AVG Email Server Edition

User Manual

Document revision 2015.11 (23.3.2015)

Contents

1. Introduction

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

Congratulations on your purchase of AVG Email Server Edition!

AVG 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 server. As with all AVG products **AVG 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.

Note: *This documentation contains description of specific Email Server Edition features. Should you require information about other AVG features, please consult the user guide to Internet Security edition, which contains all the necessary details. You can download the guide from the http://www.avg.com.*

2. AVG Installation Requirements

2.1. Operation Systems Supported

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

- Windows 2012 Server R2 Edition
- Windows 2012 Server Edition (x86 and x64)
- Windows 2008 Server R2 Edition
- Windows 2008 Server Edition (x86 and x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Email Servers Supported

The following mail servers are supported:

- MS Exchange 2003 Server version
- MS Exchange 2007 Server version
- MS Exchange 2010 Server version
- MS Exchange 2013 Server version
- Kerio MailServer – version 6.7.2 and higher

2.3. Hardware Requirements

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

- Intel Pentium CPU 1.5 GHz
- 500 MB of free hard drive space (for installation purposes)
- 512 MB of RAM memory

Recommended hardware requirements for **AVG Email Server Edition** are:

- Intel Pentium CPU 1.8 GHz
- 600 MB of free hard drive space (for installation purposes)
- 512 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 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 (or you can do this maybe even easier via menu ***Start/All Programs/AVG/Uninstall AVG***).

- If you have previously used the AVG 8.x or older version, do not forget to uninstall also individual server plug-ins.

  Note: *It will be necessary to restart the store service during the uninstallation process.*

  Exchange plug-in - run setupes.exe with the /uninstall parameter from the folder where the plug-in was installed.

  e.g. C:\AVG4ES2K\setupes.exe /uninstall

  Lotus Domino/Notes plug-in - run setupln.exe with the /uninstall parameter from folder where the plug-in was installed:

  e.g. C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange Service Packs

There is no service pack required for MS Exchange 2003 Server; 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/en-us/download/details.aspx?id=9664

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.

Service Pack for MS Exchange 2007 Server (optional):

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

Service Pack for MS Exchange 2010 Server (optional):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

3. AVG Installation Process

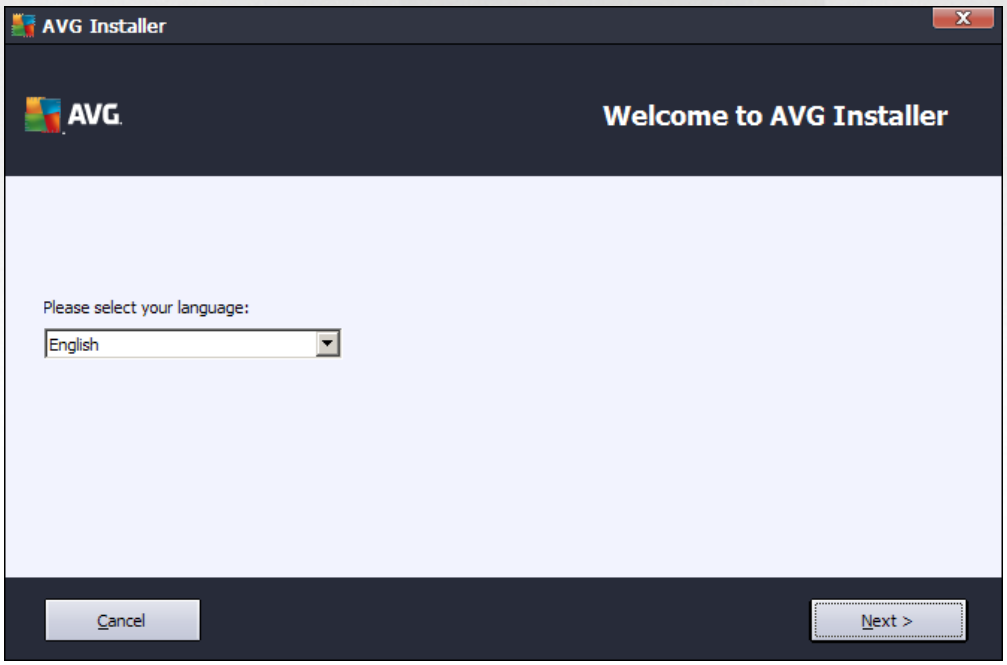
To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from the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

There are two installation packages available for your product - for 32bit operating systems (marked as x86) and for 64bit operating systems (marked as x64). Be sure to use the correct installation package for your specific operating system.

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

Once you have downloaded and saved the installation file on your hard drive, 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:

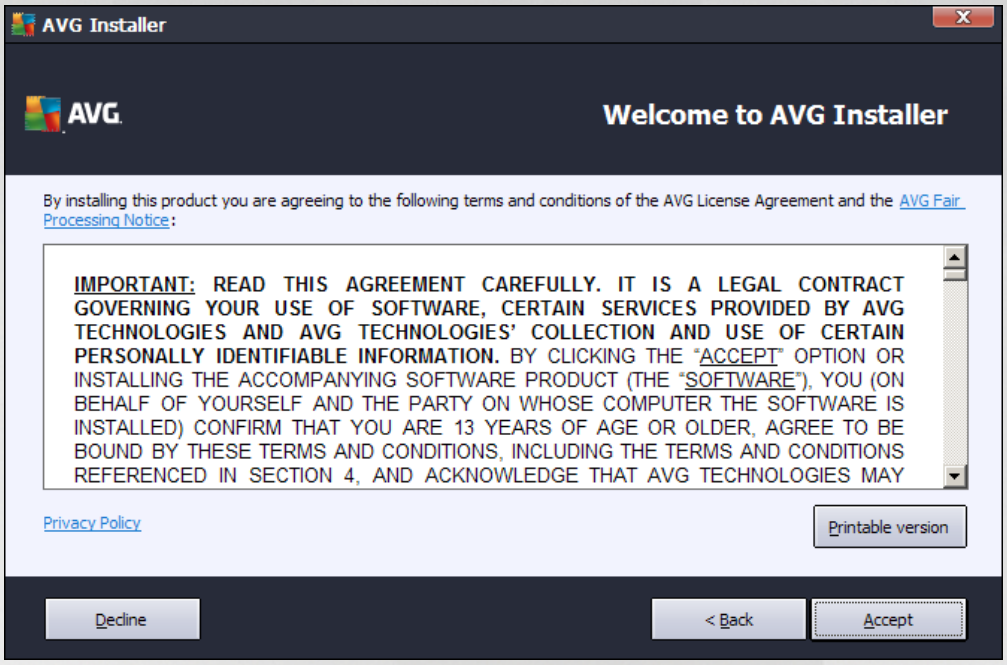
3.1. Installation Launch



The installation process always starts with this window. In here you select the language used for the installation process and press the ***Next*** button.

You will be able to choose also additional languages for the application interface later during the installation process.

3.2. License Agreement

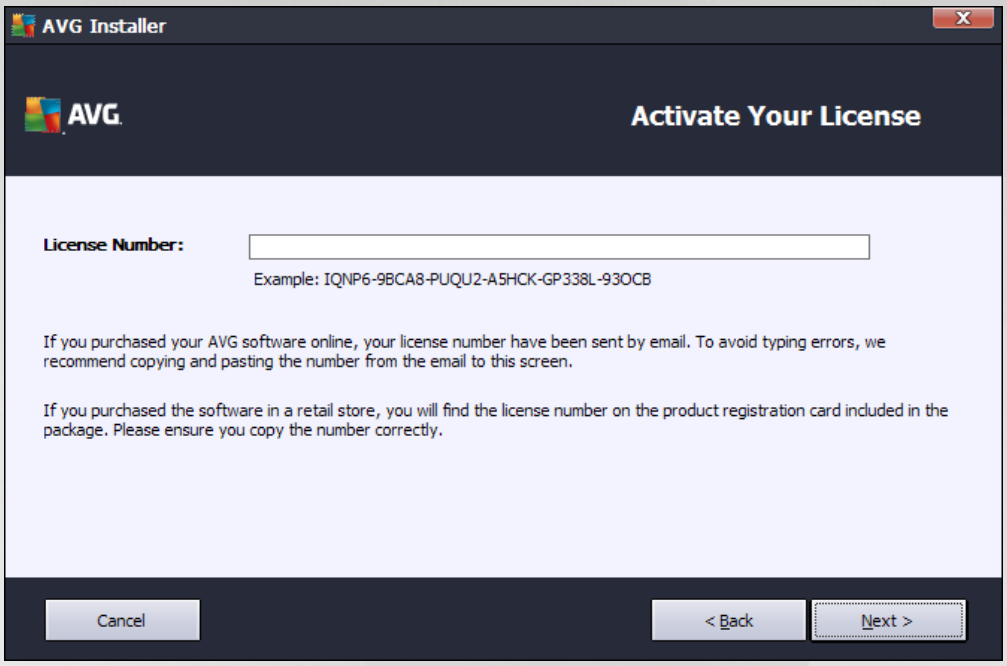


This dialog allows you to read the license conditions. Use the ***Printable version*** button to open the license text in a new window. Press the ***Accept*** button to confirm and continue to the next dialog.

3.3. Activate Your License

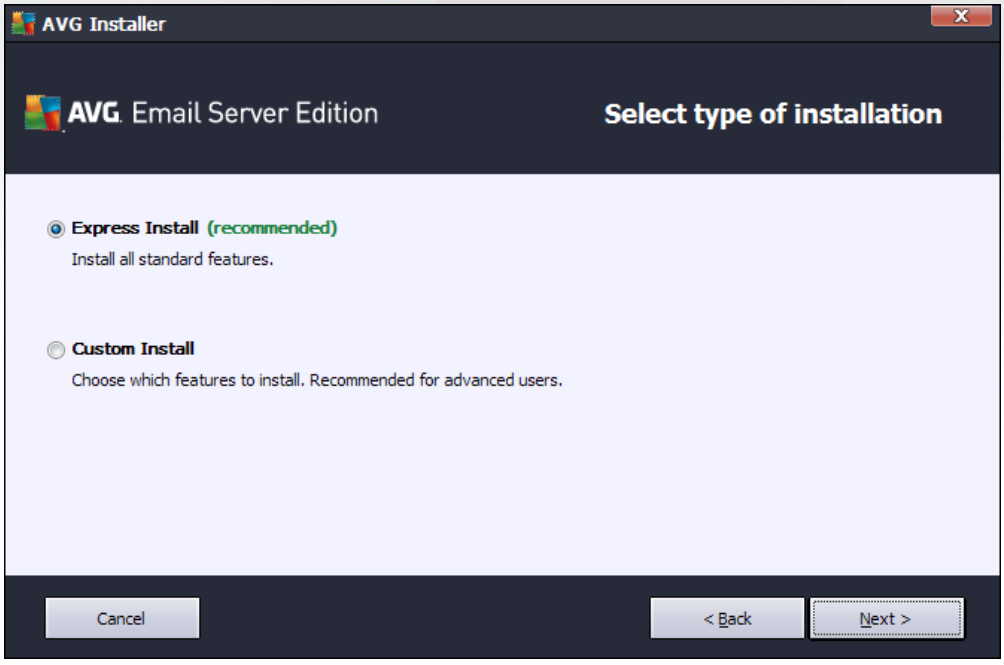
In the ***Activate your License*** dialog you have to fill in your license number.

Enter your license 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.



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

3.4. Select Installation Type



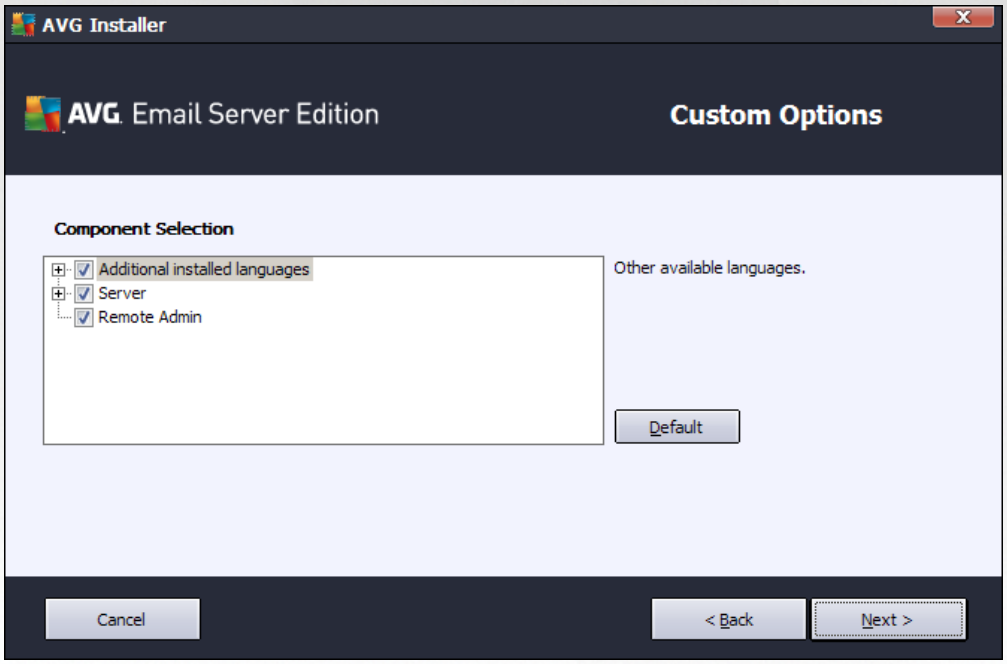
The ***Select type of Installation*** dialog offers the choice of two installation options: ***Express Install*** and ***Custom Install***.

For most users, it is highly recommended to keep to the ***Express Install*** 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 Install 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.

Upon selecting the Custom Install, the ***Destination folder*** section appears in the lower part of the dialog. It 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.

3.5. Custom Install - Custom Options



The ***Component selection*** section 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 Admin*** - if you intend to connect AVG to an AVG DataCenter (AVG Network Editions), then you need to select this option.

- ***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.

Basic overview of the individual server components (under the ***Server*** branch):

- ***Anti-Spam Server for MS Exchange***

  Checks all incoming email messages and marks unwanted emails as SPAM. It uses several analyzing methods to process each email message, offering maximum possible protection against unwanted email messages.

- ***Email Scanner for MS Exchange (routing Transport Agent)***

  Checks all incoming, outgoing and internal email messages going through the MS Exchange HUB role.

- ***Email Scanner for MS Exchange (SMTP Transport Agent)***

  Checks all email messages coming through the MS Exchange SMTP interface (can be installed for both EDGE and HUB roles).

- ***Email Scanner for MS Exchange (VSAPI)***

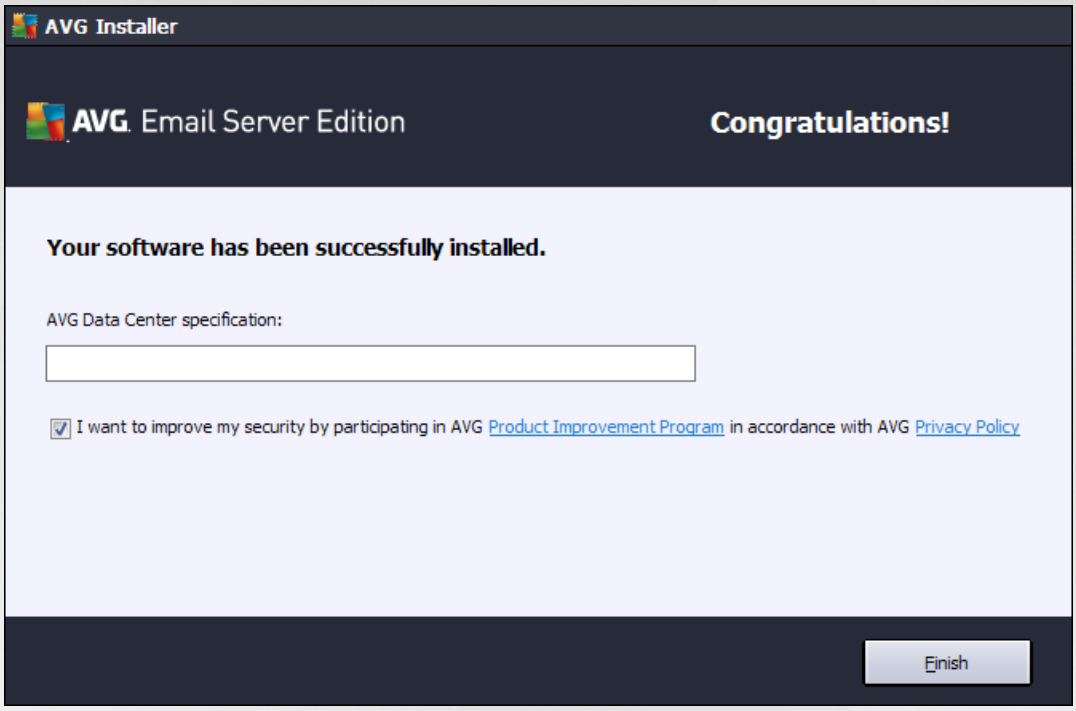
  Checks all email messages stored in user mailboxes. If any viruses are detected, they are moved to the Virus Vault, or completely removed.

For Exchange 2003 users only Anti-Spam and Email Scanner (VSAPI) components are available.

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

3.6. Installation Completion

If you selected the ***Remote Administration*** module during module selection, then the final screen will allow you to define the connection string for connecting to your AVG DataCenter.



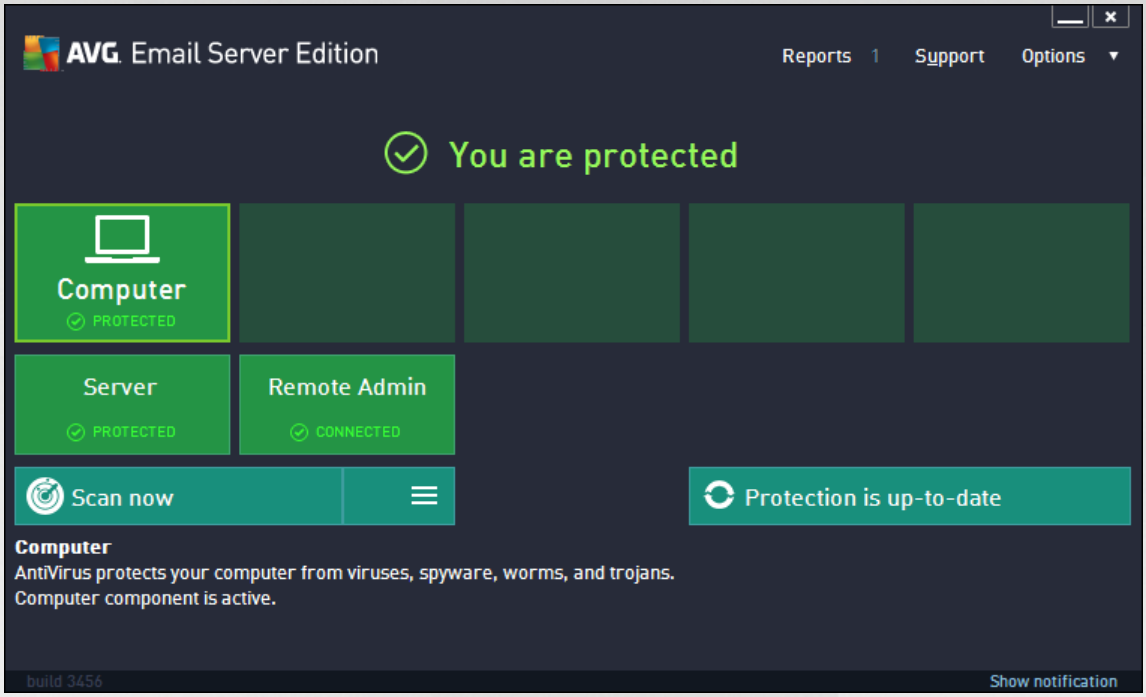
This dialog also allows you to decide whether you want to participate in the Product Improvement Program that collects anonymous information on detected threats in order to increase the overall Internet security level. If you agree with this statement, please keep the ***I want to improve my security by participating in AVG Product Improvement Program in accordance with AVG Privacy Policy*** option checked *(the option is confirmed, by default)*.

Confirm your choices by clicking the **Finish** button.

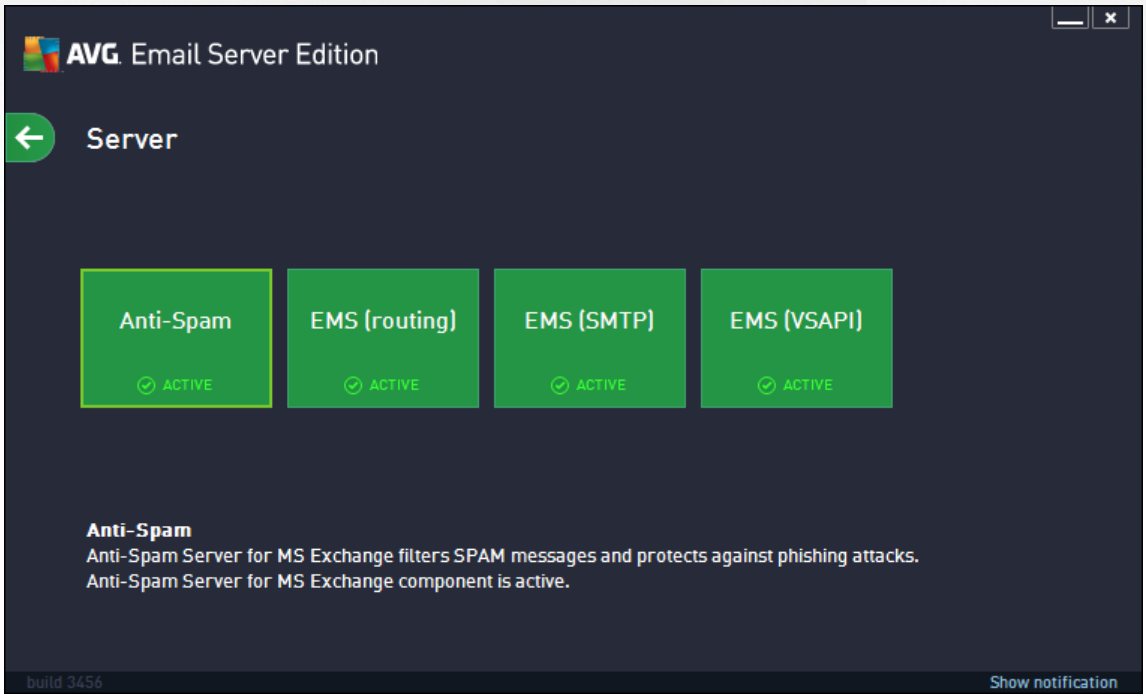
AVG is now installed on your computer and fully functional. The program is running in the background in fully automatic mode.

4. After Installation

Immediately after the installation is done, the ***AVG Email Server Edition*** main screen appears:



This manual only deals with the ***AVG Email Server Edition*** specific features; all other components and settings are being described in the AVG Desktop manual. To access the main server components dialog, click the ***Server*** button (the one circled in red in the screenshot above). You will see the following screen:



Please note that all server components will be available (unless you chose not to install some of them during the installation process, of course) only if you are using MS Exchange 2007 or higher. MS Exchange 2003 only supports Anti-Spam and Email Scanner (VSAPI) components.

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

- ***Email Scanners for MS Exchange***
- ***Anti-Spam Server for MS Exchange***
- ***AVG for Kerio MailServer***

5. Email Scanners for MS Exchange

5.1. Overview

Basic overview of the individual Email Scanner server components:

- ***EMS (routing) - Email Scanner for MS Exchange (routing Transport Agent)***

  Checks all incoming, outgoing and internal email messages going through the MS Exchange HUB role.

  Available for MS Exchange 2007/2010/2013 and can be installed for HUB role only.

- ***EMS (SMTP) - Email Scanner for MS Exchange (SMTP Transport Agent)***

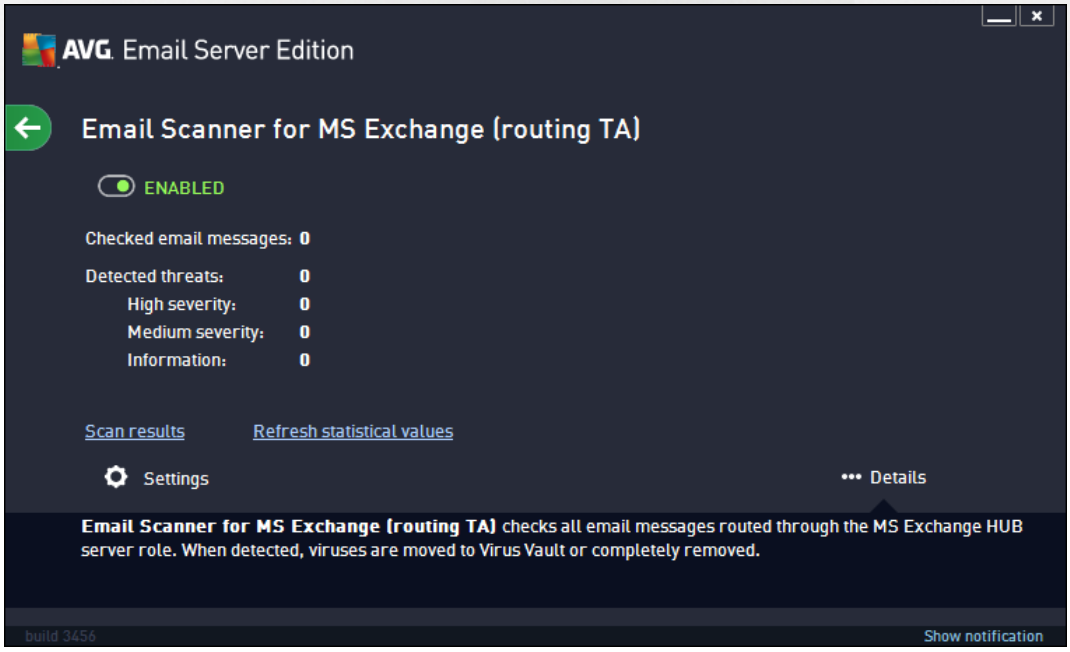
  Checks all email messages coming through the MS Exchange SMTP interface.

  Available for MS Exchange 2007/2010/2013 only and can be installed for both EDGE and HUB roles.

- ***EMS (VSAPI) - Email Scanner for MS Exchange (VSAPI)***

  Checks all email messages stored in user mailboxes. If any viruses are detected, they are moved to the Virus Vault, or completely removed.

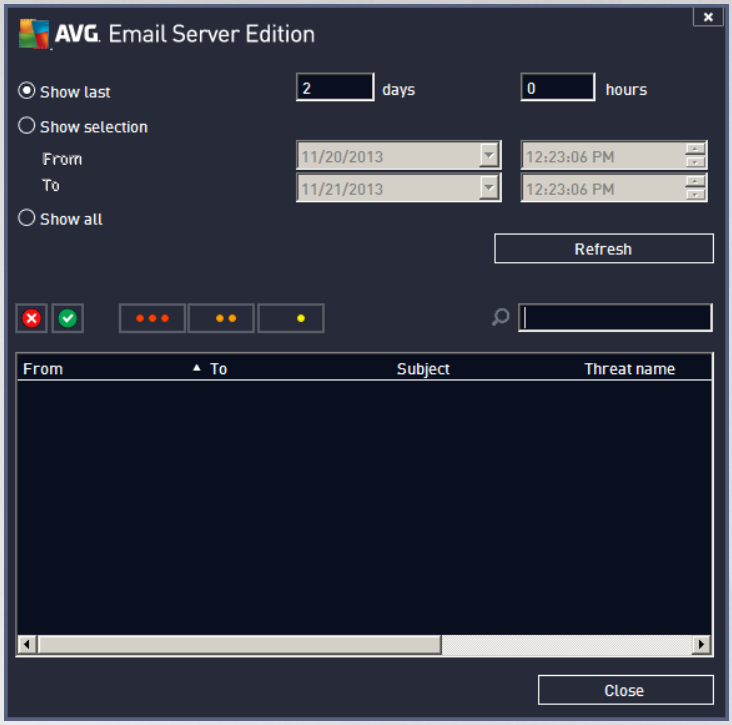
Click a required component icon to open its interface. All the components share the following common control buttons and links:



- ***ENABLED/DISABLED*** - clicking this button turns the selected component on/off (if the component is on, the button and the text are green, if it's off, they are red).

- ***Scan Results***

Opens a new dialog where you can review scan results:



Here you can check messages divided into several tabs according to their severity. See configuration of individual components for amending the severity and reporting.

By default there are displayed only results for the last two days. You can change the displayed period by amending the following options:

- o ***Show last*** - insert preferred days and hours.
- o ***Show selection*** - choose a custom time and date interval.
- o ***Show all*** - Displays results for the whole time period.

Use ***Refresh*** button to reload the results.

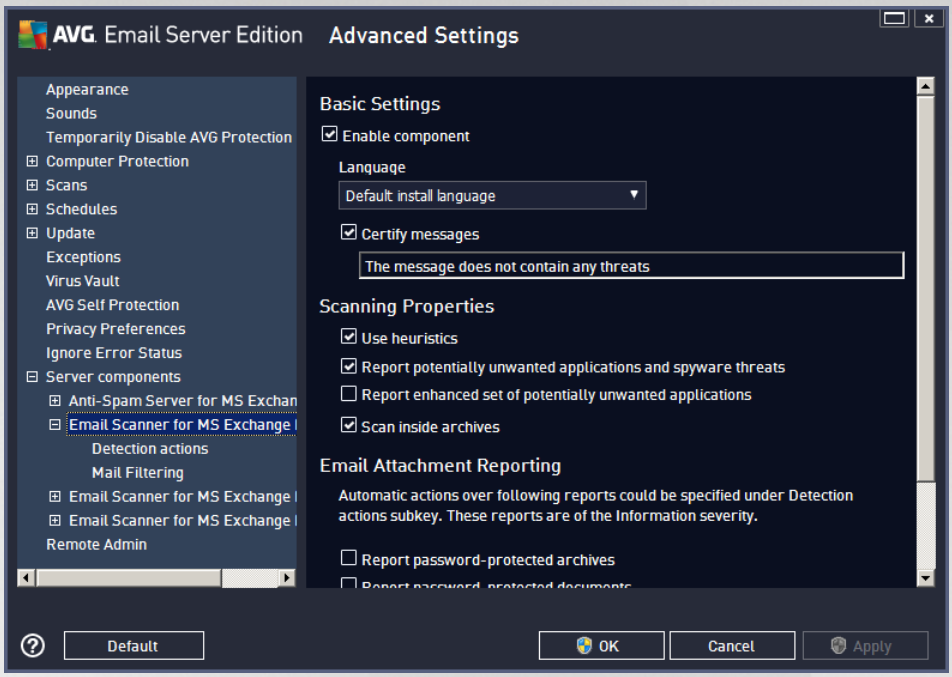
- ***Refresh statistical values*** - updates stats displayed above.

Clicking the ***Settings*** working button opens advanced settings for the selected component (you will find more information on individual settings of all components in the chapters below).

5.2. Email Scanner for MS Exchange (routing TA)

To open the settings of ***Email Scanner for MS Exchange (routing transport agent)***, select the ***Settings*** button from the interface of the component.

From the ***Server components*** list select the ***Email Scanner for MS Exchange (routing TA)*** item:



The ***Basic Settings*** section contains the following options:

- ***Enable component*** - uncheck to disable the whole component.
- ***Language*** - select preferred component language.
- ***Certify messages*** - check this if you wish to add a certification note to all scanned messages. You can customize the message in the next field.

The ***Scanning properties*** section:

- ***Use Heuristics*** - check this box to enable heuristic analysis method during scanning.
- ***Report Potentially Unwanted Applications and Spyware threats*** - check this option to report the presence of potentially unwanted applications and spyware.
- ***Report enhanced set of Potentially Unwanted Applications*** - check to detect extended package of spyware: applications that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later, or applications that always harmless but might be unwanted (various toolbars etc.). This is an additional measure that increases your computer security and comfort even more, however it can possibly block legal applications, and is therefore switched off by default. Note: This detection feature is additional to the previous option, so if you want protection from the basic types of spyware, always keep the previous box checked.
- ***Scan inside archives*** - check this option to let the scanner look also inside archived files (zip, rar, etc.).

The ***Email attachments reporting*** section allows you to choose which items should be reported during scanning. If checked, each email with such an item will contain [INFORMATION] tag in the message subject. This is the default configuration which can be easily amended in the ***Detection actions section***, part ***Information*** (see below).

The following options are available:

- ***Report password protected archives***
- ***Report password protected documents***
- ***Report files containing macro***
- ***Report hidden extensions***

There are also these sub-items available in the following tree structure:

- ***Detection actions***
- ***Mail filtering***

5.3. Email Scanner for MS Exchange (SMTP TA)

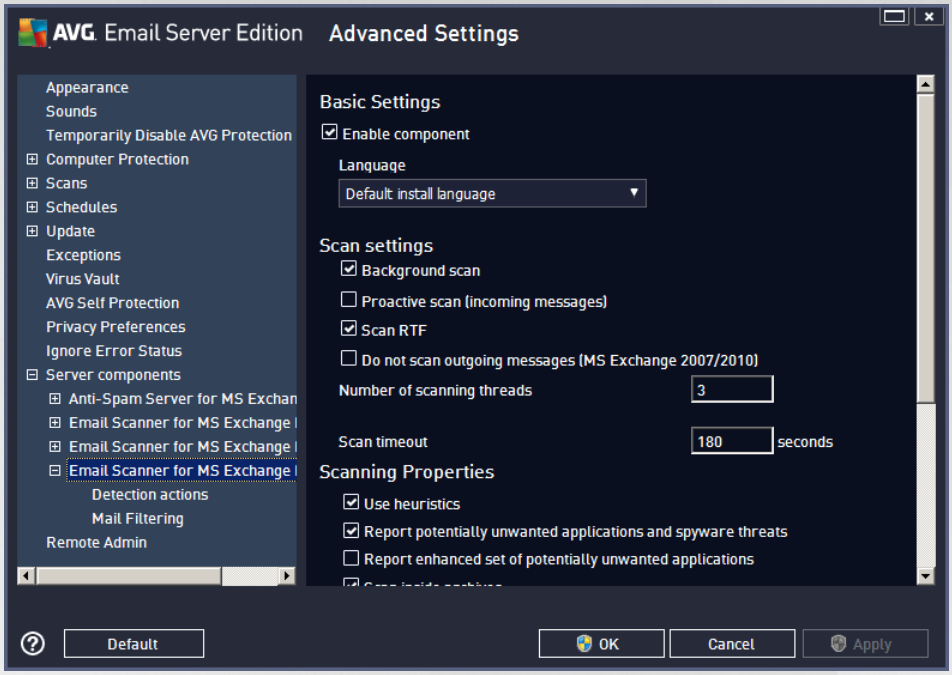
The configuration for the ***Email Scanner for MS Exchange (SMTP Transport Agent)*** is exactly the same as in the case of routing transport agent. For more information please see the ***Email Scanner for MS Exchange (routing TA)*** chapter above.

There are also these sub-items available in the following tree structure:

- ***Detection actions***
- ***Mail filtering***

5.4. Email Scanner for MS Exchange (VSAPI)

This item contains settings of the ***Email Scanner for MS Exchange (VSAPI)***.



The ***Basic Settings*** section contains the following options:

- ***Enable component*** - uncheck to disable the whole component.
- ***Language*** - select preferred component language.

The ***Scan settings*** section:

- ***Background Scan*** - 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 with the latest AVG virus base update is encountered in the users' mailbox folders, it is submitted to AVG for Exchange 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. email messages storage in the Microsoft Exchange database) are always carried out preferentially.

- ***Proactive Scan (incoming messages)***

  You can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. This scanning occurs when an item is delivered to a folder, but a request has not been made by a client.

  As soon as messages are submitted to the Exchange store, they enter the global scanning queue as low priority (maximum of 30 items). They are scanned on the first in, first out (FIFO) basis. If an item is accessed while still in the queue, it is changed to high priority.

Overflow messages will continue to the store unscanned.

Even if you disable both ***Background Scan*** and ***Proactive Scan*** options, the on access scanner will be still active when an user will try to download a message with the MS Outlook client.

- ***Scan RTF*** - you can specify here, whether the RTF file type should be scanned or not.
- ***Do not scan outgoing messages (MS Exchange 2007/2010/2013)*** - with both VSAPI and Routing Transport Agent (routing TA) server components installed (it doesn't matter if it's on one single server, or two different ones), it may occur that outgoing mail is scanned twice. The first scan is done by VSAPI On-access scanner, while the second one by the Routing Transport Agent. This might cause certain server slowdowns and moderate delays in sending emails. If you're sure that you have both server components installed and active, you can choose to avoid this double outgoing email scanning by checking this box and disabling the VSAPI On-access scanner.
- ***Number of 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.

  The minimum number of threads is computed as ('number of processors'+1) divided by 2.

  The maximum number of threads is computed as 'Number of Processors' multiplied by 5 + 1.

  If the value is the minimum or lesser value or the maximum or greater, the default value is used.

- ***Scan Timeout*** - the maximum continuous interval (in seconds) for one thread to access the message that is being scanned (the default value is 180 seconds).

The ***Scanning properties*** section:

- ***Use Heuristics*** - check this box to enable heuristic analysis method during scanning.
- ***Report Potentially Unwanted Applications and Spyware threats*** - check this option to report the presence of potentially unwanted applications and spyware.
- ***Report enhanced set of Potentially Unwanted Applications*** - check to detect extended package of spyware: applications that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later, or applications that always harmless but might be unwanted (various toolbars etc.). This is an additional measure that increases your computer security and comfort even more, however it can possibly block legal applications, and is therefore switched off by default. Note: This detection feature is additional to the previous option, so if you want protection from the basic types of spyware, always keep the previous box checked.
- ***Scan inside archives*** - check this option to let the scanner look also inside archived files (zip, rar, etc.).

The ***Email attachments reporting*** section allows you to choose which items should be reported during scanning. The default configuration can be easily amended in the ***Detection actions section***, part ***Information*** (see below).

The following options are available:

- ***Report password protected archives***
- ***Report password protected documents***
- ***Report files containing macro***
- ***Report hidden extensions***

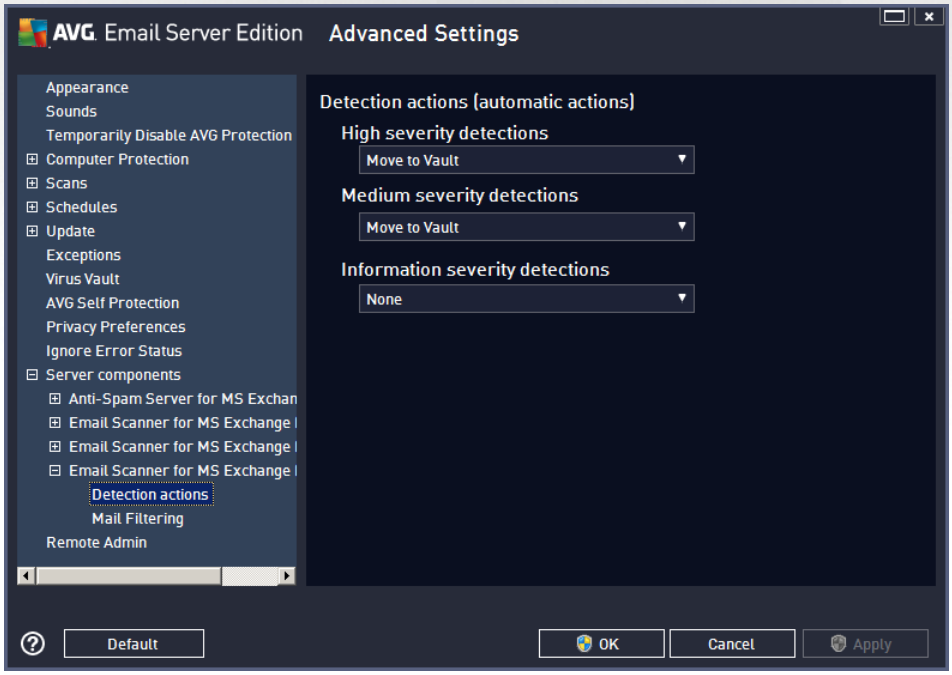
Generally, some of these features are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI 2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

- http://support.microsoft.com/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.

There are also these sub-items available in the following tree structure:

- ***Detection actions***
- ***Mail filtering***

5.5. Detection Actions



In the ***Detection actions*** sub-item you can choose automatic actions that should take place during the scanning process.

The actions are available for the following items:

- ***High severity detections*** – malicious codes that copy and spread themselves, often unnoticed until the damage is done.
- ***Medium severity detections*** – such programs, in general, vary from positively serious to only potential threats to your privacy.
- ***Information severity detections*** – includes all detected potential threats that cannot be classified as any of the above categories.

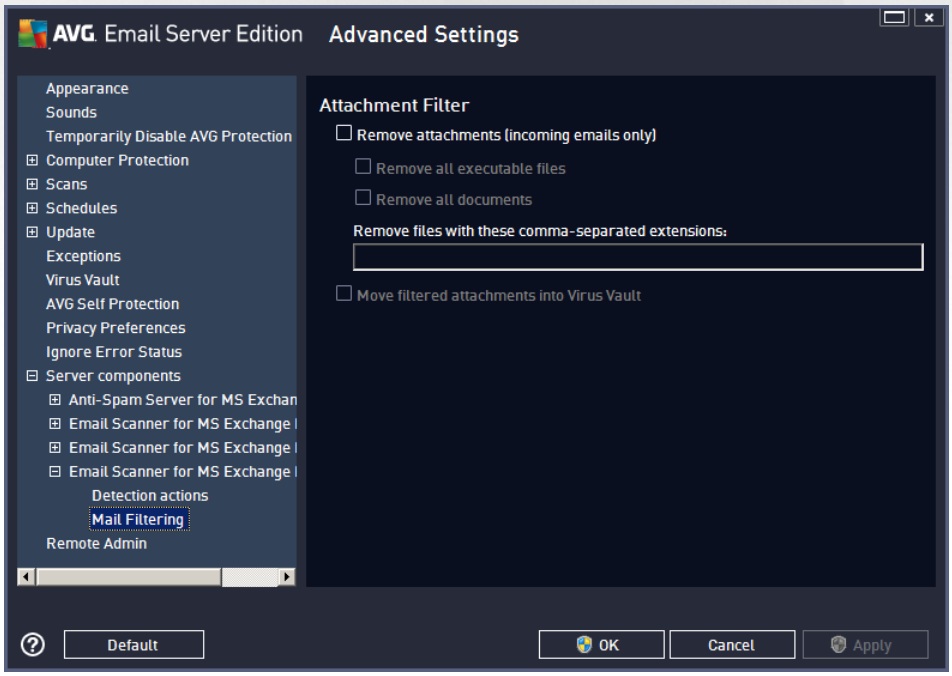
Use the roll-down menu to choose an action for each item:

- ***None*** - no action will be taken.
- ***Move to Vault*** - the given threat will be moved to Virus Vault.
- ***Remove*** - the given threat will be removed.

To select a custom subject text for messages that contain the given item/threat, check the ***Mark subject with...*** box and fill-in a preferred value.

The last mentioned feature is not available for Email Scanner for MS Exchange VSAPI.

5.6. Mail Filtering



In the ***Mail Filtering*** sub-item you can choose which attachments should be automatically removed, if any. The following options are available:

- ***Remove attachments*** - check this box to enable the feature.

- ***Remove all executable files*** - removes all executables.
- ***Remove all documents*** - removes all document files.
- ***Remove files with these comma separated extensions*** - fill the box with file extensions you wish to automatically remove. Separate the extensions with comma.
- ***Move filtered attachments into virus vault*** - check if you don't want the filtered attachments to be removed completely. With this box checked, all attachments chosen in this dialog will be automatically moved into the Virus Vault quarantine environment. It is a safe place to store potentially malicious files - you can view and examine them without endangering your system. The Virus Vault can be accessed from the upper menu of your **AVG Email Server Edition** main interface. Simply left-click the ***Options*** item a choose ***Virus Vault*** item from the drop-down menu.

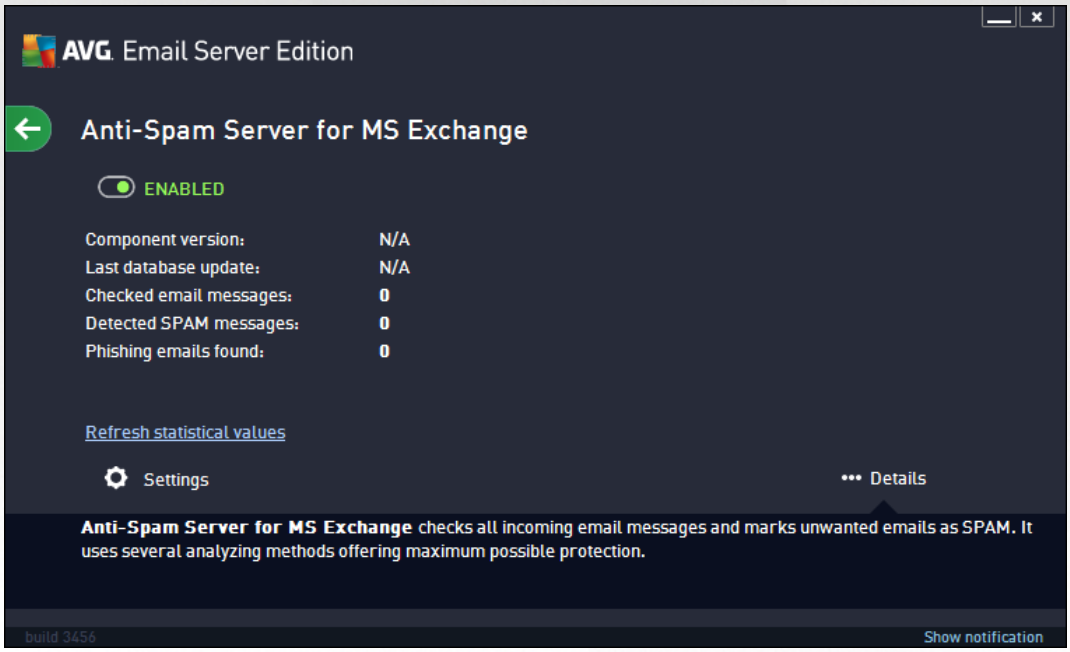
6. Anti-Spam Server for MS Exchange

6.1. Anti-Spam Principles

Spam refers to unsolicited email, mostly advertising a product or service that is mass mailed to a huge number of email addresses at a time, filling recipients' mail boxes. Spam does not refer to legitimate commercial email 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 email messages and marks unwanted emails as SPAM. It uses several analyzing methods to process each email message, offering maximum possible protection against unwanted email messages.

6.2. Anti-Spam Interface



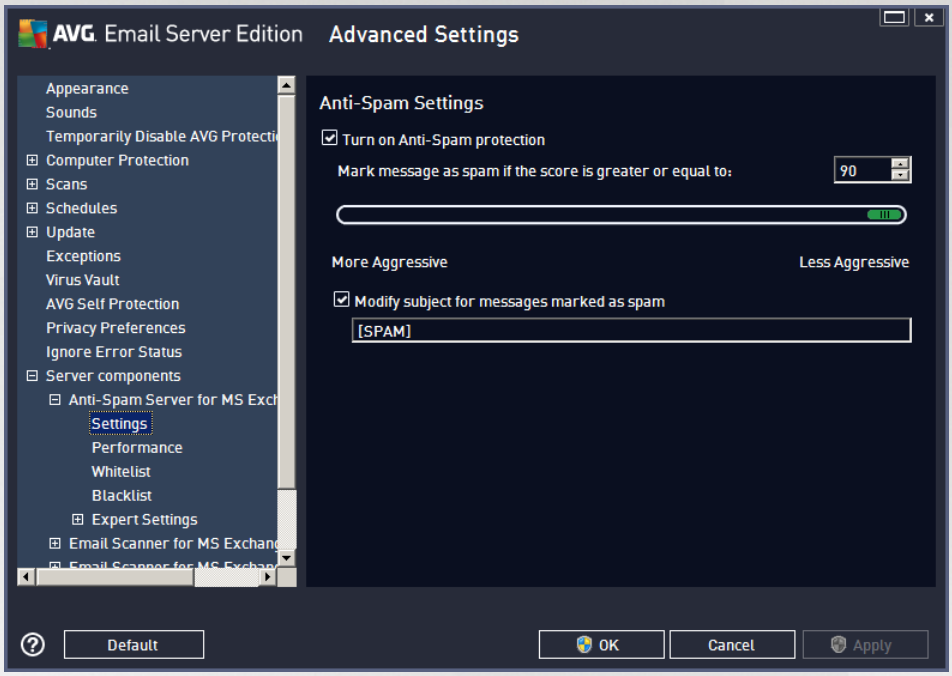
This dialog contains a brief information about the functionality of the server component, information on its current status (*Enabled/Disabled*), and some statistics.

Available buttons and links:

- ***ENABLED/DISABLED*** - clicking this button turns the selected component on/off (if the component is on, the button and the text are green, if it's off, they are red).
- ***Refresh statistical values*** - updates stats displayed above.
- ***Settings*** - use this button to open advanced Anti-Spam settings.

6.3. Anti-Spam Settings

6.3.1. Settings



In this dialog you can check the ***Turn on Anti-Spam protection*** checkbox to allow/forbid the anti-spam scanning of email 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 (*50 to 90*) or by moving the slider left or right.

Here is a general review of the scoring threshold:

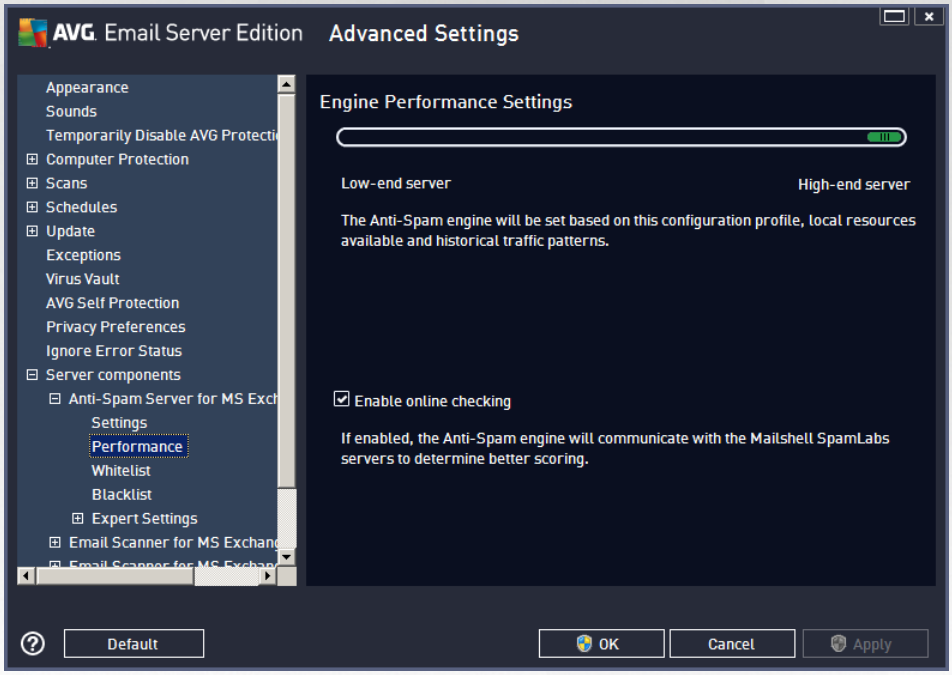
- ***Value 90*** - Most incoming email messages will be delivered normally (without being marked as spam). The most easily identified spam will be filtered out, but a significant amount of spam may still be allowed through.
- ***Value 80-89*** - Email messages likely to be spam will be filtered out. Some non-spam messages may be incorrectly filtered as well.
- ***Value 60-79*** - Considered as a quite aggressive configuration. Email messages that are possibly spam will be filtered out. Non-spam messages are likely to be caught as well.
- ***Value 50-59*** - Very aggressive configuration. Non-spam email messages are as likely to be caught as real spam messages. This threshold range is not recommended for normal use.

You can further define how the detected spam email 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 Email subject field; the desired text can be typed in the activated text field.

- ***Ask before reporting wrong detection*** - provided that during the installation process you agreed to participate in the Product Improvement Programme - this programme helps us to collect up-to-date information on the latest threats from all participants worldwide, and in return we can improve protection for everyone - i.e. you allowed reporting of detected threats to AVG. The reporting is taken care of automatically. However, you may mark this check box to confirm you want to be asked before any detected spam gets reported to AVG to make sure the message should really be classified as spam.

6.3.2. Performance



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.

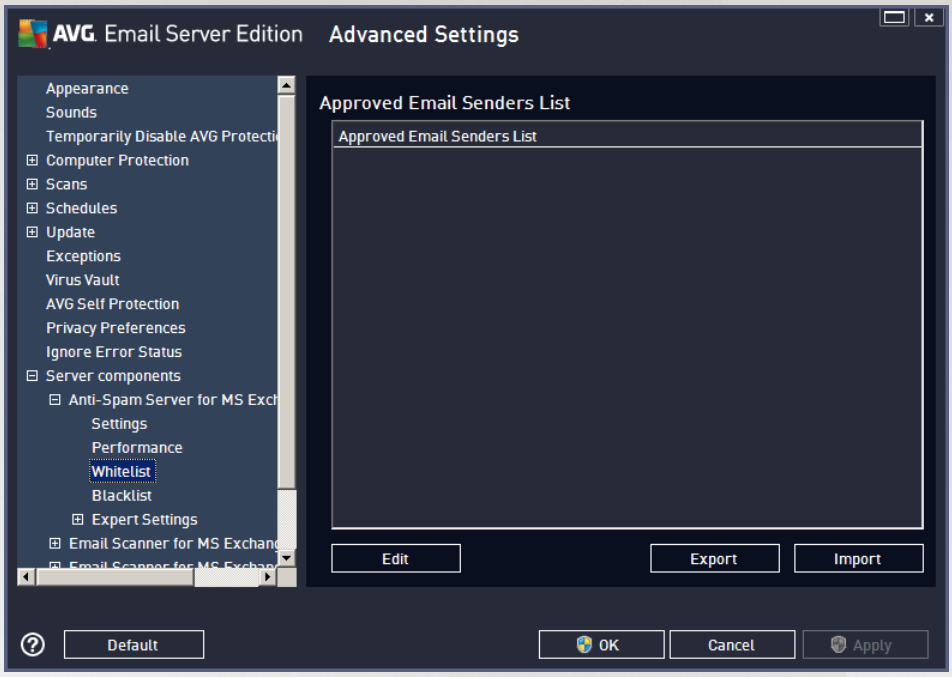
- ***High performance*** - this mode will consume large amount of memory. During the scanning process to identify spam, the following features will be used: rules and spam database cache, basic and advanced rules, spammer IP addresses and spammer databases.

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!

6.3.3. Whitelist

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



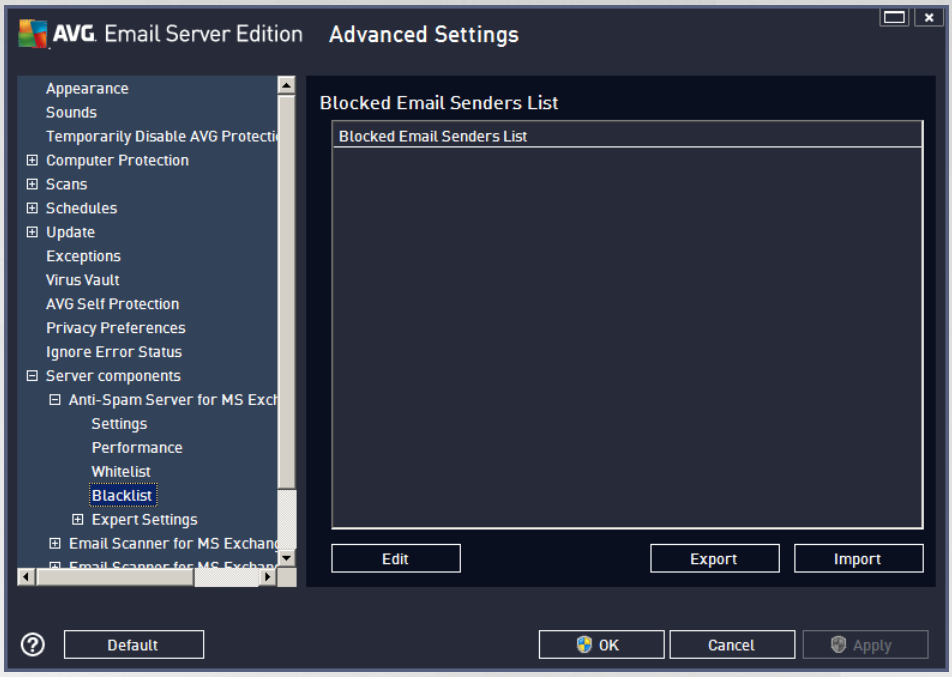
In the editing interface you can compile a list of senders that you are sure will never send you unwanted messages (spam). You can also compile a list of full domain names (e.g. *avg.com*), that you know do not generate spam messages.

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 email 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*** - you can import your existing email addresses by selecting this button. The input file can be a text file (in plain text format, and the content must contain only one item - address, domain name - per line), WAB file or the import can be done from Windows Address Book or Microsoft Office Outlook.
- ***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.

6.3.4. Blacklist

The ***Blacklist*** item opens a dialog with a global list of blocked sender email 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 email 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 email 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*** - you can import your existing email addresses by selecting this button. The input file can be a text file (in plain text format, and the content must contain only one item - address, domain name - per line), WAB file or the import can be done from Windows Address Book or Microsoft Office Outlook.
- ***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.

6.3.5. Expert Settings

This branch contains extensive setting options for the Anti-Spam component. These settings are intended exclusively for experienced users, typically network administrators who need to configure the antispam protection in full detail for the best protection of mail servers. For this reason, there is no extra help available for the individual dialogs; however, there is a brief description of each respective option directly in the user interface.

We strongly recommend not changing any settings unless you are fully familiar with the advanced settings for

Spamcatcher (MailShell Inc.). Any inappropriate changes may result in bad performance or incorrect component functionality.

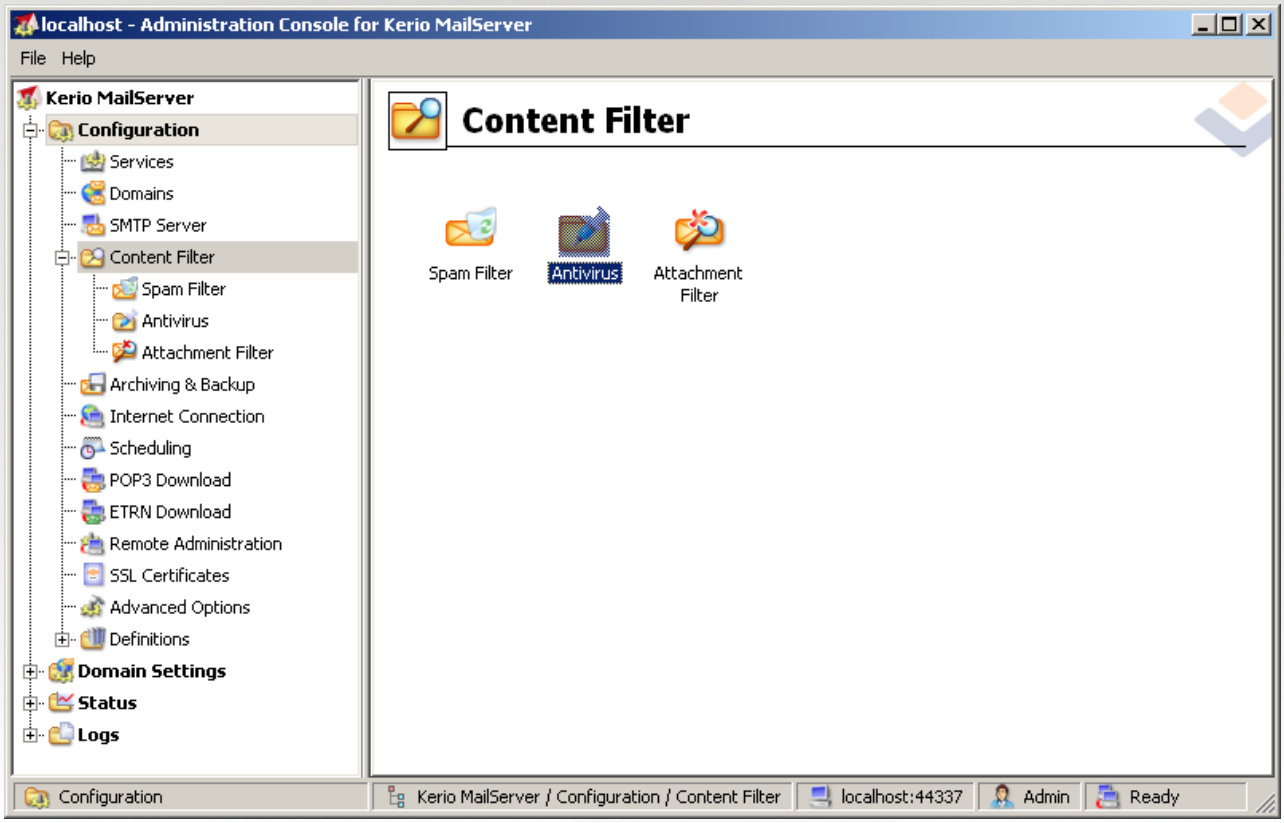
If you still believe you need to change the Anti-Spam configuration at the very advanced level, please follow the instructions provided directly in the user interface. Generally, in each dialog you will find one single specific feature that you can edit - its description is always included in the dialog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

- ***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 authentication

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 email 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:

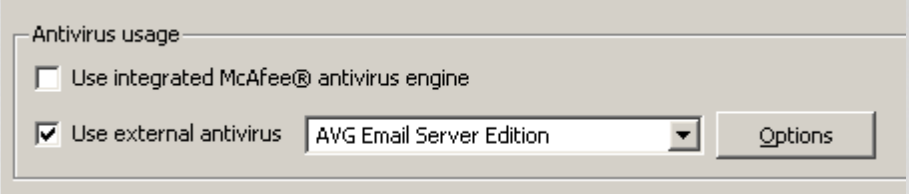


Clicking the Content Filter item will display a dialog with three items:

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

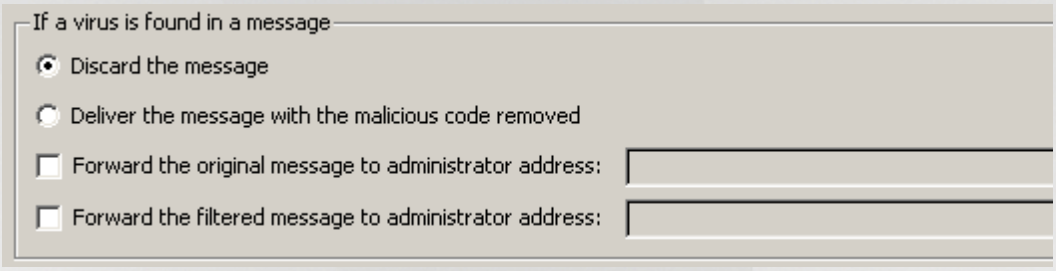
7.1.1. Antivirus

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:



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

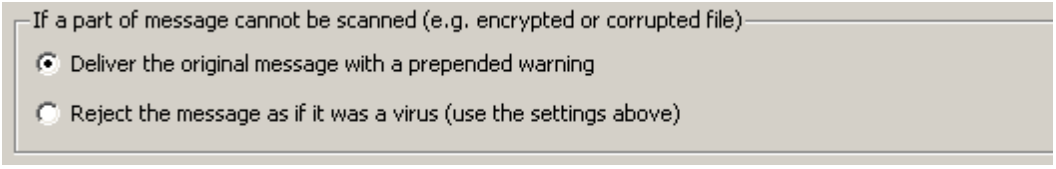
- ***If a virus is found in a message***



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)***



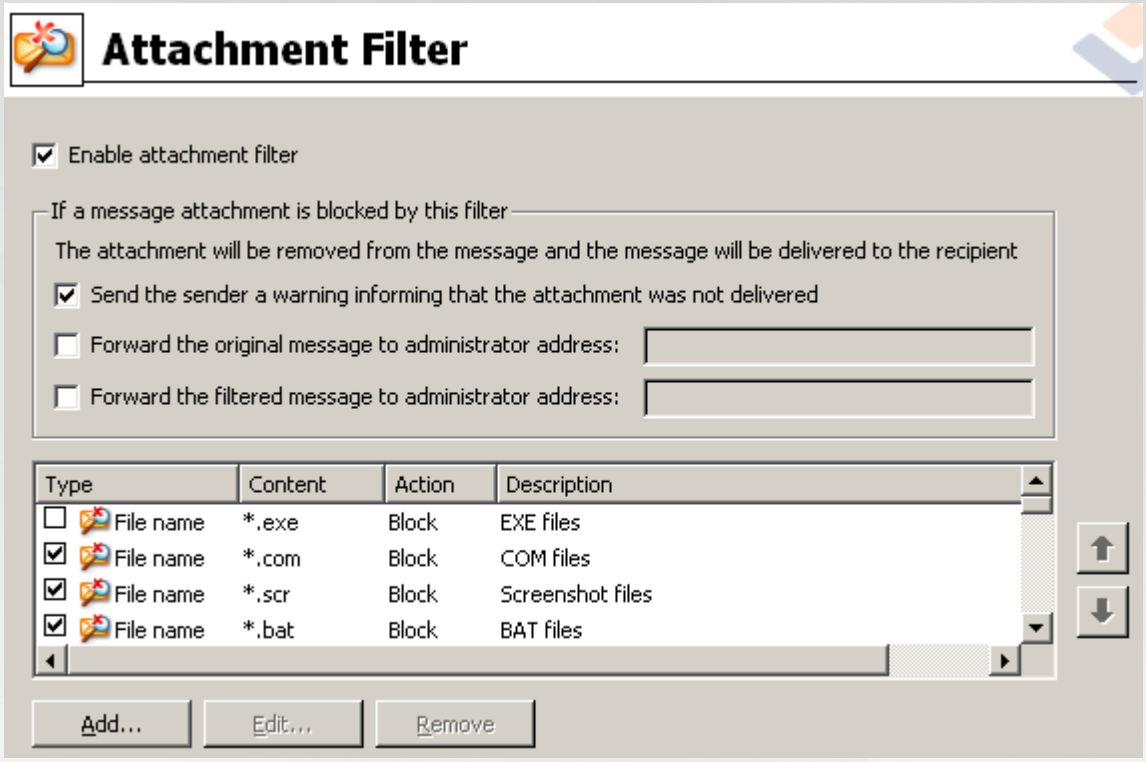
This frame specifies the action to be taken when part of the message or attachment cannot be scanned:

  - ***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.

7.1.2. Attachment Filter

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



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 email 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 (an action will be performed as defined above the list of disabled attachments).

- ***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:

- 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. 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 http://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***.