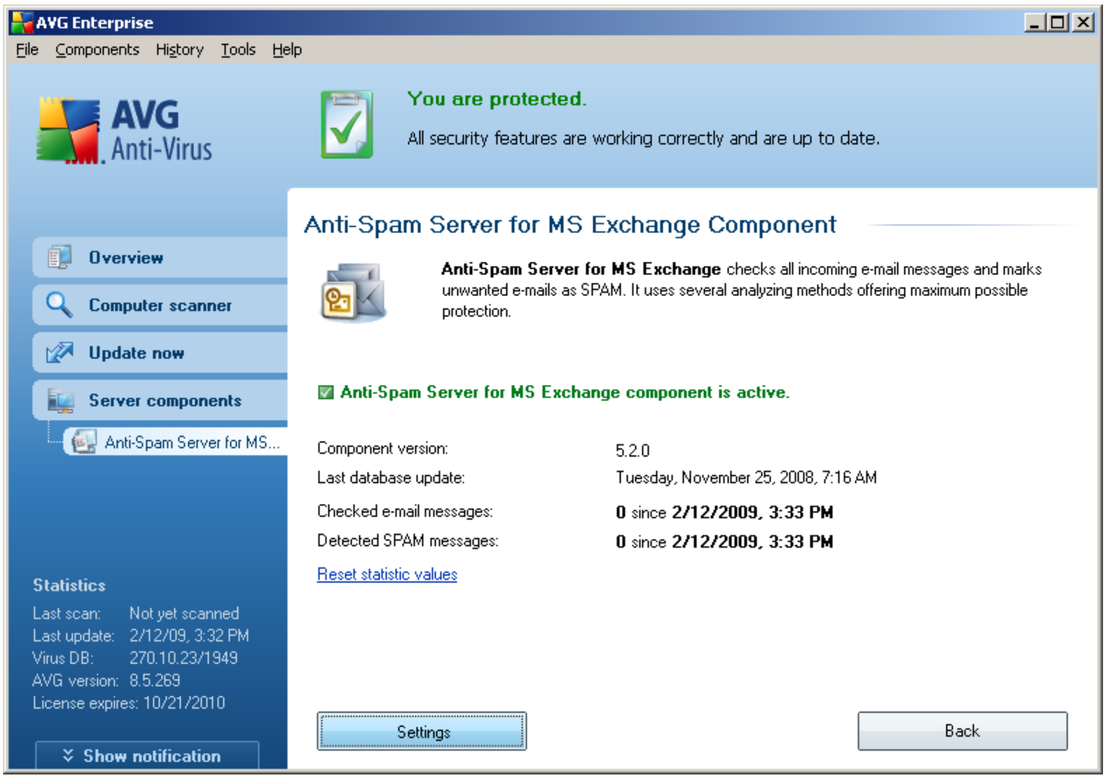
- In the Description field you can write a short description of the attachment to be filtered.

- In the If a mail message contains an attachment where field you can select the type of attachment (File name or MIME type). You can also choose a particular extension from the offered extensions list, or you can type the extension wildcard directly.

In the Then field you can decide whether to block the defined attachment or accept it.

8. Anti-Spam Configuration

8.1. Anti-Spam Interface



You are protected.

All security features are working correctly and are up to date.

Anti-Spam Server for MS Exchange Component

Anti-Spam Server for MS Exchange checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods offering maximum possible protection.

☑ Anti-Spam Server for MS Exchange component is active.

Component version:	5.2.0
Last database update:	Tuesday, November 25, 2008, 7:16 AM
Checked e-mail messages:	**0** since **2/12/2009, 3:33 PM**
Detected SPAM messages:	**0** since **2/12/2009, 3:33 PM**

Reset statistic values

Statistics

Last scan:	Not yet scanned
Last update:	2/12/09, 3:32 PM
Virus DB:	270.10.23/1949
AVG version:	8.5.269
License expires:	10/21/2010

You will find the ***Anti-Spam*** server component's dialog in the ***Server Components*** section (left menu). It contains a brief information about the functionality of the server component, information on its current status (*Anti-Spam Server for MS Exchange component is active.*), and some statistics.

You can reset the statistics by clicking on the ***Reset statistic values*** reference.

The working buttons are as follows:

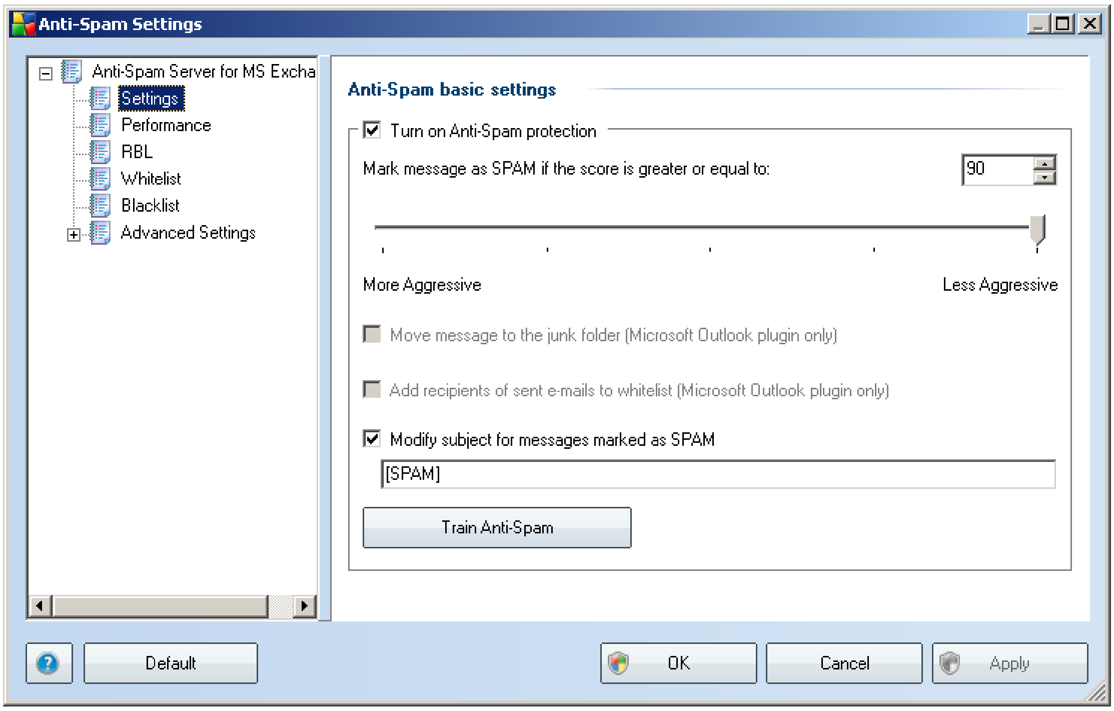
- ***Settings*** - use this button to open Anti-Spam settings.
- ***Back*** - press this button to return to the Server components overview.

8.2. Anti-Spam Principles

Spam refers to unsolicited e-mail, mostly advertising a product or service that is mass mailed to a huge number of e-mail addresses at a time, filling recipients' mail boxes. Spam does not refer to legitimate commercial e-mail for which consumers have given their consent. Spam is not only annoying, but also can often be a source of scams, viruses or offensive content.

Anti-Spam checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages.

8.3. Anti-Spam Settings



Anti-Spam Settings

- Anti-Spam Server for MS Excha
  - Settings
  - Performance
  - RBL
  - Whitelist
  - Blacklist
  - Advanced Settings

Anti-Spam basic settings

☑ Turn on Anti-Spam protection

Mark message as SPAM if the score is greater or equal to: 90

More Aggressive — Less Aggressive

□ Move message to the junk folder (Microsoft Outlook plugin only)

□ Add recipients of sent e-mails to whitelist (Microsoft Outlook plugin only)

☑ Modify subject for messages marked as SPAM

[SPAM]

In the ***Anti-Spam basic settings*** dialog you can check the ***Turn on Anti-Spam protection*** checkbox to allow/forbid the anti-spam scanning of e-mail communication.

In this dialog you can also select more or less aggressive scoring measures. The ***Anti-Spam*** filter assigns each message a score (*i.e. how similar the message content is to SPAM*) based on several dynamic scanning techniques. You can adjust the ***Mark message as spam if the score is greater or equal to*** setting by either typing the value (*0 to 100*) or by moving the slider left or right (*using the slider, the range of values is limited to 50-90*).

Generally we recommended setting the threshold between 50-90, or if you are really unsure, to 90. Here is a general review of the scoring threshold:

- ***Value 90-99*** - Most incoming e-mail messages will be delivered normally (without being marked as spam). The most easily identified spam will be filtered out, but a significant amount of spam may still be allowed through.
- ***Value 80-89*** - E-mail messages likely to be spam will be filtered out. Some non-spam messages may be incorrectly filtered as well.
- ***Value 60-79*** - Considered as a quite aggressive configuration. E-mail messages that are possibly spam will be filtered out. Non-spam messages are likely to be caught as well.
- ***Value 1-59*** - Very aggressive configuration. Non-spam e-mail messages are as likely to be caught as real spam messages. This threshold range is not recommended for normal use.
- ***Value 0*** - In this mode, you will only receive e-mail messages from senders in your ***Whitelist***. Any other e-mail messages will be considered as spam. ***This threshold range is not recommended for normal use.***

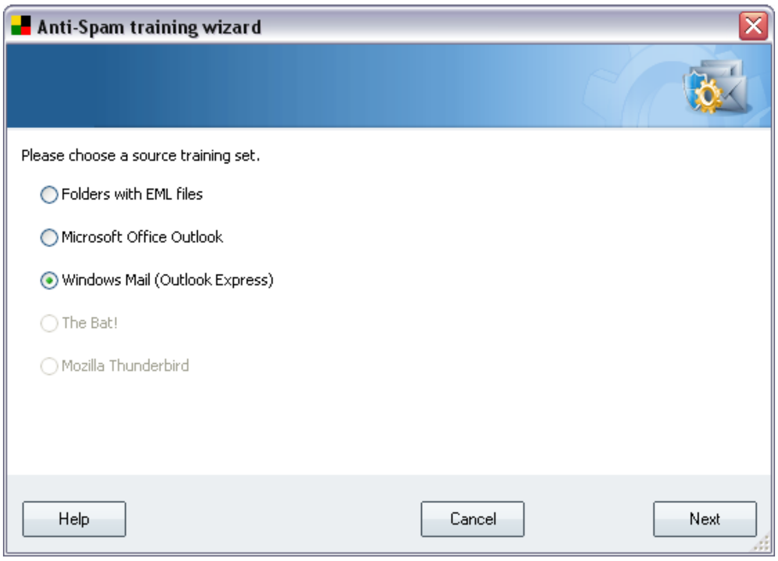
You can further define how the detected spam e-mail messages should be treated:

- ***Modify subject for messages marked as spam*** - tick this check box if you would like all messages detected as spam to be marked with a specific word or character in the e-mail subject field; the desired text can be typed in the activated text field.

Train Anti-Spam button opens the ***Anti-Spam training wizard*** described in details in the next chapter.

8.3.1. Anti-Spam Training Wizard

The first dialog of the ***Anti-Spam Training Wizard*** asks you to select the source of e-mail messages you want to use for training. Usually, you will want to use either e-mails that have been incorrectly marked as SPAM, or spam messages that have not been recognized.



Anti-Spam training wizard

Please choose a source training set.

○ Folders with EML files

○ Microsoft Office Outlook

● Windows Mail (Outlook Express)

○ The Bat!

○ Mozilla Thunderbird

There are the following options to choose from:

- ***A specific e-mail client*** - if you use one of the listed e-mail clients (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), simply select the respective option

- ***Folder with EML files*** - if you use any other e-mail program, you should first save the messages to a specific folder (in *.eml format*), or make sure that you know the location of your e-mail client message folders. Then select ***Folder with EML files***, which will enable you to locate the desired folder in the next step

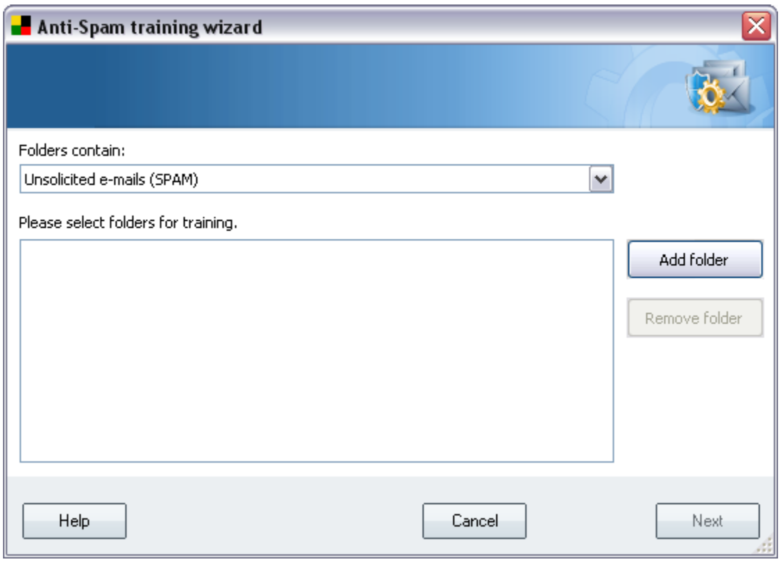
For faster and easier training process, it is a good idea to sort the e-mails in the folders beforehand, so that the folder you will use for training contains only the training messages (either wanted, or unwanted). However, it is not necessary, as you will be able to filter the e-mails later on.

Select the appropriate option and click ***Next*** to continue the wizard.

8.3.2. Select Folder with Messages

Dialog displayed in this step depends on your previous selection.

Folders with EML files



Anti-Spam training wizard
Folders contain:
Unsolicited e-mails (SPAM)
Please select folders for training.
Add folder
Remove folder
Help
Cancel
Next

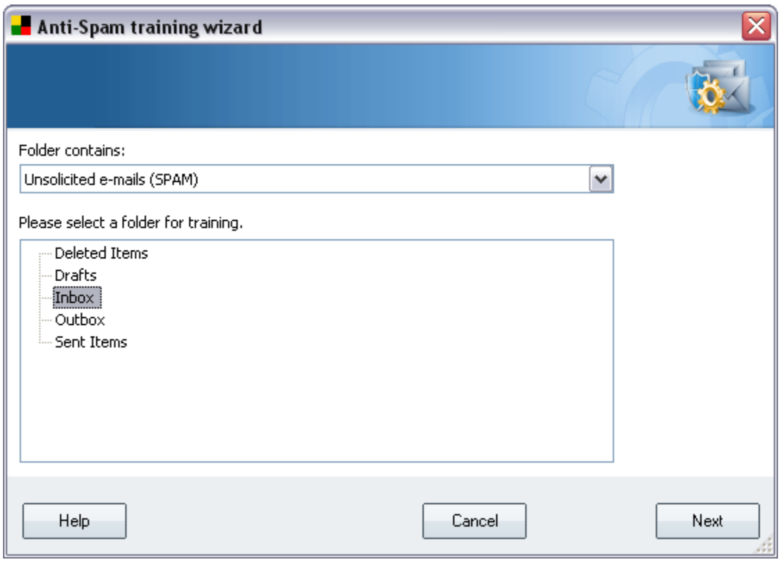
In this dialog, please select the folder with the messages you want to use for training. Press the ***Add folder*** button to locate the folder with the .eml files (*saved e-mail messages*). The selected folder will then be displayed in the dialog.

In the ***Folders contain*** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. You can also remove unwanted selected folders from the list by clicking the ***Remove folder*** button.

When done, click ***Next*** and proceed to ***Message filtering options***.

Specific e-mail client

Once you confirm one of the options, new dialog will appear.



Folder contains: Unsolicited e-mails (SPAM)

Please select a folder for training.

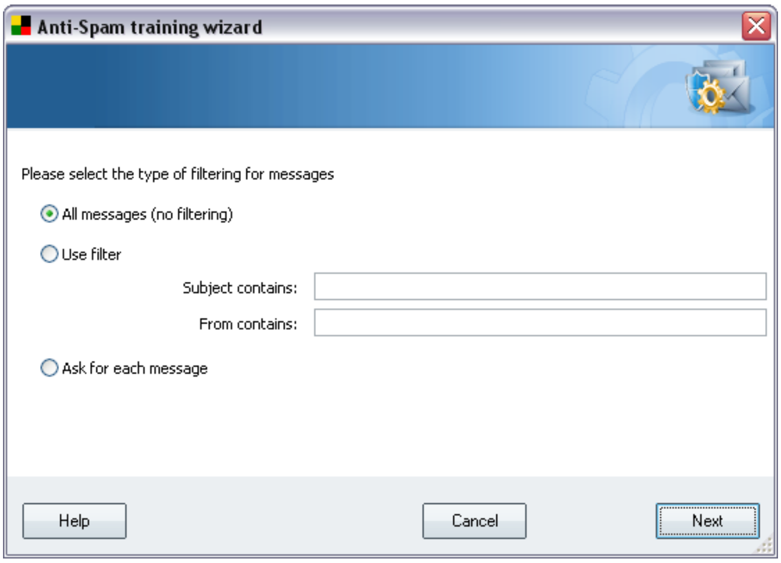
- Deleted Items
- Drafts
- Inbox
- Outbox
- Sent Items

***Note:** In case of Microsoft Office Outlook, you will be prompted to select the MS Office Outlook profile first.*

In the ***Folders contain*** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. A navigation tree of the selected e-mail client is already displayed in the main section of the dialog. Please locate the desired folder in the tree and highlight it with your mouse.

When done, click ***Next*** and proceed to ***Message filtering options***.

8.3.3. Message filtering options


Anti-Spam training wizard

Please select the type of filtering for messages

● All messages (no filtering)

○ Use filter

Subject contains:

From contains:

○ Ask for each message

In this dialog, you can set filtering of the e-mail messages.

If you are sure that the selected folder contains only messages you want to use for training, select the ***All messages (no filtering)*** option.

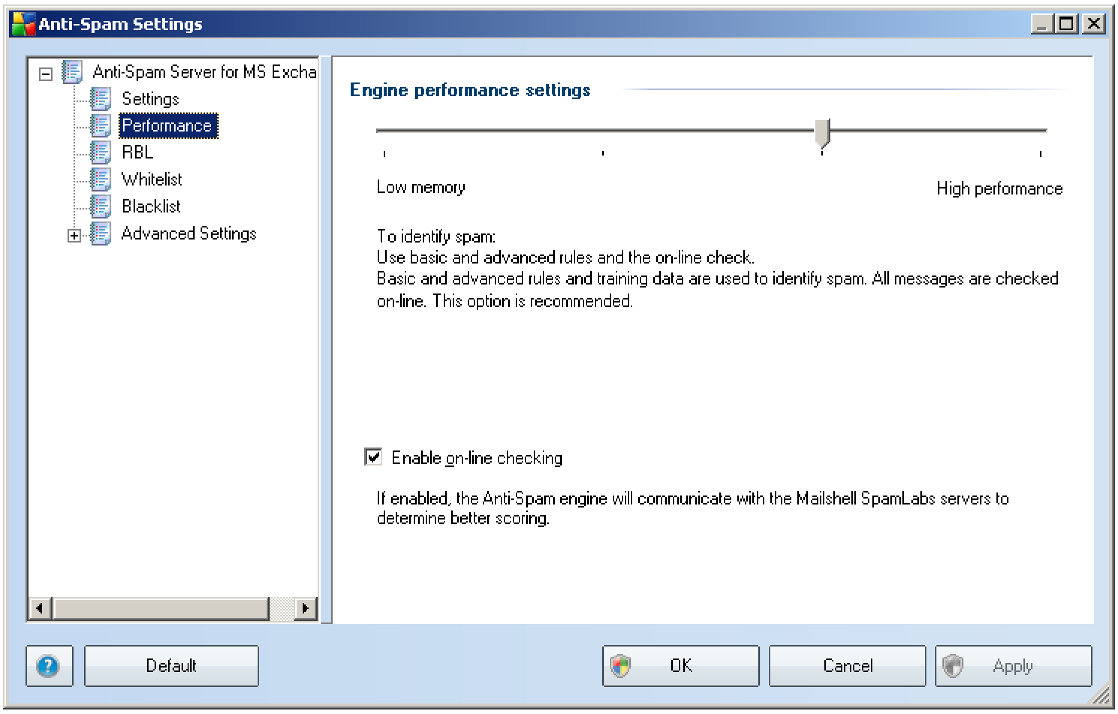
If you are unsure about the messages contained in the folder, and you want the wizard to ask you about every single message (so that you can determine whether to use it for training or not), select the ***Ask for each message*** option.

For more advanced filtering, select the ***Use filter*** option. You can fill in a word (*name*), part of a word, or phrase to be searched for in the e-mail subject and/or the sender's field. All messages matching exactly the entered criteria will be used for the training, without further prompting.

Attention!: *When you fill in both text fields, addresses that match just one of the two conditions will be used, too!*

When the appropriate option has been selected, click ***Next***. The following dialog will be informative only, telling you that the wizard is ready to process the messages. To start training, click the ***Next*** button again. Training will then start according to previously selected conditions.

8.4. Performance



Engine performance settings

Low memory

High performance

To identify spam:
Use basic and advanced rules and the on-line check.
Basic and advanced rules and training data are used to identify spam. All messages are checked on-line. This option is recommended.

☑ Enable on-line checking

If enabled, the Anti-Spam engine will communicate with the Mailshell SpamLabs servers to determine better scoring.

The ***Engine performance settings*** dialog (*linked to via the **Performance** item of the left navigation*) offers the ***Anti-Spam*** component performance settings. Move the slider left or right to change the level of scanning performance ranging between ***Low memory*** / ***High performance*** modes.

- ***Low memory*** - during the scanning process to identify spam, no rules will be used. Only training data will be used for identification. This mode is not recommended for common use, unless the computer hardware is really poor.

- ***High performance*** - this mode will consume large amount of memory. During the scanning process to identify spam, the following features will be used: rules and spam database cache, basic and advanced rules, spammer IP addresses and spammer databases.

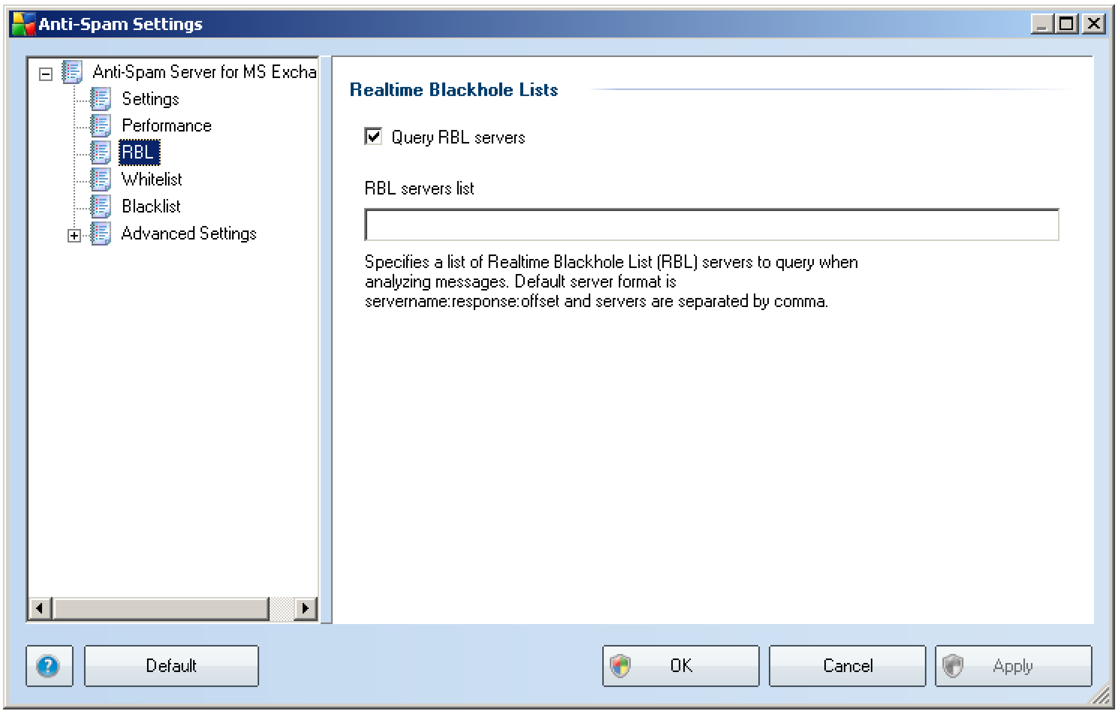
The ***Enable on-line checking*** item is on by default. It results in more precise spam detection via communication with the Mailshell servers, i.e. the scanned data will be compared with Mailshell databases online.

Generally it is recommended to keep the default settings and only change

them if you have a valid reason to do so. Any changes to this configuration should only be done by expert users!

8.5. RBL

The ***RBL*** item open an editing dialog called ***Realtime Blackhole Lists***:



☑ Query RBL servers

RBL servers list

Specifies a list of Realtime Blackhole List (RBL) servers to query when analyzing messages. Default server format is servername:response:offset and servers are separated by comma.

In this dialog you can switch on/off the ***Query RBL servers*** function.

The RBL (*Realtime Blackhole List*) server is a DNS server with an extensive database of known spam senders. When this feature is switched on, all e-mail messages will be verified against the RBL server database and marked as spam if identical to any of the database entries.

The RBL servers databases contain the latest up-to-the-minute spam fingerprints, to provide the very best and most accurate spam detection. This feature is especially useful for users who receive large amounts of spam that is not being normally detected by the Anti-Spam engine.

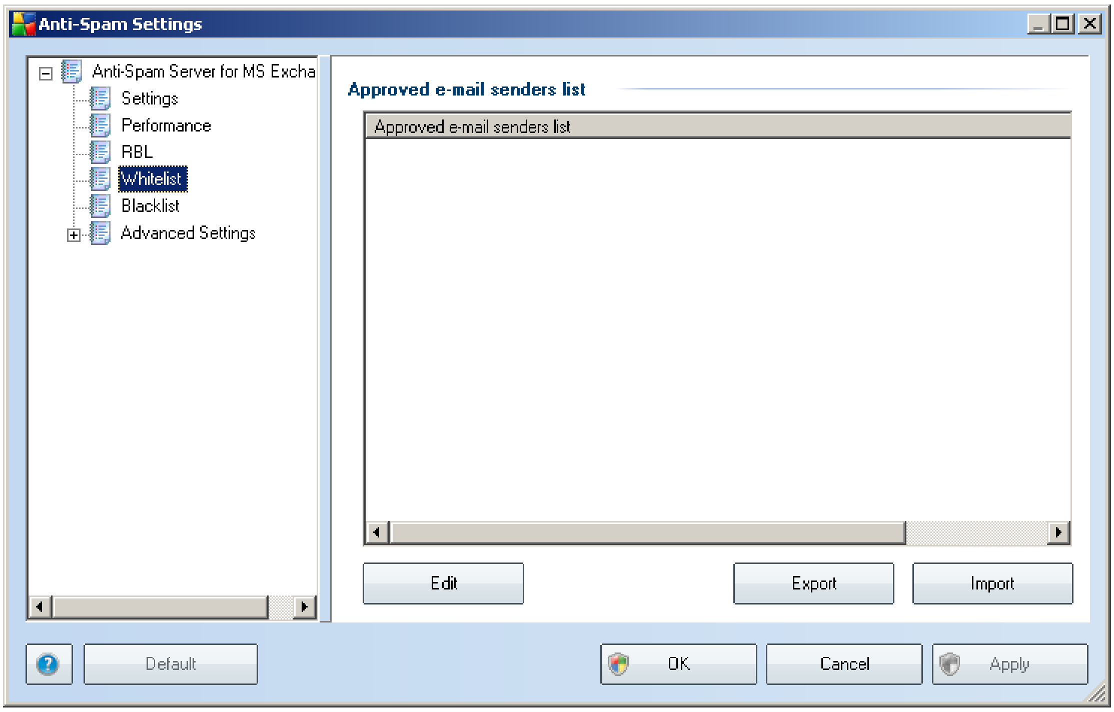
The ***RBL servers list*** allows you to define specific RBL server locations. By default, two RBL server addresses are specified. We recommend to keep the default settings unless you are an experienced user and really need to change these settings!

***Note:** Enabling this feature may, on some systems and configurations, slow down the e-mail receiving process, as every single message must be verified against the RBL server database.*

No personal data is sent to the server!

8.6. Whitelist

The ***Whitelist*** item opens a dialog with a global list of approved sender e-mail addresses and domain names whose messages will never be marked as spam.



In the editing interface you can compile a list of senders that you are sure will never send you unwanted messages (spam). You can also compile a list of full domain names (e.g. *avg.com*), that you know do not generate spam messages.

Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once. The following control buttons are available:

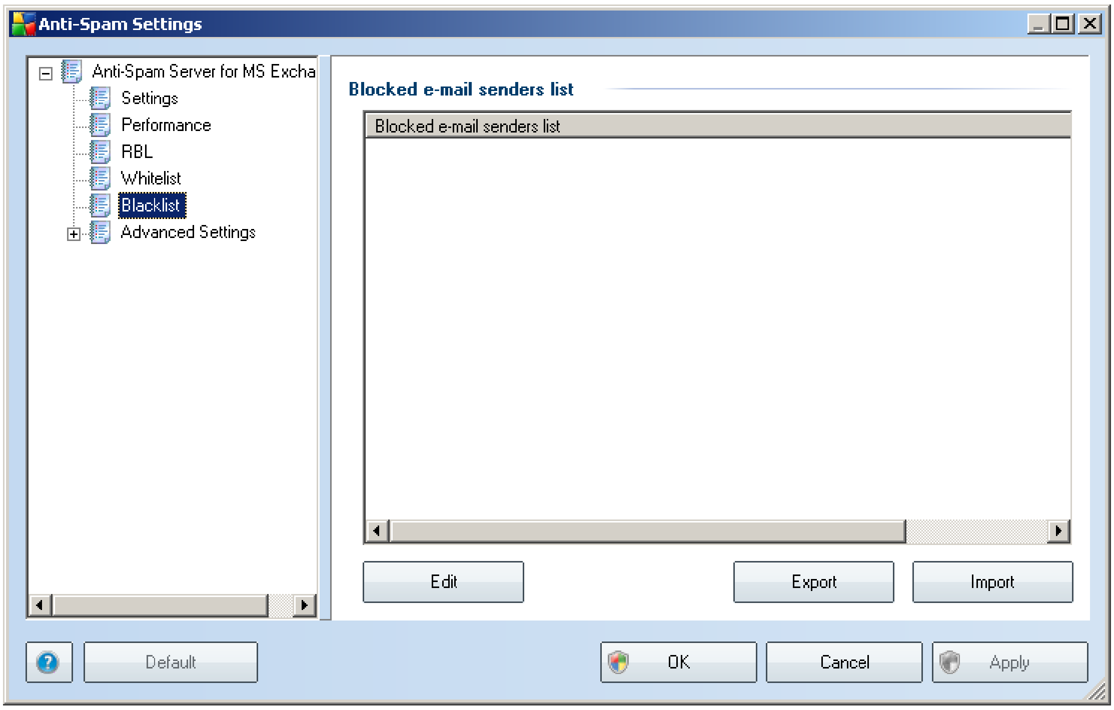
- ***Edit*** - press this button to open a dialog, where you can manually enter a list of addresses (you can also use *copy and paste*). Insert one item (sender, domain name) per line.

- ***Import*** - if you already have a text file of email addresses/domain names prepared, you can simply import it by selecting this button. The input file must be in plain text format, and the content must contain only one item (address, domain name) per line.

- ***Export*** - if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.

8.7. Blacklist

The ***Blacklist*** item opens a dialog with a global list of blocked sender e-mail addresses and domain names whose messages will always be marked as spam.



In the editing interface you can compile a list of senders that you expect to send you unwanted messages (spam). You can also compile a list of full domain names (e.g. *spammingcompany.com*), that you expect or receive spam messages from. All e-mail from the listed addresses/domains will be identified as spam.

Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once. The following control buttons are available:

- ***Edit*** - press this button to open a dialog, where you can manually enter a list of addresses (you can also use *copy and paste*). Insert one item (sender, domain name) per line.
- ***Import*** - if you already have a text file of email addresses/domain names prepared, you can simply import it by selecting this button. The input file must be in plain text format, and the content must contain only one item (address, domain name) per line.
- ***Export*** - if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.

8.8. Advanced Settings

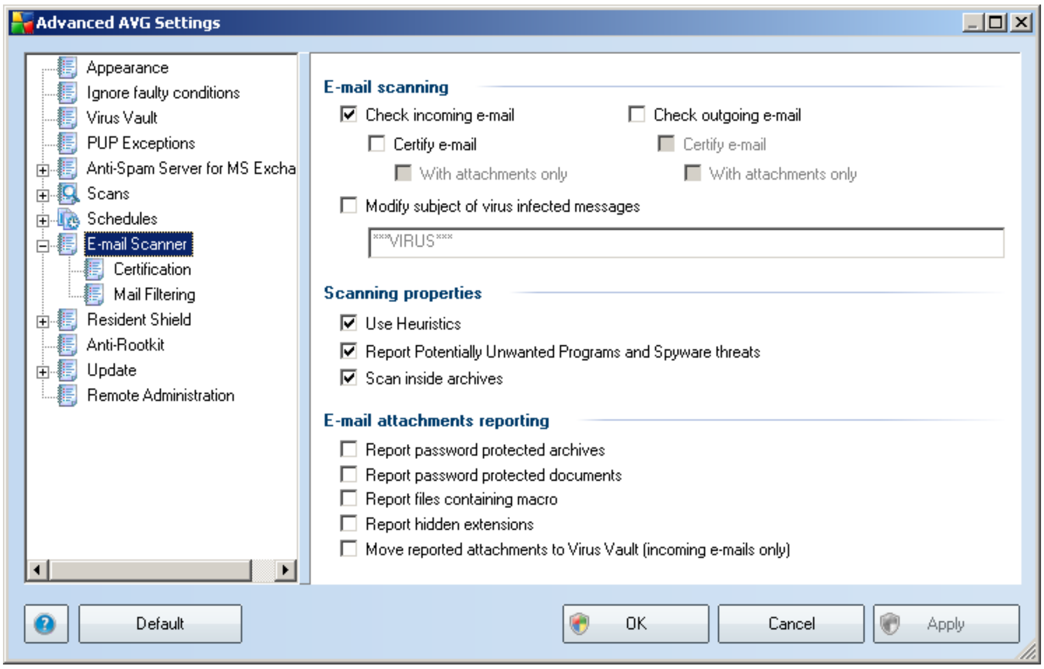
Typically it is recommended to keep the default settings and only change them if you have a valid reason to do so. Any changes to configuration should only be done by expert users!

If you still believe you need to change the Anti-Spam configuration at the very advanced level, please follow the instructions provided directly in the user interface. Generally, in each dialog you will find one single specific feature and you can edit it - its description is always included in the dialog itself:

- ***Cache*** - fingerprint, domain reputation, LegitRepute
- ***Training*** - word training, score history, score offset, maximum word entries, auto training threshold, weight, write buffer
- ***Filtering*** - language list, country list, approved IPs, blocked IPs, blocked countries, blocked charsets, spoofed senders
- ***RBL*** - RBL servers, multihit, threshold, timeout, maximum IPs
- ***Internet connection*** - timeout, proxy server, proxy server authentication

9. E-mail Scanner

The ***E-mail Scanner*** settings are configured from within the AVG E-mail Server Edition. From the application's main menu select ***Tools/Advanced Settings***. Then from the left menu in the **Advanced Settings** dialog, select the **E-Mail Scanner** item.



E-mail scanning

☑ Check incoming e-mail
□ Certify e-mail
□ With attachments only
□ Check outgoing e-mail
□ Certify e-mail
□ With attachments only
□ Modify subject of virus infected messages
VIRUS

Scanning properties

☑ Use Heuristics
☑ Report Potentially Unwanted Programs and Spyware threats
☑ Scan inside archives

E-mail attachments reporting

□ Report password protected archives
□ Report password protected documents
□ Report files containing macro
□ Report hidden extensions
□ Move reported attachments to Virus Vault (incoming e-mails only)

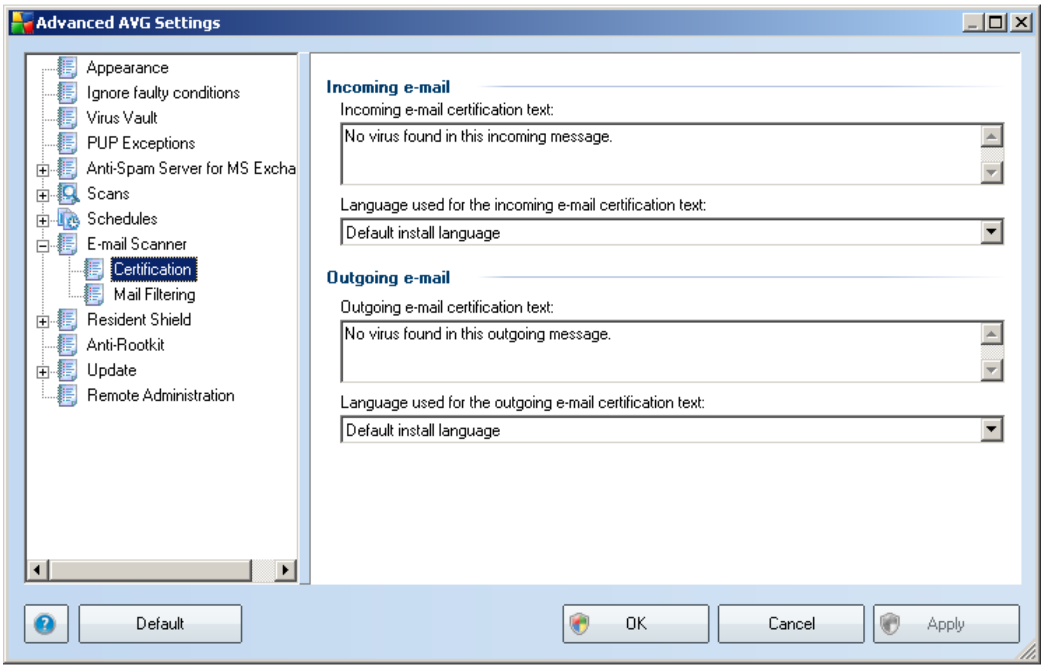
The ***E-mail Scanner*** dialog is divided into three sections:

- ***E-mail scanning*** - in this section select whether you want to scan the incoming/outgoing e-mail messages and whether all e-mails should be certified or only e-mails with attachments (e-*mail virus-free certification is not supported in HTML/RTF format*). Additionally you can choose if you want AVG to modify the subject for messages that contain potential viruses. Tick the ***Modify subject of virus infected messages*** checkbox and change the text respectively (*default value is ***VIRUS****).

- ***Scanning properties*** - specify whether the heuristic analysis method should be used during scanning (***Use heuristic***), whether you want to check for the presence of potentially unwanted programs (***Report Potentially Unwanted Programs and Spyware threats***), and whether archives should be scanned too (***Scan inside archives***).

- ***E-mail attachments reporting*** - specify whether you wish to be notified via e-mail about password protected archives, password protected documents, macro containing files and/or files with hidden extension detected as an attachment of the scanned e-mail message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the ***Virus Vault***.

9.1. Certification



Incoming e-mail

Incoming e-mail certification text: No virus found in this incoming message.

Language used for the incoming e-mail certification text: Default install language

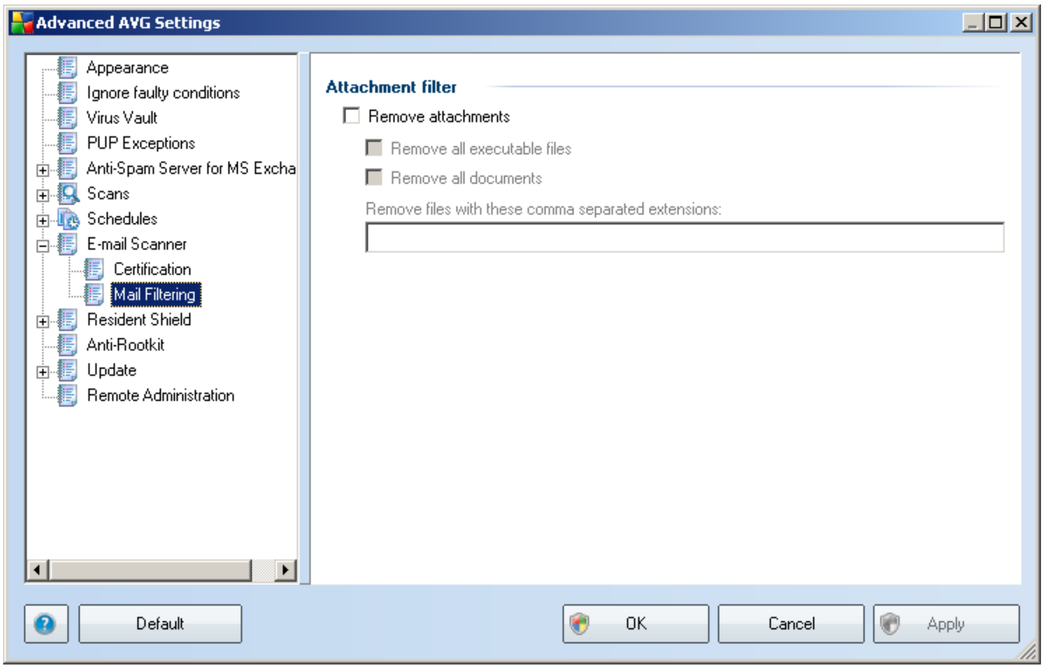
Outgoing e-mail

Outgoing e-mail certification text: No virus found in this outgoing message.

Language used for the outgoing e-mail certification text: Default install language

In the ***Certification*** dialog you can specify exactly what text the certification note should contain, and in what language. This should be specified separately for ***Incoming mail*** and ***Outgoing mail***.

9.2. Mail Filtering



Attachment filter

☐ Remove attachments

☐ Remove all executable files

☐ Remove all documents

Remove files with these comma separated extensions:

The ***Attachment filter*** dialog allows you to set up parameters for e-mail messages attachment scanning. By default, the ***Remove attachments*** option is switched off. If you decide to activate it, all e-mail message attachments detected as infectious or potentially dangerous will be removed automatically. If you want to define specific types of attachments that should be removed, select the respective option:

- ***Remove all executable files*** - all *.exe files will be deleted
- ***Remove all documents*** - all *.doc files will be deleted
- ***Remove files with these comma separated extensions*** - will remove all files with the defined extensions

10. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the ***FAQ*** section of the AVG website at www.avg.com.

If you do not succeed in finding help this way, contact the technical support department by email. Please use the contact form accessible from the system menu via ***Help / Get help online***.