

Avira AntiVir Exchange

User Manual



Contents

1 Quickstart	5
1.1 Installation on an Exchange server	5
1.2 Starting the AntiVir Exchange Management Console	5
1.3 Configuration in the AntiVir Exchange Management Console	6
1.3.1 Necessary steps in the basic configuration	6
1.3.2 Necessary steps in the policy configuration	6
1.3.3 Recommended steps in the basic configuration	7
1.3.4 Virus scan of the Exchange databases	7
1.4 Observing data in AntiVir Monitor	7
2 Installation	8
2.1 System requirements	8
2.2 Installation of Avira AntiVir Exchange on an Exchange server	8
2.3 Uninstalling Avira AntiVir Exchange	13
3 Technical description	14
3.1 The Avira AntiVir Exchange Server	14
3.1.1 The transport agent	15
3.1.2 The Avira AntiVir Exchange Service = Enterprise Message Handler (EMH)	15
3.1.3 The Avira AntiVir Exchange quarantine	15
3.1.4 The Active Directory/LDIF	16
3.1.5 Compressed files/archives: The Avira AntiVir Exchange unpacker	17
3.2 The Avira AntiVir Exchange configuration	17
4 Details on the Avira AntiVir Exchange Management Console	19
4.1 The toolbar	19
4.2 Meaning of icons	20
4.3 Basic configuration	22
4.3.1 Overview with configuration reports	22
4.3.2 Importing a configuration	23
4.3.3 AntiVir Server settings	23
4.3.4 Settings for an individual AntiVir Server	27
4.3.5 Address lists	32
4.3.6 Report templates	38
4.3.7 Creating a database connection to an SQL server	44
4.3.8 Folder settings	49
4.3.9 Utility settings	57
4.4 Policy configuration	58
4.4.1 Example of a company policy	58

4.4.2	Conditions	58
4.4.3	Job types.....	59
4.4.4	Actions.....	60
4.4.5	Processing sequence of jobs	61
4.5	AntiVir Monitor	61
4.5.1	Quarantines	61
4.5.2	Avira AntiVir Exchange reports	69
5	AntiVir scan engine.....	70
5.1	Overview.....	70
5.1.1	Job types.....	70
5.2	AntiVir Scan	70
5.3	Information store scan.....	71
5.3.1	Status of the information store.....	72
5.3.2	Virus scan in the information store - sample job	75
5.4	Configuring and enabling the AntiVir Scan Engine.....	80
5.5	Activating virus scanning - sample job	83
5.5.1	General settings	83
5.5.2	Job is mission critical	84
5.5.3	Setting address conditions.....	85
5.5.4	Setting content conditions	85
5.5.5	Defining actions	85
5.5.6	Selecting servers.....	89
5.5.7	Entering details for the job	89
5.5.8	Saving the configuration.....	89
5.6	Virus scan of password-protected archives.....	90
5.6.1	Sample job.....	90
5.7	File restrictions for the attachment	91
5.7.1	By type	91
5.7.2	By email size.....	92
5.7.3	By attachment type and/or size	92
5.7.4	Configuring fingerprints.....	93
5.7.5	Blocking file attachments by type - Sample job	93
5.7.6	Restricting email size - sample job	97
5.7.7	Blocking attachments types and sizes - sample job	100
6	AntiVir Wall	105
6.1	Job types.....	105
6.2	Address check	105
6.2.1	Blocking senders or recipients - sample job	106
6.3	Content check with dictionaries	109
6.3.1	Setting up dictionaries.....	109
6.3.2	Checking and blocking text content - sample job	112

6.4 Limiting the number of recipients	116
6.4.1 Restricting the number of recipients - sample job.....	116
7 Anti-spam	119
7.1 Avira AntiSpam Engine	119
7.1.1 Configuring AntiSpam Engine	119
7.2 Wall spam filtering jobs	122
7.2.1 AntiSpam with Wall Spam Filtering jobs	122
7.2.2 Definite no-spam criteria.....	124
7.2.3 Definite spam criteria.....	125
7.2.4 Practical tips.....	126
7.3 Anti-spam for experts	126
7.3.1 Combined criteria - example	127
7.3.2 Combining the information on spam probability.....	128
7.3.3 AntiSpam scanning - Sample job	130
7.3.4 Configuring advanced spam filtering jobs	140
7.3.5 Manual AntiSpam configuration.....	141

1 Quickstart

The quick guide to Avira AntiVir Exchange:

- [Installation on an Exchange server](#)
- [Starting the AntiVir Exchange Management Console](#)
- [Configuration in the AntiVir Exchange Management Console](#)
- [Observing data in AntiVir Monitor](#)

1.1 Installation on an Exchange server

1. To install Avira AntiVir Exchange, double-click the installation file:
 - For Microsoft Exchange 2003: *avira_antivir_exchange_2k_32bit.exe*
 - For Microsoft Exchange 2007/2010 (64-bit):
avira_antivir_exchange_2k7_64bit.exe
2. Follow the rest of the instructions in the setup until the installation is completed.
If you do not specify another installation directory, Avira AntiVir Exchange is installed in the following default directory:
C:\Programme\Avira\AntiVir Exchange\ (German)
C:\Program Files\Avira\AntiVir Exchange\ (English)
 or
C:\Programme(x86)\Avira\AntiVir Exchange\ (German)
C:\Program Files(x86)\Avira\AntiVir Exchange\ (English)
 for 64-bit versions

Warning: You must disable any real-time or on-access scan functions of the virus scanners used for the directory ... \Avira\AntiVir Exchange\AntiVirData\

1.2 Starting the AntiVir Exchange Management Console

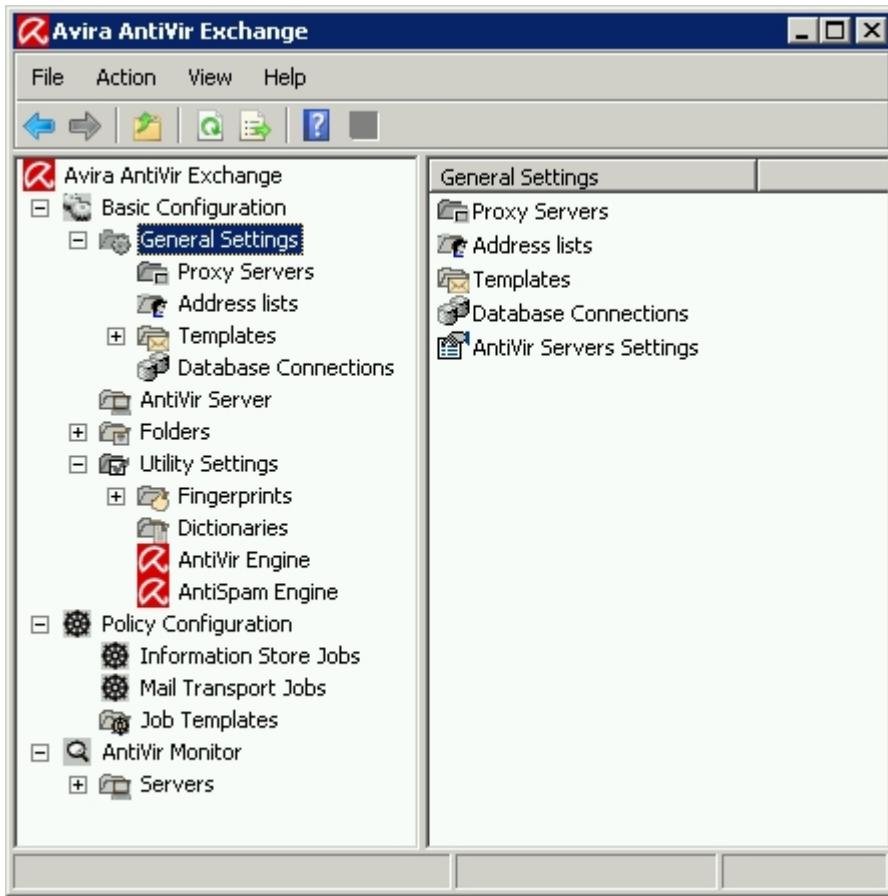
Avira AntiVir Exchange is a server product that is configured using the AntiVir Exchange Management Console. For Avira AntiVir Exchange to work, the AntiVir for Exchange service must be started. See also [The Avira AntiVir Exchange Service = Enterprise Message Handler \(EMH\)](#)

You start the console via **Start - Programs - Avira - AntiVir Exchange - AntiVir Exchange Management Console**.

When you close the AntiVir Exchange Management Console, you will be asked if you want to save changes.

Note: Open changes are indicated by (*) at the uppermost node. If you want to save your changes to the configuration, click the **Save**  button. The configuration is saved in the *ConfigData.xml* file, which is stored in the *Avira\AntiVir Exchange\Config* directory.

1.3 Configuration in the AntiVir Exchange Management Console



After the installation, make the settings described below in the AntiVir Exchange Management Console.

1.3.1 Necessary steps in the basic configuration

In the **Basic Configuration**, you define the valid servers, email addresses, common templates and utility settings.

Select **Basic Configuration - General Settings - AntiVir Server settings** on the **Email addresses** tab to check the entries for the *Administrators* and the *Internal domains*. See [AntiVir Server settings](#).

1.3.2 Necessary steps in the policy configuration

In the **Policy Configuration**, you define and enable the required jobs in accordance with your company's policies. In other words, jobs are no more than rule-based measures or actions that are applied to the mail traffic.

Carry out the following steps to create a new job:

1. Find the required template in **Job templates**.
2. Select the template and drag it into the **Mail Transport Jobs** folder. Configure the name and the properties of this job and enable the job under Properties. (*Active: Yes*)

-
3. Note the sequence in which the jobs are processed (see [Processing sequence of jobs](#)).
 4. **Save** your changes. See also [Starting the AntiVir Exchange Management Console](#).

It is important to distinguish between two categories of jobs.

Jobs for the AntiVir Scan Engine that scan for viruses, malware or malicious scripts or that filter emails according to size and/or type of file attachment and jobs for the AntiVir Wall that can be used to filter emails according to a number of criteria (e.g. addresses, words, images).

1.3.3 Recommended steps in the basic configuration

It is recommended that you make individual settings for address lists, templates, etc. in the basic configuration. These settings are, however, not mandatory for a test operation.

1. Configure the **Address lists** (for the selection in the job rules) under **General Settings**.
2. If required, change the standard templates under **General Settings**.
3. In **Utility Settings**, configure the required accessories such as word lists, fingerprints and virus scanners.

1.3.4 Virus scan of the Exchange databases

In **Policy Configuration - Information Store Jobs**, you can make the corresponding settings for each AntiVir server individually.

You cannot create information store jobs yourself. When you add a new server, a corresponding information store job is automatically available.

When you remove the server again, the information store job is also deleted.

For further information on information store jobs, see [Information store scan](#).

1.4 Observing data in AntiVir Monitor

After saving your settings, you can observe ongoing operations in Avira AntiVir Exchange with **AntiVir Monitor**.

AntiVir Monitor allows you to observe the latest "live data" and manage the **quarantines** of the configured servers, for example.

More information is available under [AntiVir Monitor](#)

2 Installation

Overview:

- [*System requirements*](#)
- [*Installation of Avira AntiVir Exchange on an Exchange server*](#)
- [*Uninstalling Avira AntiVir Exchange*](#)

2.1 System requirements

The following are the system requirements for installing Avira AntiVir Exchange:

- CD-ROM drive or network access
- RAM: Exchange recommended + additional 64 MB
- Hard drive: At least 400 MB for the installation
- Microsoft .NET Framework 2.x
- Operating systems (both 32-bit and 64-bit):
 - Windows Server 2003
 - Windows Server 2008
- Exchange server:
 - MS Exchange Server 2003
 - MS Exchange Server 2007 SP1 Update Rollup 4The following roles are supported:
 - Hub Transport Server
 - Mailbox Server
- MS Exchange Server 2010

Note: Please contact the support for information about the installation of clusters.

Warning: You must disable any real-time or on-access scan functions of the virus scanners used for the directory ... \Avira\AntiVir Exchange\AntiVirData\

2.2 Installation of Avira AntiVir Exchange on an Exchange server

1. To install Avira AntiVir Exchange, double-click the installation file, for example:
avira_antivirus_exchange_2k_32bit.exe

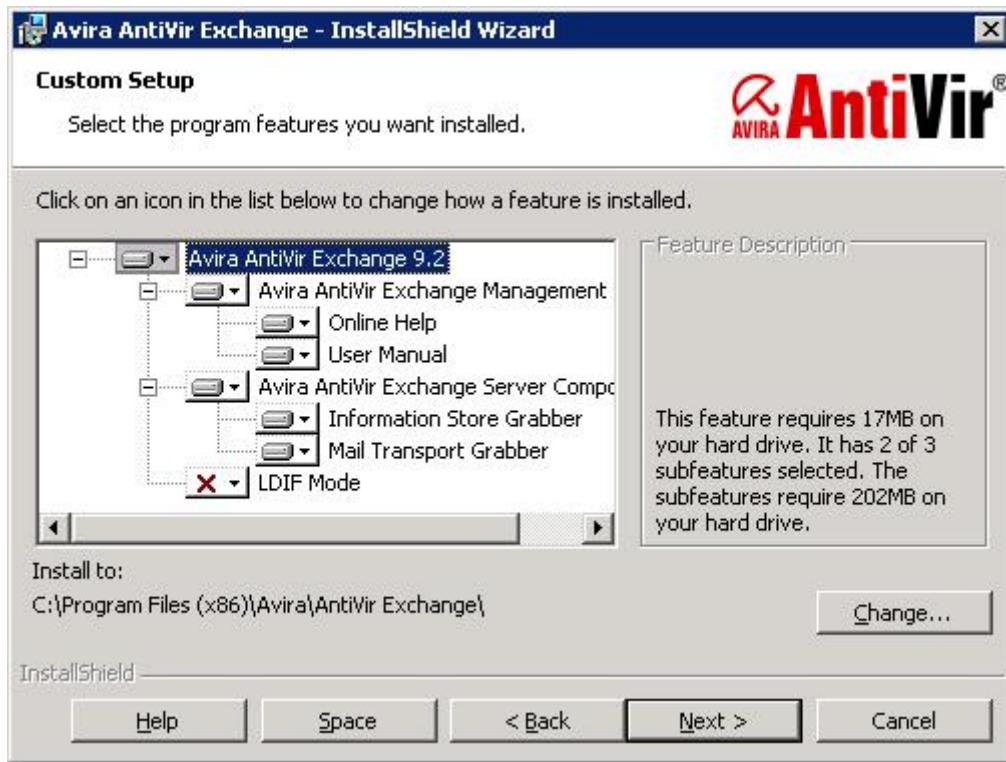
2. First select the **setup language**. Then select the platform and the language for the product.

The selected product language applies for the product interface and for the user notifications that are sent from Avira AntiVir Exchange to the users.



3. In the next dialog box, accept the *license agreement* to be able to continue and then click **Next**.

4. In the next dialog box, select the features that you want to install. When you make this selection, all server components and the AntiVir Exchange Management Console are installed.



If another active information store scan application apart from Avira AntiVir Exchange is located on the server, the information store scan function is disabled. If you want to use the information store scan, you first need to uninstall the other application.

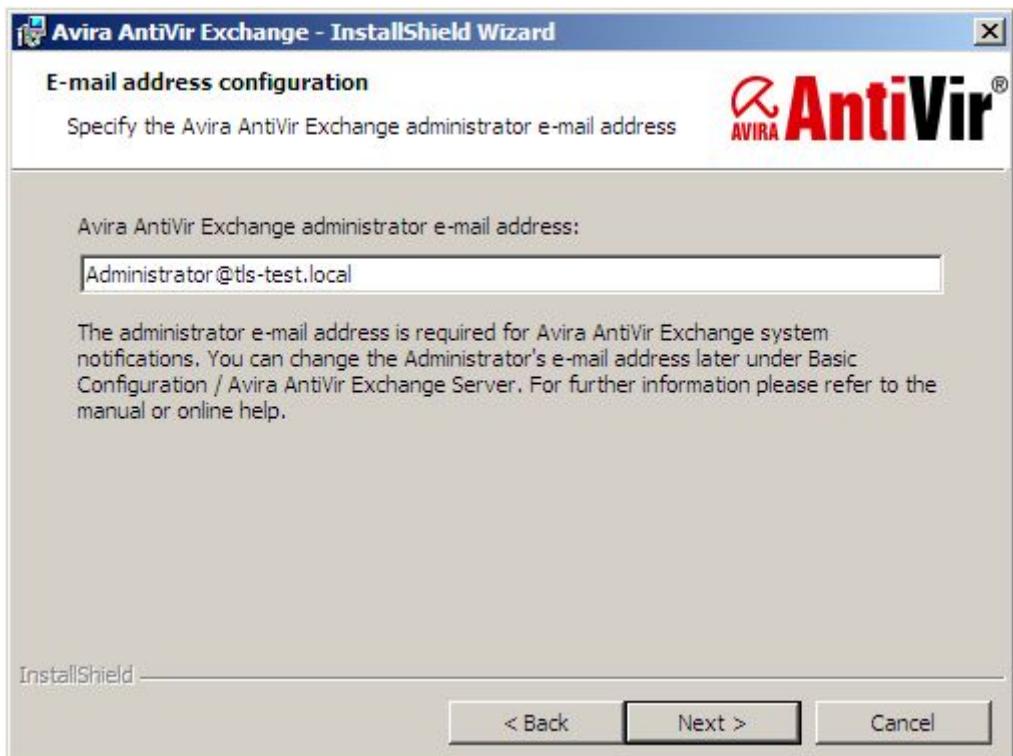
5. Click **Next**.

6. In the next dialog box, you are asked for the storage location of the configuration file.

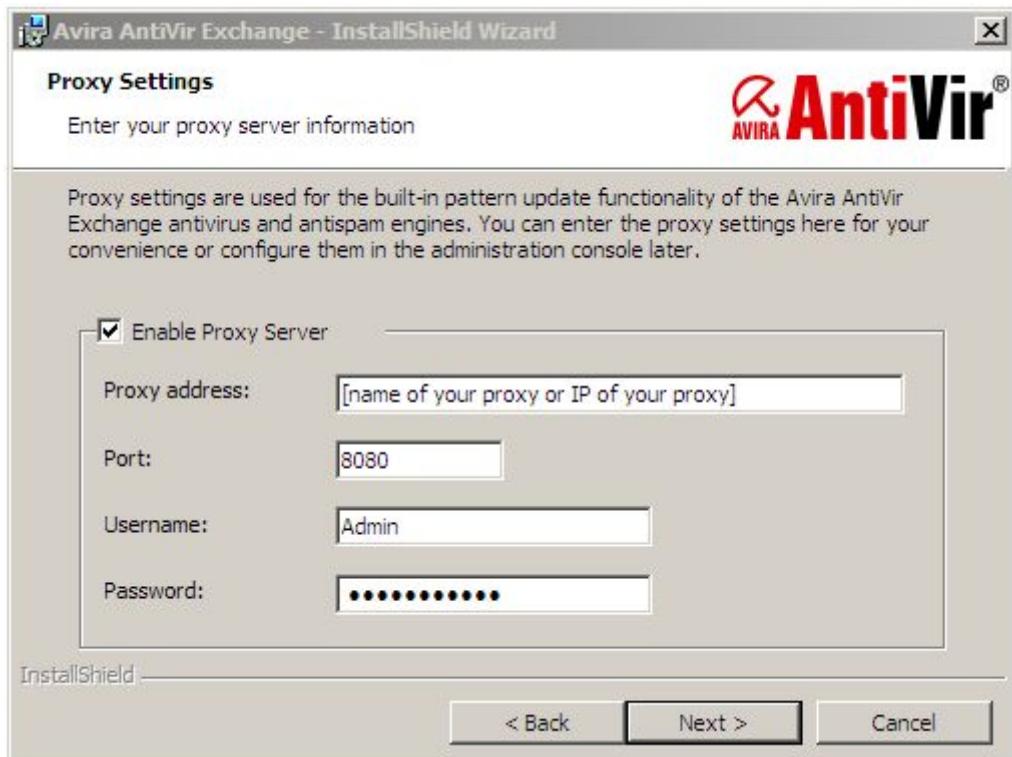


If you are not operating Avira AntiVir Exchange on multiple servers and you want to administer centrally with one configuration, confirm the default setting and click **Next**.

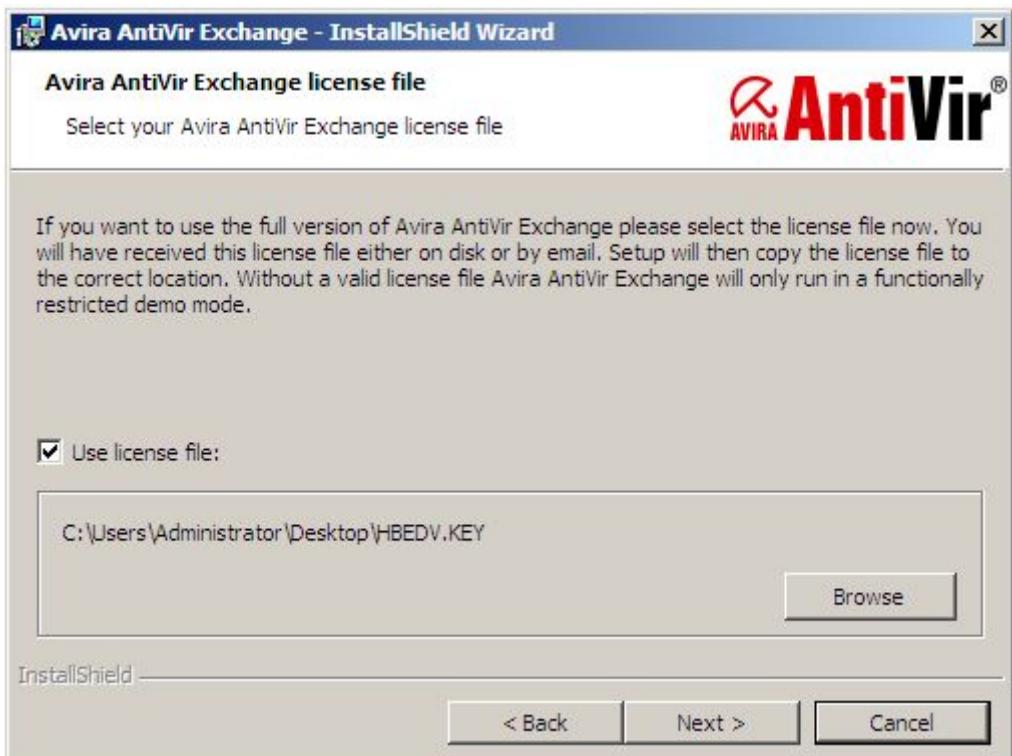
7. In the next dialog box, define the *email address of the administrator*.



8. If you are using a proxy server for the AntiVir update, check the box and enter the proxy settings for IP address, port, user and password. The password is stored in plain text.



9. In the next dialog box, you are asked for the license file.



Enable the **Use license file** option and use **Browse** to select the path for the license file.

10. You then receive a summary of your settings.



11. Now disable the on-access scanner for the directory ... \AntiVirData if you have not already done so.
12. Check your configuration settings.
These settings are accepted as the default settings in the configuration of the Avira AntiVir Exchange Server. For more information, see [AntiVir Exchange Server Settings](#).
13. Follow the rest of the instructions and click Install.
Avira AntiVir Exchange is then installed in the following directory:
<Drive>:\<Default program directory>\Avira\AntiVir Exchange\
14. When you click **Finish** in the last dialog box, Avira AntiVir Exchange is successfully installed.

The AntiVir virus scanner is completely configured and can be used straightaway. For this purpose, we provide a job for the virus scan with AntiVir, which you can simply enable.

See also [Configuring and enabling the AntiVir Scan Engine](#).

Warning: You must disable any real-time or on-access scan functions of the virus scanners used for the directory ... \Avira\AntiVir Exchange\AntiVirData\

2.3 Uninstalling Avira AntiVir Exchange

1. Click **Start - Control Panel - Programs and Features**
2. Select **Avira AntiVir Exchange**
3. Click **Next**. The setup will be launched and will uninstall Avira AntiVir Exchange.

3 Technical description

Avira AntiVir Exchange is divided into three main components:

- [The Avira AntiVir Exchange Console](#)
- [The Avira AntiVir Exchange Server](#)
- [The Avira AntiVir Exchange Configuration](#)

The Avira AntiVir Exchange Console is the user interface for configuring and administering Avira AntiVir Exchange. This is a so-called "snap-in" for the MMC.

The Avira AntiVir Exchange Console can be used to administer individual Exchange servers with Avira AntiVir Exchange installed or entire "Avira AntiVir Exchange server farms". This makes daily administration much easier, particularly in a multi-server environment.

The Avira AntiVir Exchange Console gives the administrator access to all the necessary configuration information and to the AntiVir Monitor (which includes an overview of quarantines) of the Avira AntiVir Exchange Servers. Two different access methods are used for configuration purposes and to access the quarantines.

1. Standard Windows file access
Windows data access is required in order to access the Avira AntiVir Exchange configuration, for example to administer security settings. The Avira AntiVir Exchange configuration may be available locally.
2. SOAP and SSL
The [AntiVir Monitor](#) is accessed via SOAP and SSL. A defined communication port is used for communication purposes.

The Avira AntiVir Exchange Console supports two modes:

1. Local administration
Here the Avira AntiVir Exchange Console is run directly on the Exchange server on which all the Avira AntiVir Exchange components have been installed. This mode is suitable for smaller environments and administration takes place on the local server.
2. Remote administration
In this case the Avira AntiVir Exchange Console is not run on the Exchange server, but is installed on a client instead.

The Avira AntiVir Exchange Console runs on the following operating systems:

- Windows 2003
- Windows XP Professional
- Windows 2008
- Windows Vista
- Windows 7

The remote administration option is suitable for central administration in multi-server environments. The Avira AntiVir Exchange Console uses one or more Exchange servers to configure and administer Avira AntiVir Exchange.

3.1 The Avira AntiVir Exchange Server

Avira AntiVir Exchange Server is the term used to refer to the Avira AntiVir Exchange functions and processes that run solely on the Exchange server.

The Avira AntiVir Exchange Server can be installed both in simple environments and in front-end/back-end environments.

The Avira AntiVir Exchange Server is in turn divided into a number of different areas.

3.1.1 The transport agent

The transport agent is a process that ensures that all emails, schedule queries, etc. sent, received or routed by the Exchange server are "intercepted" (or grabbed).

The SMTP transport protocol is used for all transport involving emails, schedule requests, etc. The "MS SMTP Transport Stack" is part of the SMTP transport protocol. This transport stack is used to route all email traffic. It doesn't matter whether these are emails that are sent between mailboxes on the same mailbox or incoming and outgoing emails.

In every case, email must pass through the transport stack. The transport agent is "linked" to this transport stack. As a registered event sink, the transport agent monitors the email traffic and routes all relevant information to the Avira AntiVir Exchange Service – the second component of the Avira AntiVir Exchange Server. The email remains active until all processing by the Avira AntiVir Exchange Server is successfully completed.

Note: Exchange-internal information, such as replication messages, are recognized as such by the transport agent and are left unchanged in the Exchange system.

3.1.2 The Avira AntiVir Exchange Service = Enterprise Message Handler (EMH)

The Avira AntiVir Exchange Service is always started as a Windows service and accepts all information from the transport agent. All further processing by Avira AntiVir Exchange will be monitored and controlled by the Avira AntiVir Exchange Service from this point forward. If the Avira AntiVir Exchange Service is stopped, the security functions of Avira AntiVir Exchange are disabled.

The Avira AntiVir Exchange Service can access all the necessary information:

- The configured Avira AntiVir Exchange jobs
- The installed Avira AntiVir Exchange license
- The Active Directory
- The Avira AntiVir Exchange quarantine

All of this information is now used for many purposes, for example to check the emails for viruses, identify spam emails and to place them in quarantine.

After processing, the Avira AntiVir Exchange Service returns the emails to the SMTP server.

3.1.3 The Avira AntiVir Exchange quarantine

One possible option is to stop infected emails or other undesirable emails on the server. This prevents these emails from reaching the relevant recipients. These emails are placed in the Avira AntiVir Exchange quarantine instead. A number of quarantines are available on each Avira AntiVir Exchange Server after installation. Additional quarantines can be created by the administrator.

An Avira AntiVir Exchange quarantine comprises

- A quarantine directory on the Exchange server (... \AntiVirData\Quarantine\Default Quarantine)
- The emails copied to quarantine.

- A quarantine database (*LocIdxDB.mdb*).

Avira AntiVir Exchange automatically generates an entry in the quarantine database for every email placed in quarantine. This database is a Microsoft Access file.

The following information is stored in this database:

- Email subject
- Date/Time
- Sender's email
- Recipient's email
- Sender's email (SMTP)
- Recipient's e-mail (SMTP)
- Short description of the restriction detected
- Email size
- Name of the Avira AntiVir Exchange job that placed this email in quarantine
- Name of the Exchange server
- Name of the email file
- Processing history

When an Avira AntiVir Exchange quarantine is displayed with the Avira AntiVir Exchange Console, the information from the quarantine database is displayed first.

When a quarantine entry is opened, more information is loaded from the email file.

Communication with the Avira AntiVir Exchange quarantine uses SOAP (Simple Object Access Protocol) + SSL (Secure Socket Layer). This applies both to direct "local" access to the server and to access from a remote Windows workstation. Port 8008 is the default communication port. This port can be changed in the Avira AntiVir Exchange Console (**AntiVir Server** node). If this port is changed for the server, this change must also be adapted to all accessing Avira AntiVir Exchange Consoles. All computers must use the same port. SSL is used to encrypt the SOAP communication channel. All the necessary components are provided during installation.

3.1.4 The Active Directory/LDIF

Avira AntiVir Exchange does not make any changes or additions to the Active Directory (AD). However, information from the Active Directory is read out at various points by Avira AntiVir Exchange.

When starting, the Avira AntiVir Exchange Service determines which Global Catalog server is available. This is used when determining addresses from distribution lists during email processing, for example.

The Avira AntiVir Exchange Console uses the Active Directory when selecting sender/ recipient conditions.

If there is no Active Directory available because, for example, the relevant ports are not open, then it is possible to work with an LDIF file. This can be generated by means of an LDAP export from an Active Directory, Exchange user directory or Notes Name and Addressbook (NAB).

3.1.5 Compressed files/archives: The Avira AntiVir Exchange unpacker

Files are often compressed when sent by email. To ensure that the virus scan and all checks also work for archives, Avira AntiVir Exchange uses an unpacker to be able to check files within the archive. Avira AntiVir Exchange includes an unpacker which is automatically available after installation.

The unpacker supports the following archive formats:

- ACE
- CAB
- ZIP
- Selfextracting ZIP
- ARJ
- Selfextracting ARJ
- TAR
- GZIP
- TGZ (Tape archive)
- UUE (Executable compressed ASCII archive)
- LZH (LH ARC)
- RAR
- Selfextracting RAR
- Java Archive (.jar)
- BZIP2
- 7-ZIP

Note: It is possible for an archive itself to contain archives. These archives (recursively packed files) are unpacked to a depth of 5 as standard. All archives that exceed this limit are transferred to the Bad Mail area.

The default upper limit for an email including unpacked files is 300 MB. A limit like this is particularly important in so-called "ZIP of Death" attacks.

The unpacking depth and the size limit can be changed in the console under **Basic Configuration - AntiVir Server - Properties - General**.

3.2 The Avira AntiVir Exchange configuration

All the information required to run Avira AntiVir Exchange is stored in the Avira AntiVir Exchange configuration. The Avira AntiVir Exchange configuration is available in the form of an XML file (*ConfigData.xml*).

The *ConfigData.xml* file is similar in structure to a database. There are different entries for each configuration area. Because the configuration involves a single file, it is very easy to distribute and back up the configuration. When help is required with configuration problems, the *ConfigData.xml* can be sent to the Avira Support Team for analysis.

The configuration information required both by the Avira AntiVir Exchange Server and the Avira AntiVir Exchange Console. Among other things, the Avira AntiVir Exchange Server derives the data for the Avira AntiVir Exchange job to be run from this information. To be able to make changes to the configuration with the Avira AntiVir Exchange Console, access is also required to the *ConfigData.xml* file. The Avira AntiVir Exchange configuration information can be stored both in a local directory and on a network share. An entry in the registry defined which Avira AntiVir Exchange configuration is used by the Avira AntiVir Exchange Console or the Avira AntiVir Exchange Server. The path to the Avira AntiVir Exchange configuration can be specified in *C:\.....* format or as UNC path *\Servername\Share\ConfigData.xml*. If the specified Avira AntiVir Exchange configuration is unavailable, Avira AntiVir Exchange uses the so-called "Last-Known-Good" configuration. This is logged in the Windows event list.

The "Last-Known-Good" configuration is stored locally for each server and is always updated when changes have been made to the Avira AntiVir Exchange configuration and it is possible to access the "Last-Known-Good" configuration from the Avira AntiVir Exchange configuration.

Note: A parameter is available to allow a non-standard configuration to be opened with the console. For example, you could start the *Avira.msc* file with parameter *config* and the required configuration file as follows:

"C:\Programs\Avira\AntiVir Exchange\Avira.msc" config

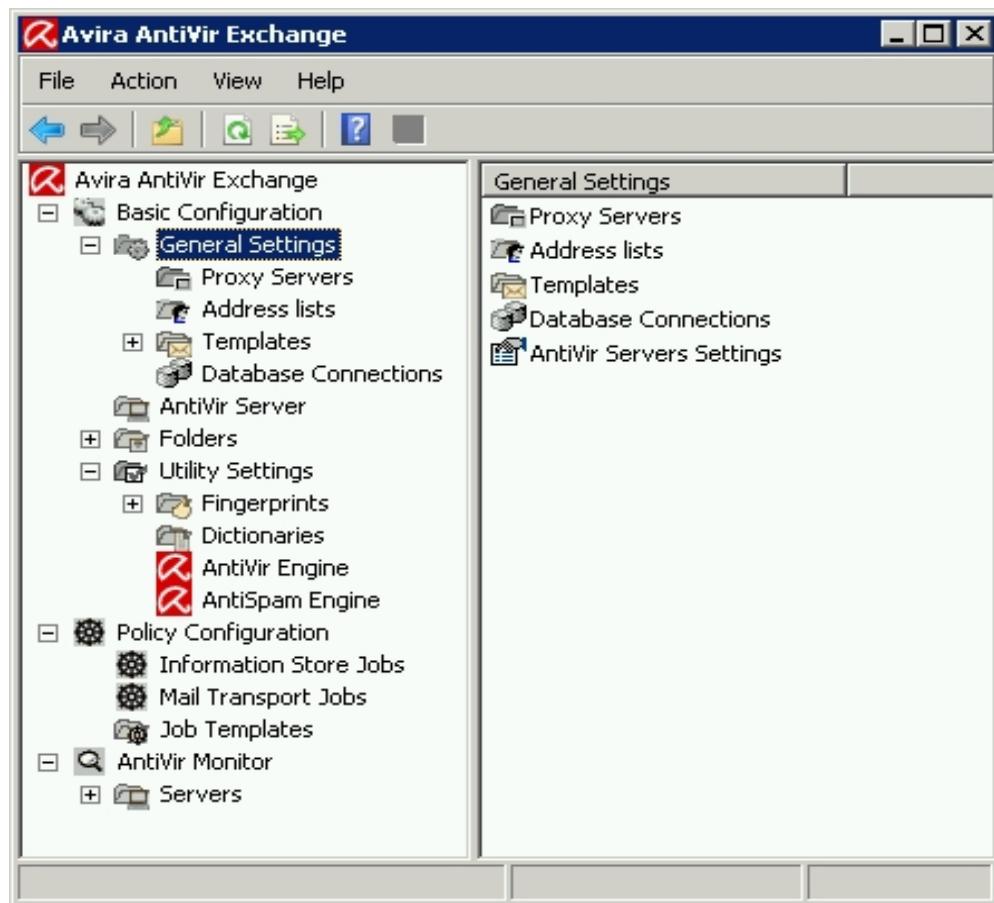
"C:\OtherFolder\Directory\ConfigData.xml"

You can also specify a UNC path here.

4 Details on the Avira AntiVir Exchange Management Console

1. Open the AntiVir Exchange Management Console
2. In the left hand column select the **Basic Configuration**, **Policy Configuration** or **AntiVir Monitor**.

The corresponding subfolders can be seen in the right hand window.



3. To launch **Online Help** click on in the toolbar or on **Show Help File** in the menu.

4.1 The toolbar

	Back
	Forwards
	Up one level
	Properties of the selected object
	Refresh

	Export list
	Help
	Save
	Increase position/order by one
	Decrease position/order by one
	Enable job
	Disable job
	New object
	Set filter in quarantine / bad mail

4.2 Meaning of icons

	Avira AntiVir Exchange Console start and logo
	Basic Configuration for the general settings of all modules.
	Node for General Settings
	The folder for the address lists
	A single Avira AntiVir Exchange address list (red collar), supplied with Avira AntiVir Exchange and cannot be changed.
	A single user-defined address list (yellow collar), can be created by the user and configured under Properties
	The folder for Sample notifications , containing the various samples for every job type and recipient.
	A single sample notifications , configurable under Properties
	The folder for the individual database connections .
	The icon for a single database connection , configurable under Properties .
	A list of all Avira AntiVir Exchange servers. Servers can be added, removed and configured. The shared properties for all servers are configured under General Settings - AntiVir Server Settings , or, alternatively, by right-clicking on AntiVir Server - Properties . These include the standard email addresses and internal domain(s)
	General AntiVir Server Settings under the General Settings node in the right-hand window.
	A single server, configurable under Properties .

	Folder Settings and Utility Settings. The quarantines are found under Folder Settings and all additional items to be configured, such as virus scanner, fingerprints and dictionaries, are found under Utility Settings.
	The quarantine folder structure. This contains all quarantine folders.
	A single quarantine folder, configurable under Properties .
	The folder for fingerprint groups.
	A logically related fingerprint group.
	A single fingerprint, configurable under Properties.
	The folder for the word lists used to filter content.
	A single dictionary, configurable under Properties.
	The AntiVir virus scanner, configurable under Properties.
	Policy configuration for configuring individual jobs based on your company's policies.
	Folder for sample jobs, containing the jobs for individual job types.
	An AntiVir job or AntiVir Wall job, which can have various job types, configurable under Properties.
	An active job, configurable under Properties.
	An inactive job, configurable under Properties.
	The AntiVir Monitor for viewing all quarantine folders on each available server. The quarantine folders contain the copies of the original emails, including the attachments.
	The quarantine folders with original mails for inspection. Detailed information can be retrieved for every email.
	A single quarantine item
	Invalid quarantine item
	Resent quarantine item
	Information store for quarantine item.
	Time and day of quarantine update
	Folder for different AntiVir reports delivered with Avira AntiVir Exchange.
	Individual AntiVir report.

The view of the Avira AntiVir Exchange Console comprises three areas:

- [Basic configuration](#)
- [Policy configuration](#)
- [AntiVir Exchange Monitor](#)

4.3 Basic configuration

The basic configuration is where general settings and the most important basic settings are made for the modules.

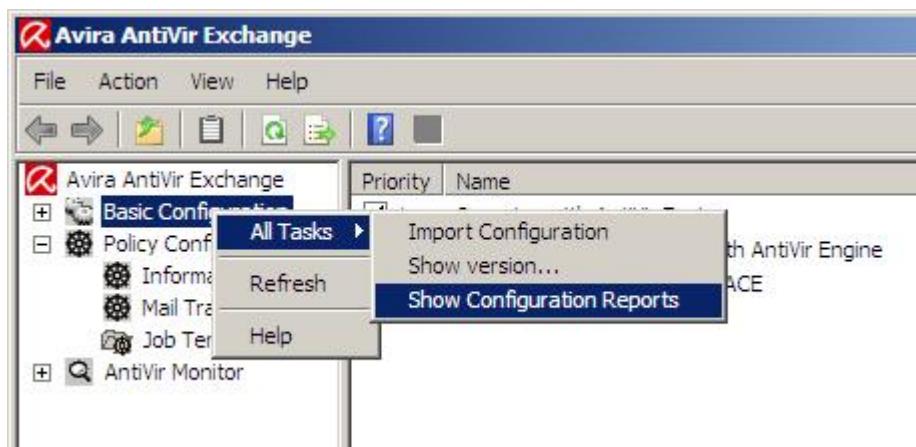
The basic configuration is used to manage:

- General settings, such as:
 - Proxy server
 - Address lists
 - Notification templates (templates)
 - Database connections
 - AntiVir servers
- All folders (e.g. quarantine folders)
- and the utilities:
 - Word lists for the content check
 - Fingerprints for blocking attachments
 - AntiVir engine
 - AntiSpam engine

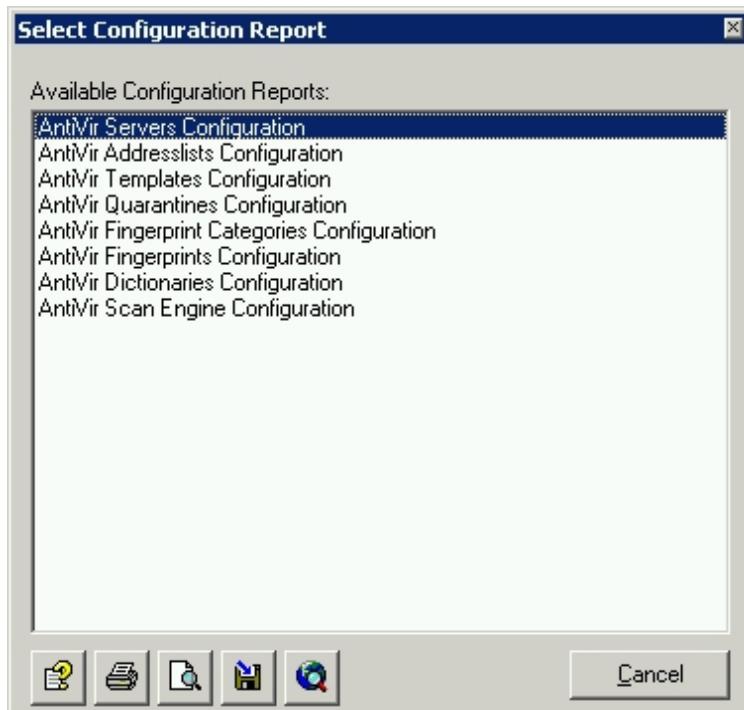
4.3.1 Overview with configuration reports

A configuration report provides an overview of the current configuration:

1. Right-click on *Basic Configuration* and select *All Tasks - Show Configuration Reports*.



2. Click the required report.



3. Click *Show report*. The report is then opened as a HTML file in the browser.
4. Click *Report preview* to display a print preview.
5. Click *Save report* to save the selected report as a HTML file.

4.3.2 Importing a configuration

Warning: Before changing an object in the basic configuration, it is recommended that you create a copy of the old object of the same name and rename it. The new version replaces the old one, which means that your own changes to the object are then lost.

If a modified version is available:

1. Select **Basic Configuration - All Tasks - Import Configuration** to reinstall all elements/objects such as word lists or fingerprints.
2. For this, select the corresponding XML file provided by Avira.

Warning: This function does not import the full configuration (ConfigData.xml) including the jobs, but instead imports only individual basis objects.

4.3.3 AntiVir Server settings

Under AntiVir Server Settings you can configure the default settings for all Avira AntiVir Exchange servers. Each server can also be configured on an individual basis. For more details see [Settings for an individual AntiVir server](#).

1. Select *Basic Configuration - General Settings*
2. Open *Properties*:
 - In the right-hand window click on *AntiVir Server Settings* and right-click to select *Properties*.

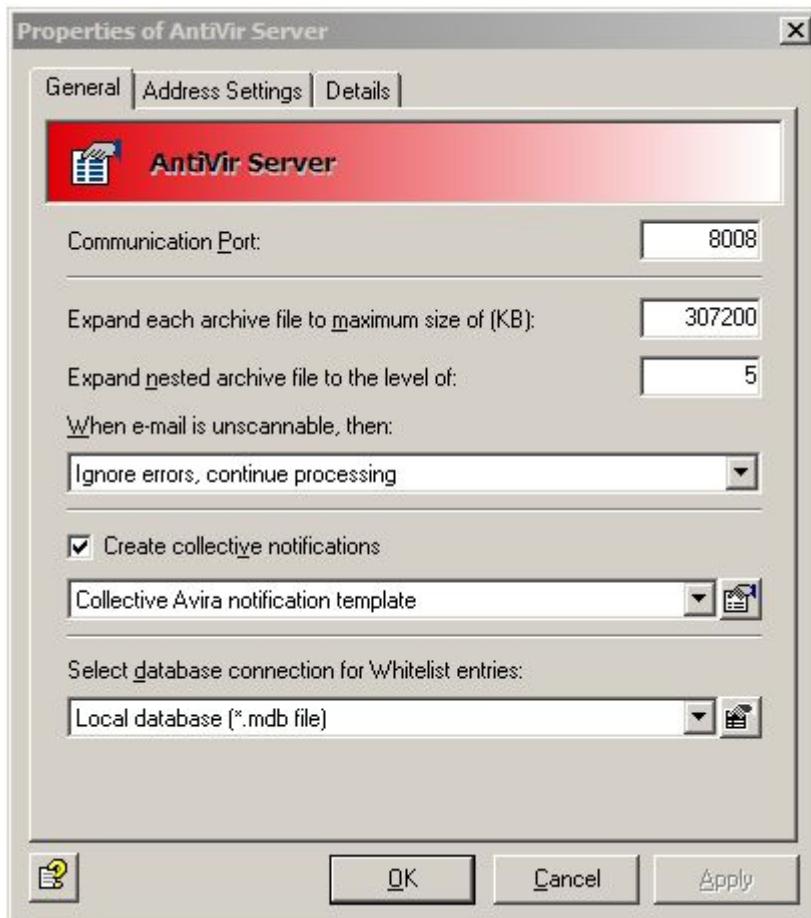
- Properties can also be opened by double-clicking on *AntiVir Server Settings*.
- Alternatively, you can access the properties in the left-hand window under *Basic Configuration* by right-clicking *AntiVir Server*.

Packed files and AntiVir Monitor

The settings on the *General* tab define the maximum permissible size for unpacked files on the hard disk and the maximum permissible unpacking depth for archives. Emails that exceed these values are transferred to the *Bad Mail* area.

Warning: Make sure that your communication port is set correctly for the AntiVir Monitor. Otherwise it will not be possible to communicate with the servers.

Port 8008 is used as the default during installation. The values entered here apply to all servers.



In this context you should also read the description of how to assign rights and make security settings under [AntiVir Monitor](#).

Unscannable elements

Unscannable elements, for example emails including encrypted attachments, can be subject to cross-server actions which are automatically performed when the program identifies an element as unscannable.

You can choose between two options from the drop-down. Either the fact that the email is unscannable can be ignored and the email is processed or the email is automatically moved to the bad mail directory.

Combined notification

Each job can generally be configured so that, when a particular event occurs, the recipients, senders and/or administrators are notified of this event (*Actions* tab in Job Properties).

If several of these events occur for a processed email, then the default setting for Avira AntiVir Exchange emails is that they do not send a separate notification for every event, but rather that all notifications are sent as a collective notification. This means that the recipients of this collective notification only receive one email that lists all incoming events.

The recipients of this *Collective Notification* only receive one email that lists all incoming events. Collective Notifications is used as the template in this case. You can modify this template or create new templates (with **Basic Configuration - General Settings - Templates - Collective Notifications**).

Note: If you suppress the sending of collective notifications and instead wish to send a separate email notification for every event that occurs, you should disable the *Create collective notifications* field under *General Settings - AntiVir Server Settings - General Tab*.

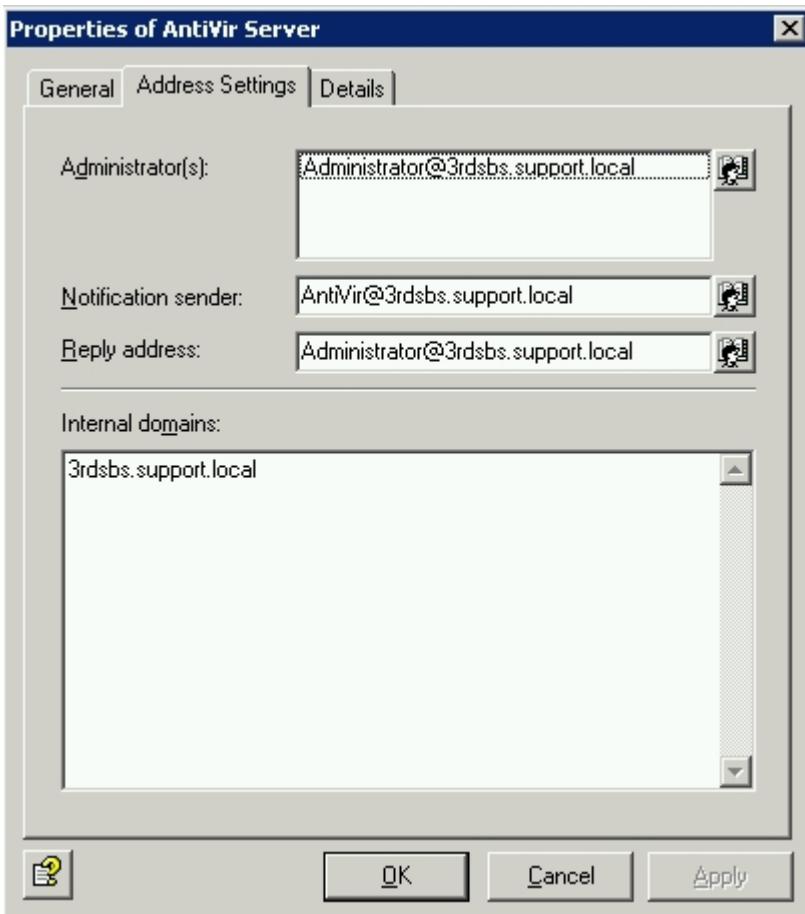
Central whitelist

In multi-email environments every participating server creates its own user whitelists. Without email synchronization, each user therefore receives a separate whitelist for each server and each whitelist has to be managed separately. To be able to manage these whitelists centrally, thus simplifying administration, instead of the regular local database based on Microsoft Jet-Engine, you can also set up a Microsoft SQL server to save the data for all participating Avira AntiVir Exchange servers in a central SQL database.

To create central user whitelists, you must first configure a database connection between the SQL server and the Avira AntiVir Exchange server (*Basic Configuration - Database Connections*). As soon as this connection is in place, select the relevant configuration in the *Database Connection for Whitelist Entries* field.

Defining email addresses and internal domains

Avira AntiVir Exchange requires a number of basic settings for the mail domain of the emails to be processed. During installation, the email address of the specified Avira AntiVir Exchange administrator is used to enter the following basic settings for Avira AntiVir Exchange:



- *Administrator(s)*: The Avira AntiVir Exchange administrator addresses entered here receive important status notifications from the Avira AntiVir Exchange installation and the configured administrator notifications. The installation enters the queried administrator address as the default.
- *Notification sender*: The sender displayed in Avira AntiVir Exchange notifications. The installation enters Avira AntiVir Exchange with the mail domain of the queried administrator address as the default.
- *Reply address*: The recipient of replies to these notifications in Avira AntiVir Exchange notifications. The installation enters the queried administrator address as the default.
- *Internal domains*: The mail domains specified here are seen as internal mail domains, while all others are considered external mail domains. This setting is used to differentiate between incoming and outgoing emails in the Avira AntiVir Exchange rules on the basis of the sender and recipient addresses of an email. For example, a spam filter job will only deal with incoming emails, while AntiVir should not be applied to outgoing emails.

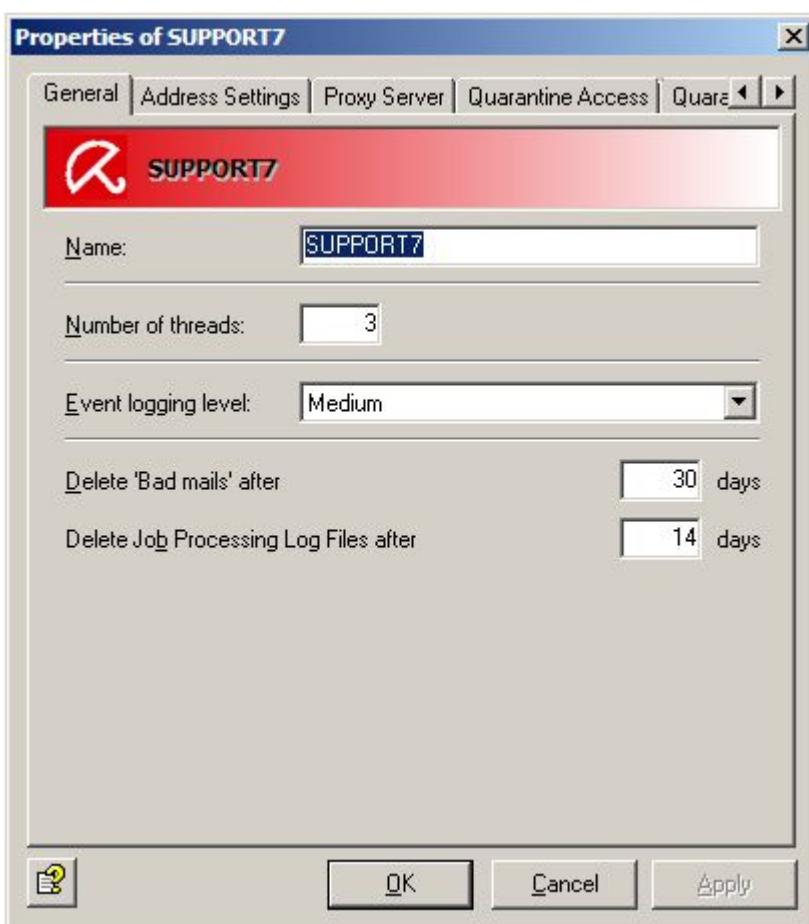
Multiple domains are separated with Return. Subdomains are automatically included if the main domain is preceded by the prefix "*." as a wildcard, e.g. *.domain.com. The installation enters the mail domain of the queried administrator address as the default.

These entries apply to all Avira AntiVir Exchange servers. The settings can be changed here at any time.

4.3.4 Settings for an individual AntiVir Server

Select **Basic Configuration**, click AntiVir Server in the left-hand window and select the required server in the right-hand window with a double-click. To create a new server, right-click on **AntiVir Server - New - AntiVir Server**. Right-click on **Properties** and configure the settings for the new server.

General server settings



1. Enter the **name** of the Exchange server.
The current Exchange server name is automatically entered during installation.
2. Define the maximum number of simultaneously processed emails in the **Number of Threads** field.
The number of emails that can be reasonably processed by AntiVir depends on the configuration and performance of your server.
3. Select the **log level for the event log** which can be viewed with the event viewer (Windows Event Log).
Levels range from **None** to **Maximum**.
4. Decide on the number of days for which the emails are to remain in Bad Mail quarantine.
The emails are automatically deleted after this number of days elapses.

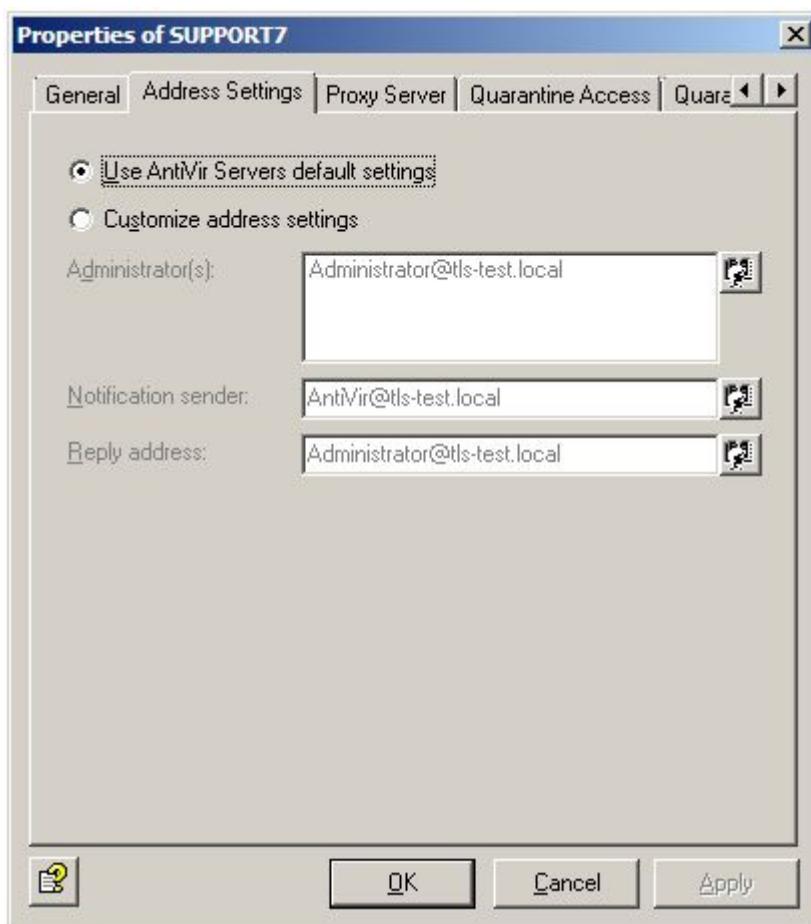
5. Define the number of days after which a job processing log is to be deleted in the Log folder.

Note: To be able to access a newly created server immediately in the AntiVir Monitor, update the view in the monitor (right-click on **AntiVir Monitor - Update**, or use the icon in the toolbar).

Individual email addresses for an AntiVir Server

The settings for each server are taken from the properties of all AntiVir Servers that are set automatically during installation or that have been entered individually by you. These settings are regarded as **AntiVir Server default settings**.

If you need individual settings for a server, enable the option **Customize address settings** and enter the addresses in the relevant fields.



Using proxy servers

If a proxy server is required in your network environment for Internet connections, you can select the appropriate proxy server for every AntiVir Server. For example for downloading updates from the Internet.

Click the **Proxy servers** tab.



If you wish to connect your AntiVir Server to a proxy server, select your user-defined appropriate proxy server from the list.

Proxy server settings

If you have already specified the connection data for the proxy server while installing Avira AntiVir Exchange, you will see these proxy server settings under **Basic Configuration - General Settings - Proxy Servers**.

Otherwise, you should enter the proxy server settings there:

- **Name/IP Address:** The full name or IP address of the proxy server.
Example 1: proxy.mydomain.de
Example 2: 127.0.0.1
- **Port:** Port number of the proxy server. The specified port is used to communicate with the proxy server.
Example: 8000
- **User and password** (optional): Authentication data under which the update service logs onto the proxy server.
Example: proxy_user

A proxy server is deleted by right-clicking and selecting **Delete**. Please note that you cannot delete a proxy server that is already in use by an object.

If the actions of the virus scanner and AntiSpam engine are to be executed by means of a proxy server, make the appropriate settings in the **proxy server** tab.

User-specific access to quarantine

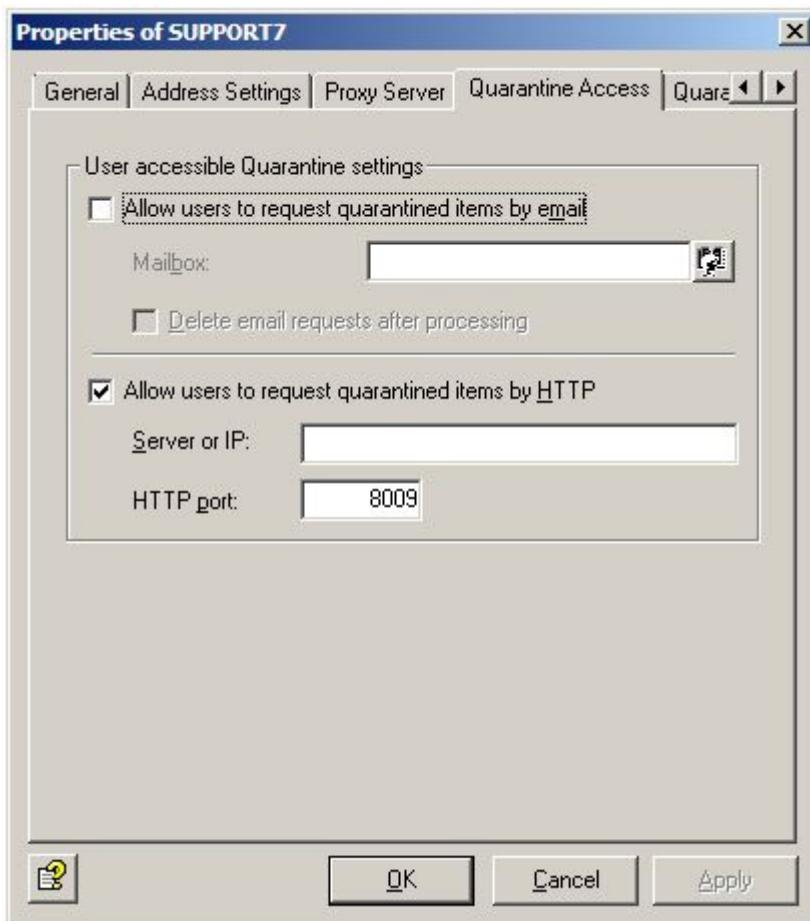
Avira AntiVir Exchange allows users to access their own quarantine emails.

Which emails are available and which users have access can be configured individually for each quarantine. This function is particularly interesting in relation to spam filtering, i.e. for spam quarantines. In addition, the administrator has less work to do because users can deliver the individual quarantine emails themselves.

They can define whether users are permitted to access their quarantine emails and which type of emails they can access for each individual server. The user receives a quarantine summary report containing information on quarantined emails and, by clicking on the appropriate action for the relevant email, thereby creating a request.

Individually configured for each quarantine, these actions are **Request** (deliver to recipients of the summary report), **Approve** (delivery to all recipients) and/or **Remove** (flag email for deletion in the quarantine). User access is by means of an email request or a HTTP request.

Click the Quarantine Access tab::



Allow users to request quarantined items by email: The quarantine request is initiated by means of an email request. If the user clicks on the action link for the required email in his quarantine summary report, the email request is automatically generated and sent to the email address you define in the **Mailbox** field on this tab.

This requires that the email address specified here should exist and that the email is sent via the server on which Avira AntiVir Exchange, and the corresponding quarantines, are installed.

We recommend that you set up the mailbox on the relevant server. The content of the email is read out, thereby performing the action required by the user. AntiVir recognizes request emails from users by:

1. the email address (specified in the **Mailbox** field)
2. the keyword for a user request in the email (User Request)

Finally, the request mail is placed in the specified mailbox.

Enable the **Delete email requests after processing** option if the request emails are to be deleted from the specified mailbox after processing.

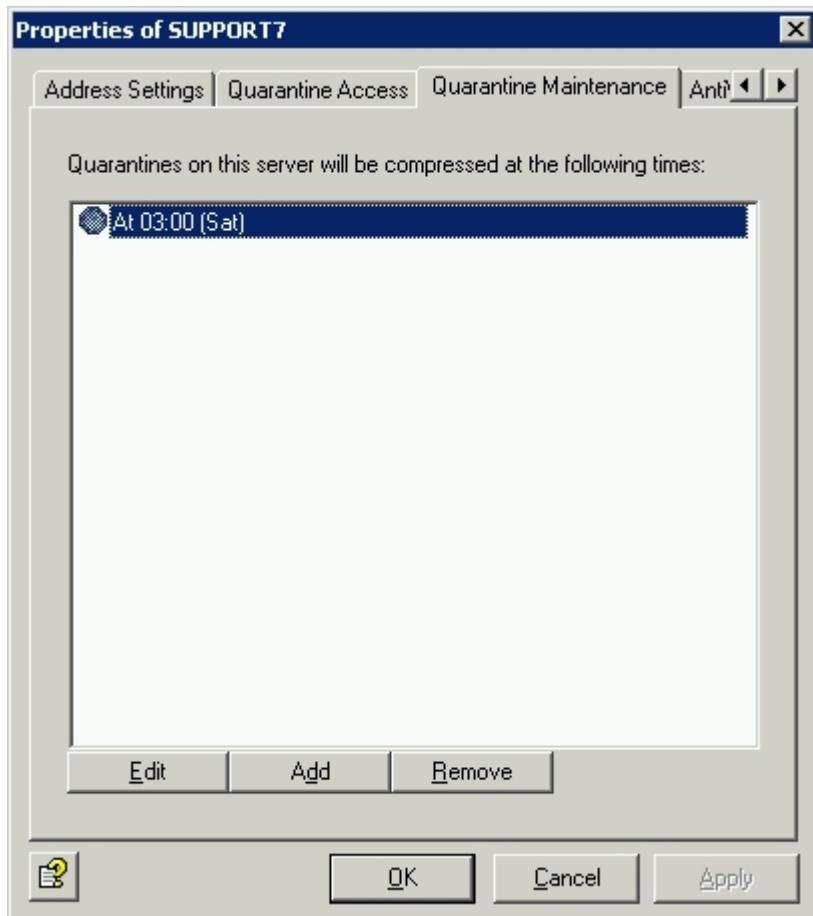
Allow users to request quarantined items by HTTP: The quarantine request is initiated by means of HTTP. The default browser opens as soon as the user has clicked the required action. The user receives a message indicating that his request is being processed. This request requires a free port. The standard entry is port 8009:

Warning: The response to users displayed by the browser is always the same (*OK_Response.html* in directory *AntiVir\App-Data*). The user will not be notified if the requested email no longer exists, because it has already been deleted in the quarantine for example.

Quarantine Maintenance

This tab is used to set the time at which the server quarantines are to be compressed. The compression involves physically deleting all emails marked for deletion and releasing the memory space again.

The default setting for compression is every Saturday at 3 a.m.. To change the time or frequency, click **Edit** and set the required times.



Note: You can also compress a quarantine manually if necessary by right-clicking on the relevant quarantine in AntiVir Monitor and selecting the **All Tasks - Compress Quarantine** command.

Viewing a list of all jobs

The **AntiVir Jobs** tab contains a list of all the jobs defined on this server.

To process a job on the server, call the job properties directly.

4.3.5 Address lists

You can create your own address lists which can be selected in the job in the **Basic Configuration - General Settings** under **Address Lists**. The available addresses can be found in the Active Directory.

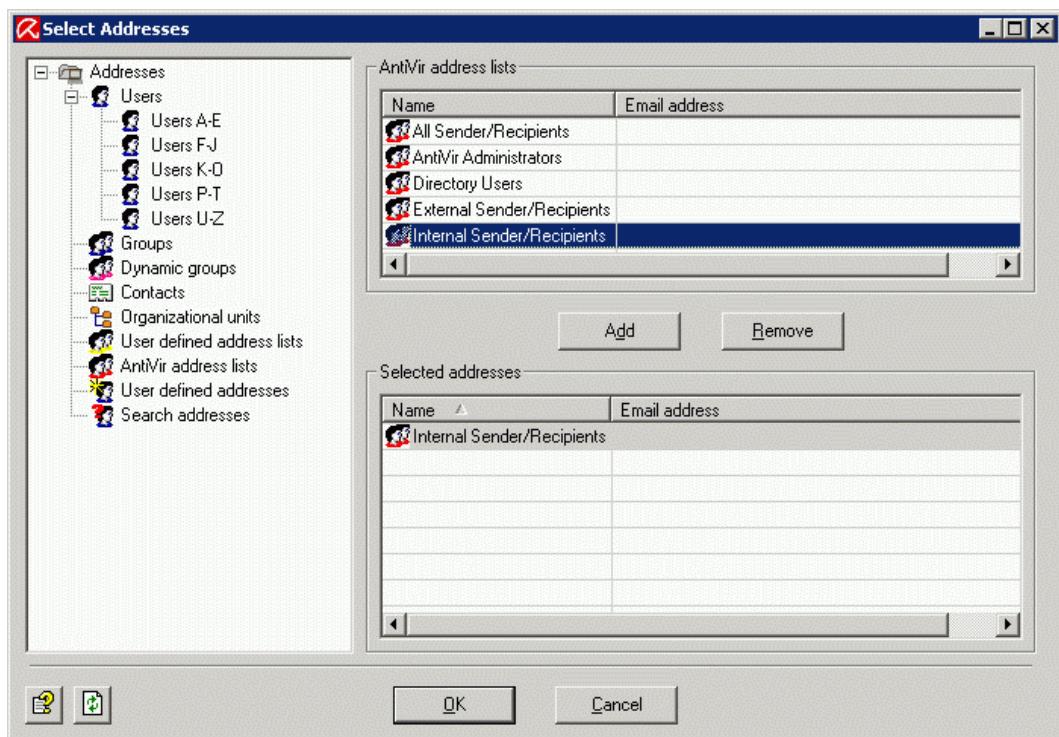
Creating, editing and deleting address lists

1. Open **Basic Configuration - General Settings**
2. Right-click **Address Lists** and select **New - Address List**.
3. Give the address list a mnemonic name.
4. Click on the **Select Addresses** icon: 
5. In the window that then opens, select the required addresses under the various headings with **Add**.

You can enter your own addresses in the input field and add these to the address list.

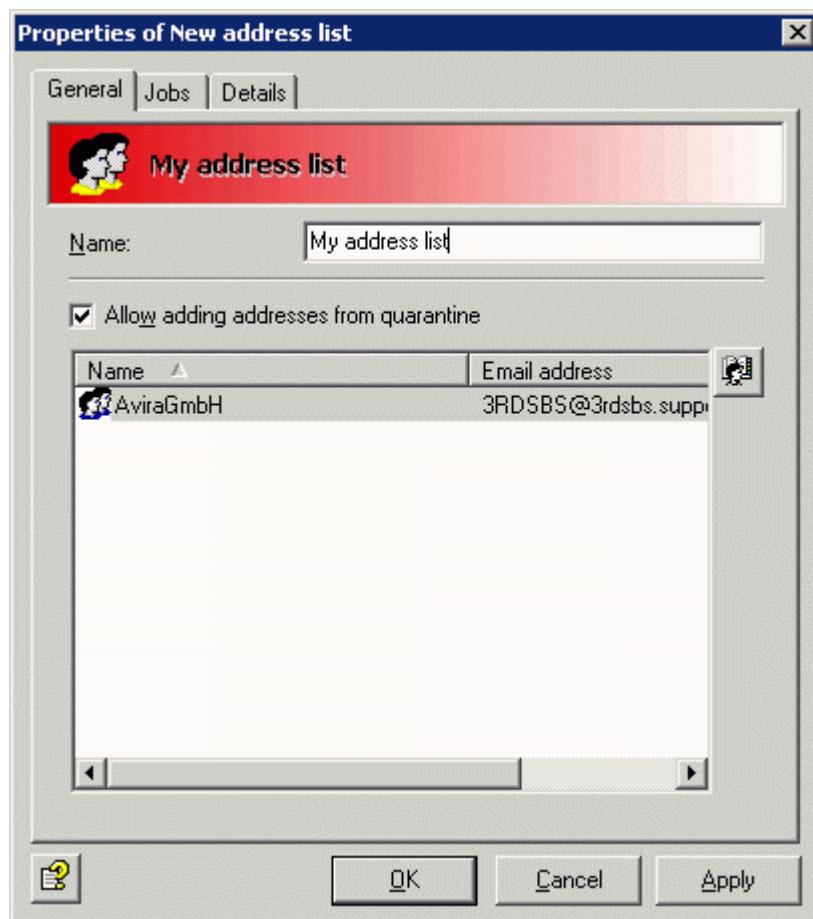
The * (asterisk) and ? (question mark) symbols can be used as wildcards. It is also possible to enter formally invalid email addresses, such as info@domain. Separate the various entries with a carriage return (Enter key).

If you have created an extensive list of your own addresses, you can run a text search in this list by clicking: . The text search function is also available in the dictionaries. To delete an entry from the list, mark it and click **Remove**.



6. Click **OK**.

Your address list should look something like this:



7. **Allow adding addresses from quarantine:**

This is where you decide whether direct access to this address list is to be permitted from a quarantined email. When you view a quarantined email in [AntiVir Monitor](#) you can use the **Add** button to add the sender address for the quarantined email to various address lists. The following address lists are released for direct access in the delivery default setting:

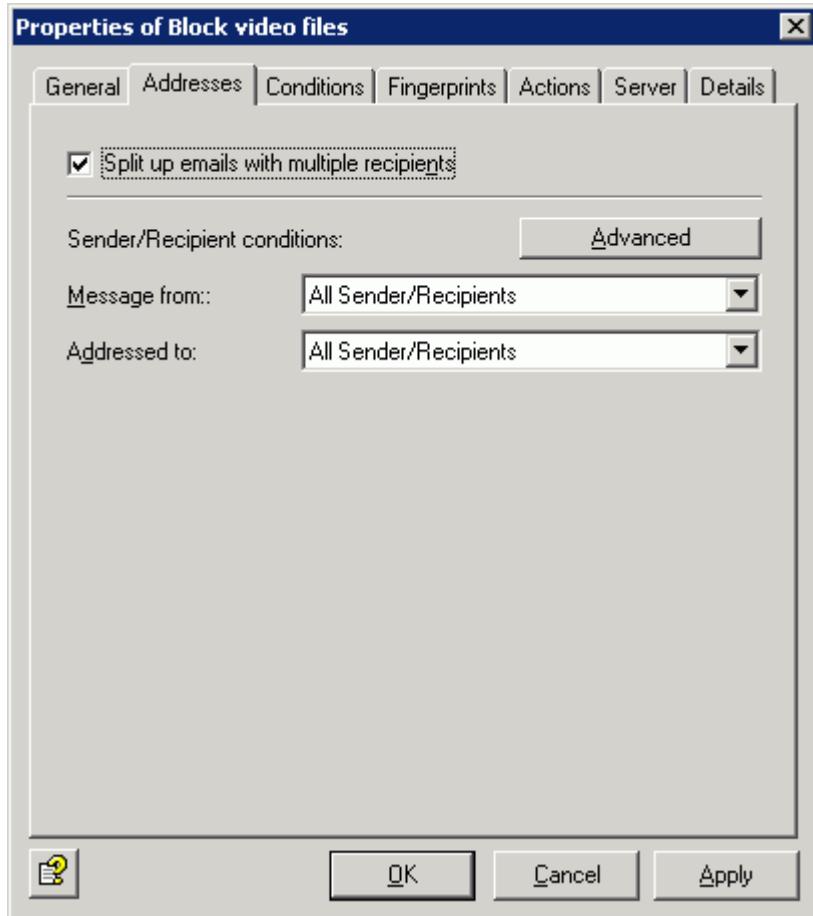
- Anti-Spam: Blacklist
- Anti-Spam: Newsletter Blacklist
- Anti-Spam: Newsletter Whitelist
- Anti-Spam: Whitelist

8. Click **OK** again.

9. To delete, mark the address list by right-clicking and select Delete from the context menu.

Usage and handling in a job

In each job you can use the Addresses tab to choose the users to whom the job is to apply. You can use the next tab to set the most common scenarios:



Here you can choose whether the job applies to all users or is to be restricted to internal or external users. You can make this choice for both senders and recipients.

Note: Both conditions in the **Message from** and **Addressed to** fields must apply if an action is to be triggered (AND link).

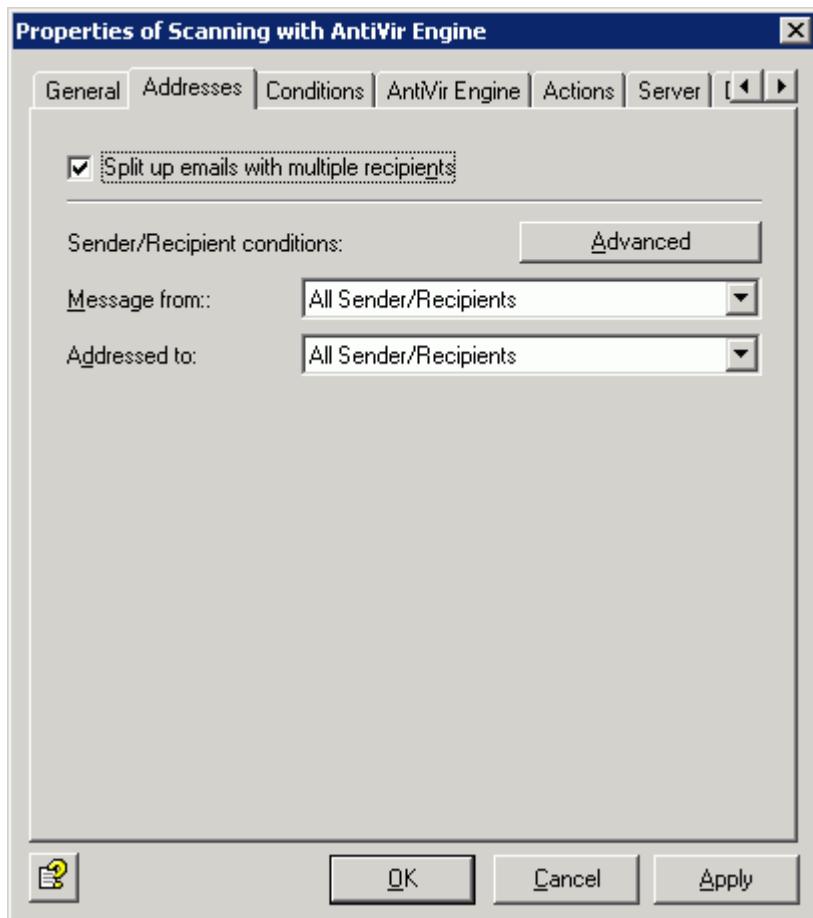
Split up emails with multiple recipients: When an email is addressed to several recipients and one or more of them is entered in a job in the address scan, this email is split into two emails: one email for the defined recipients of the address check and one for the non-defined recipients. The job then only processes the email with the recipients who are defined. Emails are not split up if you have not defined address scanning for recipients. The splitting of emails will impact on the performance of your server.

Scanning for viruses

Company policy: All emails are to be scanned for viruses. In this case it is not enough only to scan the emails from external senders. It is also necessary to ensure that no infected emails leave the company. The defined actions (scan for viruses, clean file if necessary and copy to quarantine) must be performed independently of the senders or recipients.

Implementation: Action will be taken at **Message from:** <All Senders/Recipients> and at **Addressed to:** <All Senders/Recipients>. There are no exceptions. Every email from every sender to every recipient is scanned for viruses.

This is how the address settings are displayed in the job:



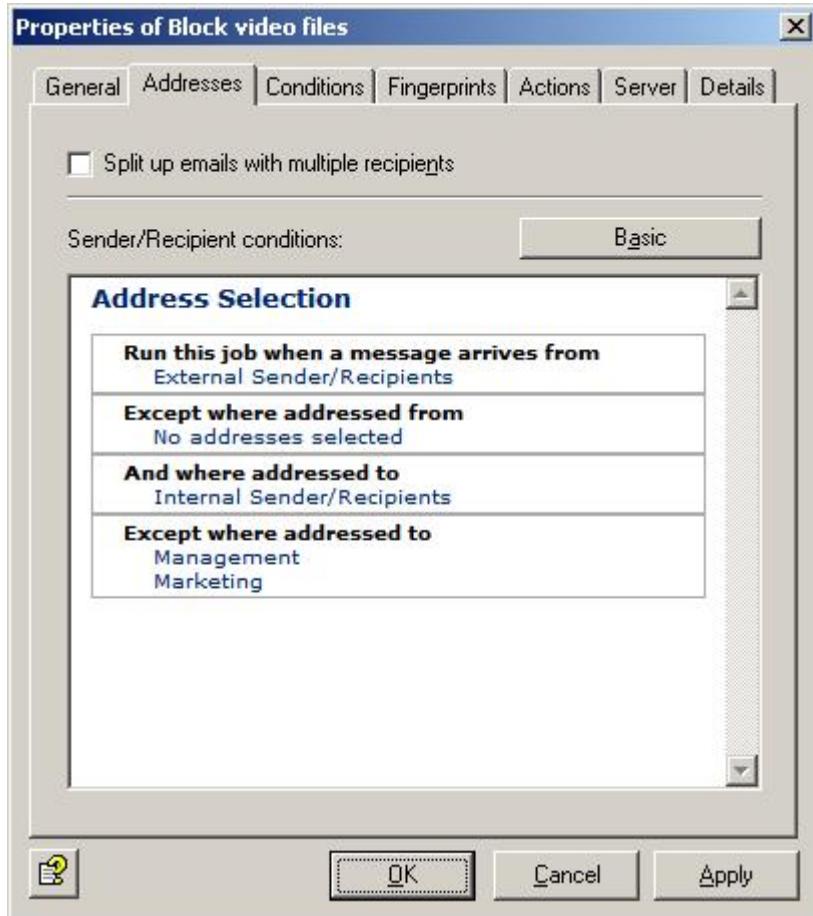
The advanced scan can be used to implement more complex company policies with ease. Click the **Advanced** button. Afterwards, click the **Basic** button to return to simple selection.

Here is an example of a job that blocks file attachments

Company policy: No emails containing video attachments are to be allowed to reach the company via the Internet. However, an exception to this rule is to be defined for the marketing department and for senior management.

- **Run this job when a message arrives from** checks the sender(s). The exception **Except where addressed from** also applies.
- and **where addressed to** scans the recipient(s). The exception **Except where addressed to** also applies.

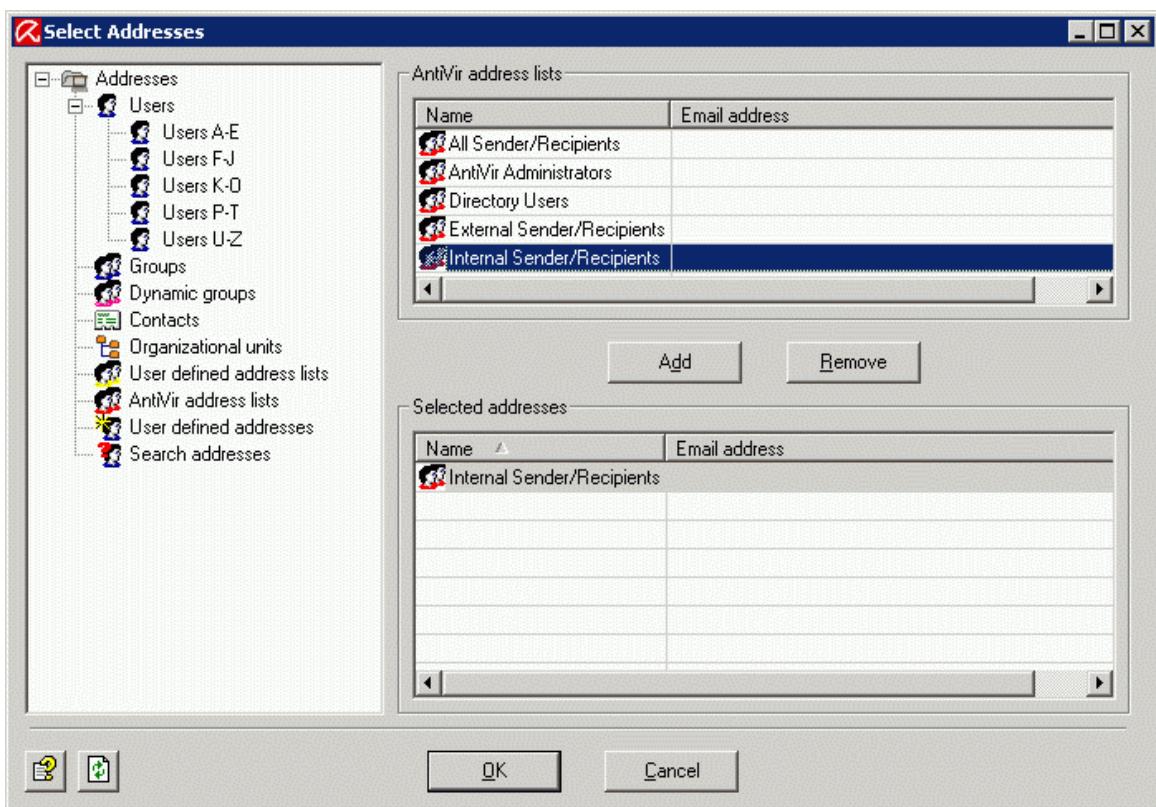
Implementation: The address settings in the job should look like this: The defined action in the job (in other words the blocking of attachments) will be executed under **Run this job when a message arrives from: <External Senders/Recipients>** and under **And where addressed to** is to be sent to **<Internal Senders/Recipients>**. Under **Except where addressed to** you should define an exception for the marketing departments and senior management that you have already entered as a group in the Active Directory (AD) or that you can create in a separate address list. This means that all video attachments sent by external senders to internal recipients will be intercepted unless the recipient is in the marketing department team or a member of senior management. This is how the address settings are displayed in the job:



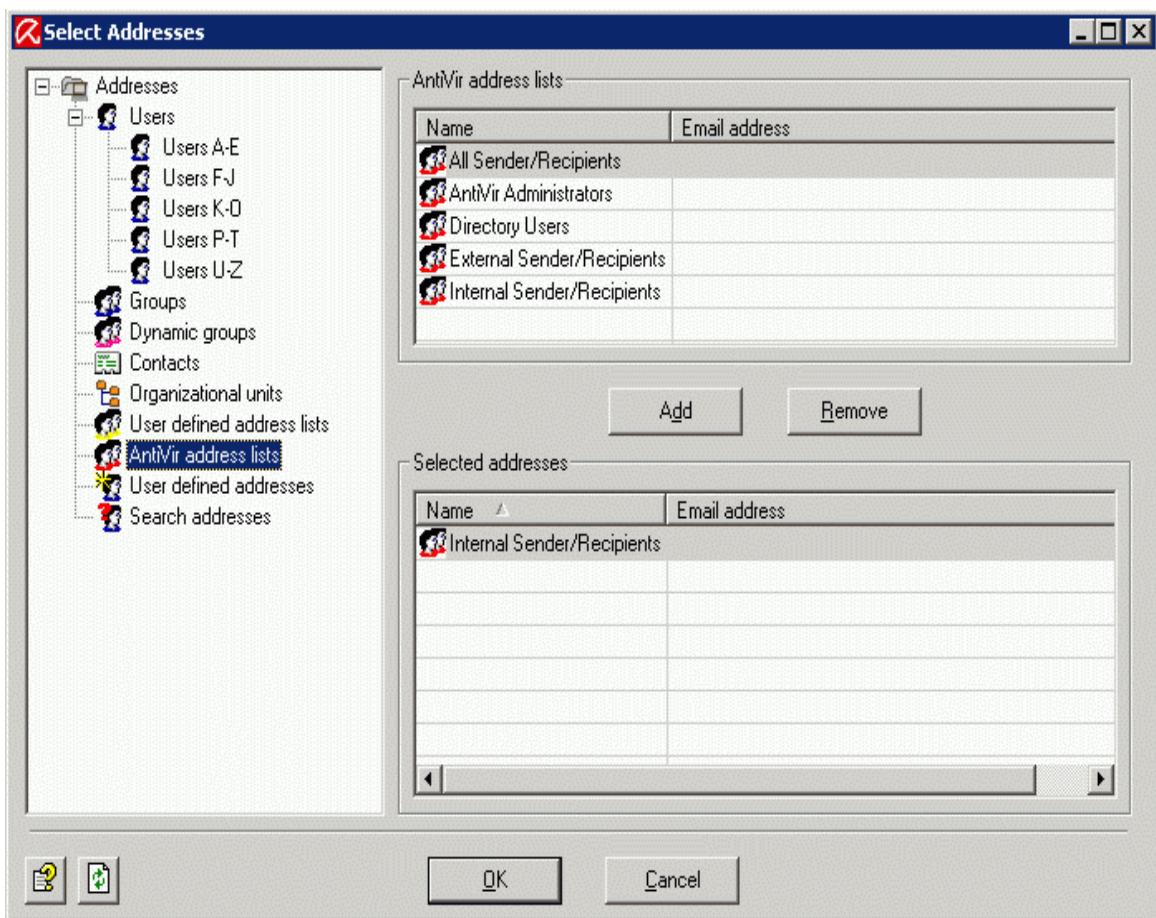
Note: All specified conditions in the **Run this job when a message arrives from** and **And where addressed to** fields must apply if an action is to be triggered (AND link). If several addresses are entered within the same condition (e.g. **And where addressed to**), only one needs to match for the action to be triggered. The exceptions (**Except where ...**) are of no relevance for the basic triggering of the action. Emails to or from these exception addresses are simply forwarded without the defined actions being executed.

Click **Internal Senders/Recipients, No Address Selected** or a corresponding entry in the exceptions to call up the address selection window and to define the addresses for this specific condition:

Details on the Avira AntiVir Exchange Management Console



The AntiVir address lists are also available:



Avira AntiVir Exchange address lists are fixed lists from which settings for the higher Avira AntiVir Exchange servers are generated that are requested and entered upon installation, or that you have configured manually. See [AntiVir Exchange Server Settings](#).

Note: **User defined address lists** and **AntiVir address lists** are only displayed when an address is selected for a job. **User defined address lists** can be changed anytime, **AntiVir address lists** cannot be changed.

4.3.6 Report templates

In every job you can decide under **Actions** who is to receive a report when Avira AntiVir Exchange detects a prohibited email.

When you create a new job, you can select the appropriate template for the job type. For more detailed information about the various job types see [Policy configuration](#).

The report templates for the various jobs (content check, virus scan, etc.) are created in the **Basic Configuration**.

Creating report templates

You will find preconfigured report templates for the various modules under **Basic Configuration - General Settings - Templates**.

1. Click Templates and select the template type.
2. Right-click on the required template in the right-hand window and select **Properties**.
3. Enter the subject.
4. Click on the **Notification text - Edit** tab for the text of the notification. You can change the layout of the text using the formatting menu bar; this information will then be converted internally into HTML commands. If you retrieve the source text with the  button, you can also enter HTML commands directly.
5. The **Jobs** tab shows the jobs in which the notification template is used.
6. Click **OK**.

List of notification variables

The following variables, which can also be entered directly with the arrow next to the  button, can be used in the notification texts and in the subject lines of the notifications. Please note that the tokens [VAR] and [/VAR] are case-sensitive and must always be written in uppercase form.

General

Category, variable type	Variable	Description
General: Sender	[VAR]Mailsender[/VAR]	Sender of the triggering email.
General: Sender (SMTP)	[VAR]From[/VAR]	Sender SMTP of the triggering email.
General: Subject	[VAR]Subject[/VAR]	Subject line of the triggering email.

Details on the Avira AntiVir Exchange Management Console

General: Date and Time	[VAR]Date[/VAR]	Date and time when the job triggered the action.
General: Date	[VAR]DateOnly[/VAR]	Date when the job triggered the action.
General: Recipient(s)	[VAR]Recipients[/VAR]	Recipients of the triggering email.
General: Job Name	[VAR]Jobname[/VAR]	Name of the job that started an action.
General: Invalid Recipients	[VAR]UnrestrictedRecipients[/VAR]	Recipients of the triggering email not defined in the address (input) conditions.
General: Quarantine folder	[VAR]Quarantine[/VAR]	The quarantine where an email has been placed.
General: ID of a Quarantine email	[VAR]QuarantineDocRef[/VAR]	Unique identifier of the email moved to quarantine
General: Server	[VAR]Server[/VAR]	Server used to send the relevant email; in this case the name entered in the configuration.
General: Server (network name)	[VAR]ServerFQDN[/VAR]	Server used to send the relevant email; in this case the network name of the server (fully qualified domain name).
General: Time	[VAR]TimeOnly[/VAR]	Time when the triggering job ran.
General: Avira AntiVir Exchange Report	[VAR]ToolReport[/VAR]	Short summary of the scan results.
General: Avira AntiVir Exchange Report (details)	[VAR]ToolReportDetails[/VAR]	Results of the scans with all details.
General: Applicable recipients	[VAR]RestrictedRecipients[/VAR]	Recipients of the triggering email defined in the address (input) conditions.

AntiVir

Category, variable type	Variable	Description
AntiVir: Attachment size	[VAR]AttachmentSize[/VAR]	Size of the prohibited/affected attachment
AntiVir: Attachment type	[VAR]FingerprintName[/VAR]	Name of the prohibited file type
AntiVir: Fingerprint category	[VAR]Fingerprintcategory[/VAR]	Category of the prohibited file type

AntiVir: Email size	[VAR]MessageSize[/VAR]	Size of the entire email
AntiVir: Attachment name	[VAR]AttachmentName[/VAR]	Name of the prohibited/affected attachments
AntiVir: Email size limit	[VAR]SetSizeLimit[/VAR]	Maximum email size defined in the job
AntiVir: Virus name	[VAR]Virusname[/VAR]	Names of the viruses detected
AntiVir: Virus scanner	[VAR]VirusScanner[/VAR]	Names of the detecting virus scanners

Information store scan

Category, variable type	Variable	Description
IS-Scan: Database	[VAR]VSAPI_Database[/VAR]	Name of the information store in which the message was located at the time of the virus scan
IS-Scan: Database URL	[VAR]VSAPI_Url[/VAR]	URL of the information store in which the message was located at the time of the virus scan
IS-Scan: Error description	[VAR]VSAPI_ErrorText[/VAR]	Further description in the event of an error by the information store job
IS-Scan: Submit time	[VAR]VSAPI_SubmitTime[/VAR]	Date and time the message was sent.
IS-Scan: MessageUrl URL	[VAR]VSAPI_MessageUrl[/VAR]	URL of the information store of the message at the time of the virus scan
IS-Scan: Folder	[VAR]VSAPI_Folder[/VAR]	Name of the information store folder in which the message was located at the time of the virus scan
IS-Scan: Mailbox	[VAR]VSAPI_Mailbox[/VAR]	Name of the owner of the mailbox in which the message was located at the time of the virus scan
IS-Scan: Server	[VAR]VSAPI_Server[/VAR]	Name of the server on which the virus scan by the information store scan took place
IS-Scan: Virus scanner	[VAR]virusscanner[/VAR]	Name of the detecting virus scanner
IS-Scan: Virus name	[VAR]virusname[/VAR]	Names of the viruses detected
IS-Scan: Delivery time	[VAR]VSAPI_DeliveryTime[/VAR]	Date and time the message was delivered.

Details on the Avira AntiVir Exchange Management Console

AntiVir Wall

Category, variable type	Variable	Description
Content scan		
Wall: Content checking details	[VAR]DeniedContentTabHTML[/VAR]	Detailed information about the words/phrases found
Wall: Mail part	[VAR]DeniedMailParts[/VAR]	Affected triggering attachments/message texts
Wall: Restricted dictionaries	[VAR]DeniedWordlists[/VAR]	Triggering dictionary with value/threshold attained
Wall: Restricted words	[VAR]DeniedWord[/VAR]	Triggering word with value/threshold attained
Anti-spam check		
Wall: Spam analysis details	[VAR]SpamReportHTML[/VAR]	Detailed information about the individual spam criteria
Wall: Spam probability	[VAR]SpamValue[/VAR]	Determined spam probability in the form of a value (0 - 100). This value is compared with the individually set thresholds in the Advanced Spam Filtering job.
Wall: Spam level	[VAR]SpamLevel[/VAR]	AntiVir Wall enters a spam level in the email header of every scanned email as a number of stars in increments of 10 (e.g. (X-SPAM-TAG: * means the spam probability is between 0 and 10, X-SPAMTAG:*** means the probability is between 20 and 30). You can search for this string in the Outlook header and formulate a rule that assigns various actions to all emails with three or more stars, for example. You will find more information about regulatory options in Outlook in the Outlook Help.
Address scan		
Wall: Number of recipients	[VAR]NumberRecipient[/VAR]	Number of addressed recipients
Wall: Max. number of recipients	[VAR]SetRecipientLimit[/VAR]	Restriction on the number of recipients set in the job

Wall: Restricted senders	[VAR]DeniedSender[/VAR]	Name of the triggering sender
Wall: Restricted recipients	[VAR]DeniedRecipient[/VAR]	Name of the triggering recipients

Quarantine summary report

Category, variable type	Variable	Description
Summary: Sender	[VAR]From[/VAR]	Summary report sender
Summary: Reply to	[VAR]ReplyTo[/VAR]	The address to which replies to the summary report are to be sent (NotificationReplyTo)
Summary: Subject	[VAR]Subject[/VAR]	Summary report subject
Summary: Current summary support date	[VAR]Nowdate[/VAR]	Date when the current summary report was generated
Summary: Last summary report date	[VAR]Lastdate[/VAR]	Date when the last summary report was generated
Summary: Current summary report date and time	[VAR]Now[/VAR]	Date and time when the current summary report was generated
Summary: Last summary report date and time	[VAR]Last[/VAR]	Date and time when the last summary report was generated
Summary: Recipients	[VAR]RcptTo[/VAR]	Summary report recipients
Summary: Fully qualified domain name	[VAR]FQDN[/VAR]	Full network name of the server where the quarantine is located for which the summary reports are generated.
Collective notification: List of Quarantine emails	[VAR]HtmlList[/VAR]	Complete list of all quarantine objects for the relevant recipient with HTML formatting (mandatory field in the quarantine summary report).
Summary: HTTP port	[VAR]HTTPPort[/VAR]	HTTP server port
Summary: HTTP server	[VAR]HTTPServer[/VAR]	HTTP server for sending a user query via HTTP
Summary: Quarantine	[VAR]Displayname[/VAR]	Name of the quarantine from which the list of emails was created
Summary: Server	[VAR]Server[/VAR]	Short name of the server where the quarantine is located for which the summary reports are generated
Summary: Current summary report time	[VAR]Nowtime[/VAR]	Time when the current summary report was generated
Summary: Last summary report time	[VAR]Lasttime[/VAR]	Time when the last summary report was generated

Collective notifications

Category, variable type	Variable	Description
Collective notification: Table of contents	[VAR]TOCList[/VAR]	Numbered HTML list of all notifications (Subject). Each list entry is linked with the associated entry in the notification list (variable "NotificationList").
Collective notification: Notification list	[VAR]NotificationList[/VAR]	HTML list of all notifications (body), each separated by a vertical separating line.

Whitelist

Category, variable type	Variable	Description
Userlist: Entries	[VAR]HtmlList[/VAR]	Complete list of all entries for the relevant recipient with HTML formatting (mandatory field in the whitelist notification).
Userlist: Fully Qualified Domain Name	[VAR]FQDN[/VAR]	Full network name of the server where the whitelist is located for which the summary reports are generated.
Userlist: HTTP Port	[VAR]HTTPPort[/VAR]	HTTP server port
Userlist: HTTP Server	[VAR]HTTPServer[/VAR]	HTTP server for sending a user query via HTTP
Userlist: Name	[VAR]Displayname[/VAR]	Name of the whitelist from which the list of emails was created
Userlist: Recipients	[VAR]RcptTo[/VAR]	Whitelist report recipients
Userlist: Reply address	[VAR]ReplyTo[/VAR]	The address to which replies to the whitelist notification are to be sent (NotificationReplyTo)
Userlist: Sender	[VAR]From[/VAR]	Whitelist notification senders
Userlist: Server	[VAR]Server[/VAR]	Short name of the server where the whitelist is located for which the notifications are generated
Userlist: Number of entries	[VAR]CollectedSize[/VAR]	Overall size of whitelist notification

Userlist: Subject	[VAR]Subject[/VAR]	Notification subject
Userlist: Number	[VAR]SummaryPart[/VAR]	If more than 3,000 new entries appear in a whitelist, the user receives several whitelist notifications. The variable returns the current number for the notification (“1” for the first 3,000 entries, “2” for the next 3,000, etc.).
Whitelist: Send whitelist by web	[VAR]link::HTTP_SendWhitelist [/VAR]	Whitelist query and notification via HTTP
Whitelist: Send whitelist by mail	[VAR]link::MAIL_SendWhitelist [/VAR]	Whitelist query and notification via email
Whitelist: Clear whitelist by web	[VAR]link::HTTP_ClearWhitelis [/VAR]	Delete whitelist via HTTP
Whitelist: Clear whitelist by mail	[VAR]link::MAIL_ClearWhitelist [/VAR]	Delete whitelist via email
Blacklist: Send blacklist via HTTP	[VAR]link::HTTP_SendBlacklist[/VAR]	Blacklist request and notification via HTTP
Blacklist: Send blacklist by email	[VAR]link::MAIL_SendBlacklist[/VAR]	Blacklist request and notification by email
Blacklist: Delete blacklist via HTTP	[VAR]link::HTTP_ClearBlacklist[/VAR]	Blacklist deleted via HTTP
Blacklist: Delete blacklist by email	[VAR]link::MAIL_ClearBlacklist[/VAR]	Blacklist deleted by email

4.3.7 Creating a database connection to an SQL server

Connection with SQL servers

You can use database connections to link external databases to Avira AntiVir Exchange. Instead of the regular local database based on Microsoft Jet-Engine, it is also possible to use a Microsoft SQL server that saves the Avira AntiVir Exchange data in an SQL database. At present, MS SQL Server 2000 and MS SQL Server 2005 are supported, while MS SQL Server 2005 Express can also be used when CPU and memory capacity are limited.

Options available with SQL servers

In multi-server environments without server synchronization you can use a Microsoft SQL server to ensure that each user only receives a central whitelist for all participating servers.

In addition, the Microsoft SQL Server can also be used with quarantine databases.

If several SQL servers and multiple Avira AntiVir Exchange Servers are installed in a multi-server environment, these can be arranged in pairs. This means that there is a local SQL server installed on every Avira AntiVir Exchange Server, so that only one database connection is required.

Note: Bear in mind that Avira AntiVir Exchange is optimized for use as a local database based on MS Jet Engine. In the case of complex server environments, extensive configurations are required on Avira AntiVir Exchange and on the MS SQL server that cannot be explained here. If you have specific questions, please contact our support team.

Configuring the database connection

The following sections describe the configuration of database connections between Avira AntiVir Exchange and an Microsoft SQL server. During configuration, please note the distinction between a central MS SQL server for central user whitelists and a local MS SQL server for the quarantine.

SQL server and Avira AntiVir Exchange Server:

If the SQL server and the Avira AntiVir Exchange Server are installed on the same computer, the following requirements must be met:

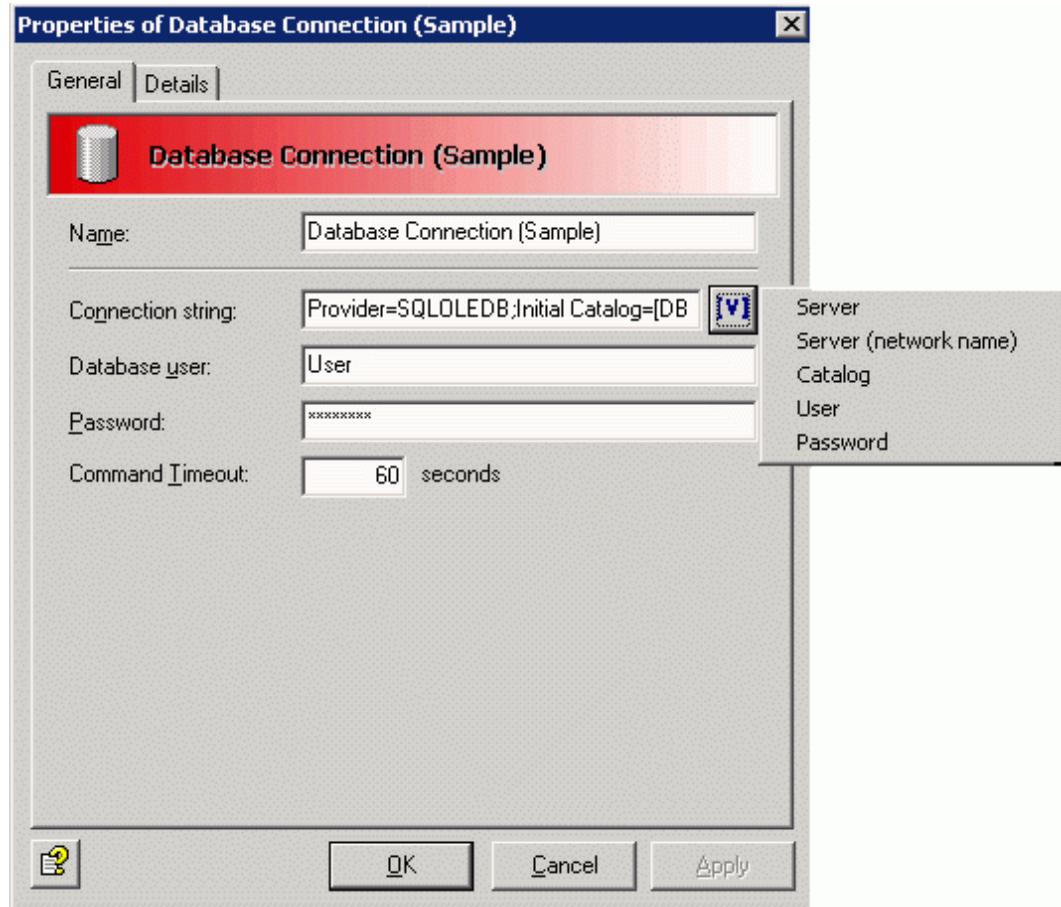
- Installations of SQL server and Avira AntiVir Exchange Server are complete.
- Database(s) are configured and the associated tables are created
- At least one user is created as a database user
- The database user has corresponding access rights to the database
- The ADO driver is installed on the Avira AntiVir Exchange Server

If the SQL server and the Avira AntiVir Exchange Server are installed on different systems, it is also necessary to ensure that:

- the protocol set on the SQL server meets the requirements for external server operations.
- The service has been restarted after the SQL server was configured.

The database connection between Avira AntiVir Exchange and the SQL server is established by means of the ADO protocol.

1. For this purpose you should create a new database connection under **Basic Configuration - General Settings - Database Connections** under **Address Lists**.
2. Assign a **name** for the connection configuration and define the details for the ADO string in the **Connection string** field.
3. Enter the required values manually or use the stored Avira AntiVir Exchange variables (server, database, etc.), which are then replaced by the relevant values during runtime.



The following **example** is one of many configuration options for the ADO string. You will find detailed explanations of this and other options and configurations of the MS SQL ADO string in the appropriate Microsoft documentation.

Sample connection string:

```
Provider=SQLOLEDB;User  
ID=[ADOUUser];Password=[ADOPwd];Trusted_Connection=No;Initial  
Catalog=[DBCatalog];Data Source=LOCALHOST\SQLEXPRESS;
```

- Provider=SQLOLEDB; Obligatory parameter that specifies the provider. Enter the value manually (no AntiVir variable available).
- User ID=[ADOUUser]; Password=[ADOPwd]; Obligatory parameter; enter the parameters 'User ID=' and 'Password=' manually in the string and set the AntiVir variables **Database user** and **Password**. The inserted [ADOUUser] and [ADOPwd] will be replaced by the contents of the field from point 3 during evaluation. It is recommended that variables should be used as this prevents the values in the ADO string from appearing in plain text. However, in theory, the values can also be entered manually. In this case the two fields at point 3 should be left empty.
- Trusted_Connection=No; Optional parameter for SQL authentication. To enable the SQL server to recognize the Avira AntiVir Exchange Server as a trusted server, enter 'Trusted_Connection=No;' manually (no Avira AntiVir Exchange variable available).

- `Initial Catalog=[DBCatalog]` ; Obligatory parameter that specifies the database to be used. Enter the parameter '`Initial Catalog=`' in the string manually and set the Avira AntiVir Exchange variable **Database**. If you use the SQL server for the quarantine, the variable [DBCatalog] is replaced with the name of the **database** defined under **Quarantine - Properties** in the **Folder name** field. If, on the other hand, you use the SQL server for a central whitelist, the variable [DBCatalog] is replaced with the fixed name '`Whitelist`'. The variable [DBCatalog] enables you to use a database connection for several databases within an MS SQL server. Please note that the databases must be created under precisely this name. Otherwise a connection cannot be established.
- `Data Source=LOCALHOST\SQLEXPRESS` ; Obligatory parameter for a locally installed MS SQL Server 2005 Express. In this case, enter the parameter '`Data Source=`' manually and, if necessary, set the Avira AntiVir Exchange variable **Server**. The [Server] variable is replaced by the NetBiosName of the server at runtime. If you work in complex server environments with subdomains, you can also use the Avira AntiVir Exchange **Server (network)** variable. In this case, the [ServerFQDN] variable is set and the FQDN (Fully Qualified Domain Name) of the server is read out. If the SQL server is used for central whitelists, manually enter the name of the central SQL server here.

Exception: In the case of a central SQL server, e.g. when the SQL server is used for central whitelists, the two Avira AntiVir Exchange variables **Server** and **Server (network)** cannot be used in the ADO string. Instead you should enter the name of the SQL server manually, i.e. `Data-Source=Name_des_Servers`;

4. Enter the name of the SQL user permitted to access the database in the **Database user** field (shown in the graphic as User). Enter the associated **Password** in the next field. The values entered here can be read out using the variables [ADOUser] and [ADOPwd] in the ADO string.
5. The **Command Timeout** field is used to specify the waiting period in seconds before the database connection is closed if the database does not return data. You are advised to begin with a value of 60 seconds when using large databases.

Configuring central whitelists

If the email is handled in multi-server environments, every server creates its own user whitelists. Without server synchronization, each user therefore receives a separate whitelist for each participating server and each whitelist has to be maintained separately. To be able to administer these whitelists centrally, thus simplifying administration, instead of the regular local database based on Microsoft Jet-Engine, you can also set up a Microsoft SQL server to save the data for all participating Avira AntiVir Exchange Servers in a central SQL database.

To configure central whitelists, you must first configure a database connection between the SQL server and the Avira AntiVir Exchange Server. More settings are required within Avira AntiVir Exchange after this, so that Avira AntiVir Exchange can use the entries from the whitelist database.

The configuration of the database connection depends on the server environment

1. Proceed according to operating environment, as in the scenarios under [Configuring the database connection](#).
2. Enter the central SQL server under `Data Source=`.

Note: Bear in mind that the [DBCatalog] variable for the whitelist database is replaced with the fixed database name in the ADO string of the database connection.

3. Under **AntiVir Servers Settings - Properties** select the SQL server in the **Database connection for whitelist entries** field. This field contains all data sources entered under database connections for selection.
4. Open the Wall job **Advanced Spam Filtering - Actions - Definite Criteria** and enable the **Emails from senders in user whitelist** field

Configuring a quarantine database

In addition to the option for using the Microsoft SQL server for whitelists, the server can also be used locally with quarantine databases. The index for a quarantine is regularly listed in the local database (Microsoft Jet engine). If the capacity of a Jet database is not sufficient, you can also save these entries in a locally installed SQL server. You must have installed MS SQL on the email server for this purpose.

The configuration of the database connection depends on the server environment

1. Proceed according to operating environment, as in the scenarios under [Configuring the database connection](#).
2. Enter Source= under data on every LOCALHOST server, so as to be able to access the locally installed SQL server.

Note: Bear in mind that the [DBCatalog] variable for the name of the quarantine database is replaced with the folder name under **Quarantine - Properties - Folder name** in the ADO string of the database connection. This means that one database connection can be used for several quarantine databases.

In the case of SQL databases, it is also possible that the database service might fail or be unavailable. Consequently, the quarantine name would also be unavailable during this downtime, so that emails to be quarantined in this time would not be saved correctly. As with the **mission critical** option in the job, the same option is also available for the quarantine (enable **Quarantine - Right click: Properties - Quarantine is mission critical**) to control the handling of emails in the event of a quarantine error.

If a quarantine is set to 'mission critical', any quarantine errors that occur are reported to the job. The job is then canceled and the error routine of this job is started. The way in which the email is dealt with, i.e. whether the job ignores the email or moves it to the bad mail directory, depends on the 'mission critical' setting in the job itself.

Handling problems with SQL servers

There may be several different reasons why problems arise while installing or configuring SQL servers. This is why we can only offer some advice on how to analyze errors:

- Make sure that the SQL server browser is enabled.
- Check the port (default: 1433) or adapt it to your server environment.

Path for *Microsoft SQL Server 2005*: Double-click **Configuration Tools - SQL Server Configuration Manager** under **SQL Native Client Configuration - Client Protocols - TCP/IP**.

Path for *Microsoft SQL Server 2005*: **Configuration Tools - SQL Server Configuration Manager - SQL Server 2005 Services - SQL Server Browser** (Status: Running).

If a central SQL server is installed that runs on a system other than the AntiVir Server, the following requirements must also be met:

- If you use *Microsoft SQL Server 2005*, select **Configuration Tools - SQL Server Surface Area Configuration - Surface Area Configuration for Services and Connections**. For **MSSQLSERVER - Database Engine - Remote Connections** select the option **Using both TCP/IP and named paths** to permit the connection to the SQL server configured in the ADO string.
- The SQL server service must be restarted after configuration.

Note: You should also note the configuration options for quarantine (**mission critical**) if the database service fails.

4.3.8 Folder settings

Configuring a quarantine

A quarantine is a folder in which all emails affected by the conditions are stored if you defined this with the **Copy to Quarantine** action. When you install Avira AntiVir Exchange, a folder called Quarantine is created in the data directory. This folder initially contains some default quarantines and later all additional newly created quarantines.

1. You can configure existing quarantines and create new ones under **Basic Configuration - Folders - Quarantines**. Click **Quarantines**.

All available quarantines are displayed in the right-hand window.

To create a new quarantine:

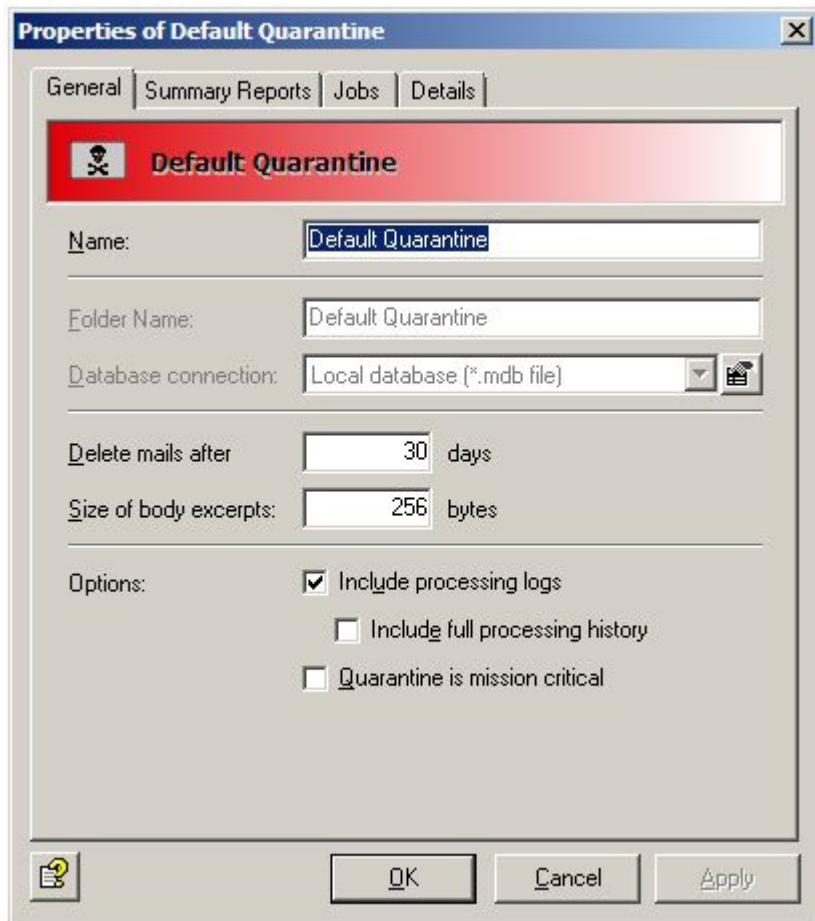
- Right-click **Quarantines** and select **New - Quarantine**.
- The **Folder name** from the description is then transferred. Only characters from A-Z and 0-9 are transferred; all other characters are converted to underscores.
- You can overwrite the suggested **Folder name**.

Note: Do not enter an absolute path here. You only need to enter the folder name.

- When you save the configuration, EMH automatically creates the new quarantine and it is then also displayed in the AntiVir Monitor (update the view!).

Warning: The size of a quarantine is restricted to 1 GB.

2. Right-click on an existing quarantine in the right-hand window and select **Properties**.



3. You can give the quarantine a meaningful name under **Name**. However, the **Folder name** of the quarantine remains unchanged. The entry in the Folder name field is only available for some, newly created quarantines.
4. Define how many days an email that was placed in quarantine should be kept before it is automatically deleted.
5. Use **Size of body excerpts** to determine whether and how much of the text from the body of the email (message text) is to be written to the database.
When setting this value, make sure to take data protection aspects and the required space in the database into account.
Warning: The size of a quarantine is restricted to 1 GB.
6. With **Include processing logs**, you can log the processing of the emails placed in this quarantine.
This allows you, for example, to trace the reasons for an email being placed in quarantine. In the AntiVir Monitor, you can access the respective email and view the processing log including detailed information via the **Processing Log** tab.
7. **Quarantine is mission critical:**
If this field is enabled, any quarantine errors that occur are reported to the job. The job is then canceled and the error routine of this job is started. The way in which the email is dealt with, i.e. whether the job ignores the email or moves it to the bad mail directory, depends on the 'mission critical' setting in the job itself. For information on 'mission critical' in the job, see [Job is mission critical](#).

Example: A job that checks for viruses finds a virus in an incoming email. The job is configured in such a way that the email is delivered to the default quarantine but not to the recipient. The quarantine is not available due to a quarantine error. The email therefore cannot be placed in quarantine. The following are possible settings for the quarantine and the job:

- Quarantine + Job are both NOT ‘mission critical’:Result: The quarantine error is ignored. The email cannot be copied to the quarantine and is also not delivered.
- Quarantine is NOT ‘mission critical’ + Job IS ‘mission critical’:Result: see above.
- Quarantine IS ‘mission critical’ + Job is NOT ‘mission critical’:Result: The job processing is canceled and the virulent (!) email is transferred unprocessed to the next job in the processing chain.
- Quarantine + Job are both ‘mission critical’:Result: The email is moved to the Bad mail quarantine and is kept there. The email is not delivered.

Warning: For as long as the quarantine error is not fixed, the error will be repeatedly reported to the job if the ‘mission critical’ option (in the quarantine) is enabled.

If the job itself is not ‘mission critical’, it turns itself off after a certain time and does not process any further emails.

If, however, the job is ‘mission critical’, every email is transferred to the bad mail area and is not delivered until such time as the error is fixed.

Irrespective of the ‘mission critical’ setting, the Avira AntiVir Exchange administrators are informed by email about errors that occur frequently in the quarantine or in the job.

8. In the **Summary Reports**, you can now configure a quarantine summary report for this quarantine.

Note: If you want to allow the users access to the processing of whitelists, select Quarantine Summary Report with Whitelist Support under Template.

Setting up quarantine summary reports

A **Quarantine Summary Report** provides information on emails that Avira AntiVir Exchange placed in quarantine.

Summary reports can be sent to various recipients/recipient groups and can contain a list of various quarantine emails. The emails in question, the actions that the recipient of the summary report can start for these emails and the additional information that the summary report contains are all configured separately in each summary report.

Each type of notification comprises two parts:

- The template in which the form of the summary report is defined.
The templates of the summary reports can be edited under **Basic Configuration - General Settings - Templates - Quarantine Summary Reports**. The variables available here are exclusively related to the summary reports and their form. Configure the quarantine summary report template as described under [Creating notification templates](#).

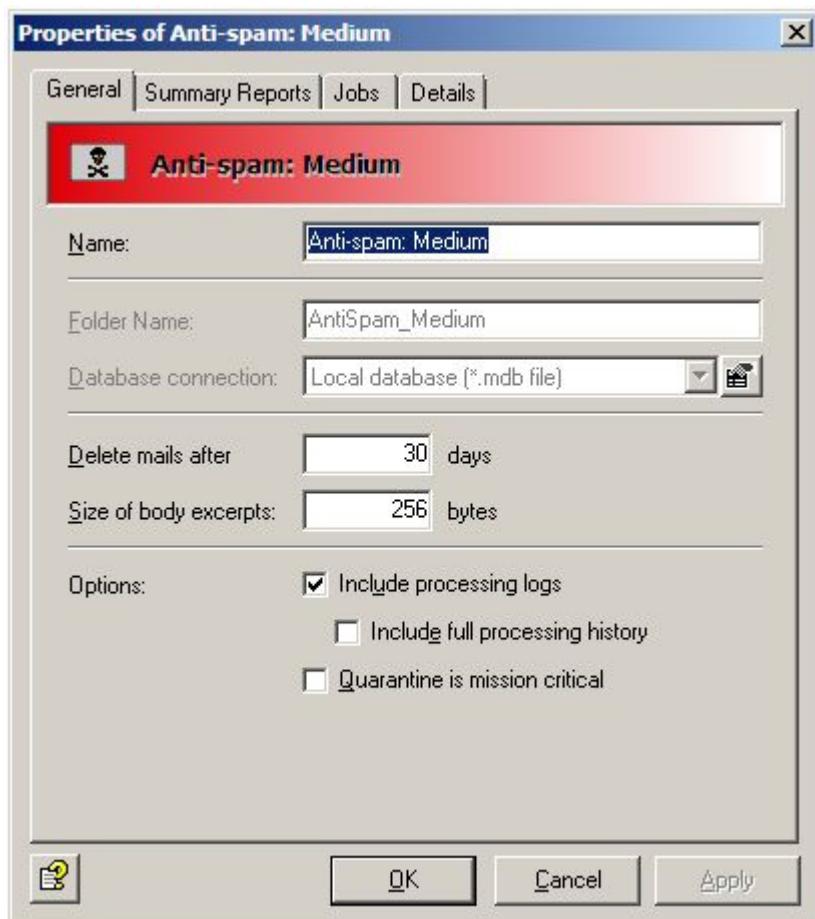
- A list of emails placed in quarantine (the actual content of the summary report), in which fields are used to define which emails and email fields are to be listed in the summary report created.

The content of the summary report is also defined using the **Summary Report: List of Quarantine Mails** variable ([VAR] HTMLList [/VAR]), which is a mandatory entry in each summary report. The entries that this list contains are defined under **Basic Settings - Folders - Quarantines - Properties of a Quarantine - Summary Reports - Add - Fields**.

The **Summary Report: Sender** variable under **Templates** designates the sender of the summary report (the same sender as for all Avira AntiVir Exchange notifications and is defined under AntiVir Server Settings). The check box for the **Sender** in the Fields tab in a quarantine designates the sender of the emails placed in quarantine that are listed in the list of emails.

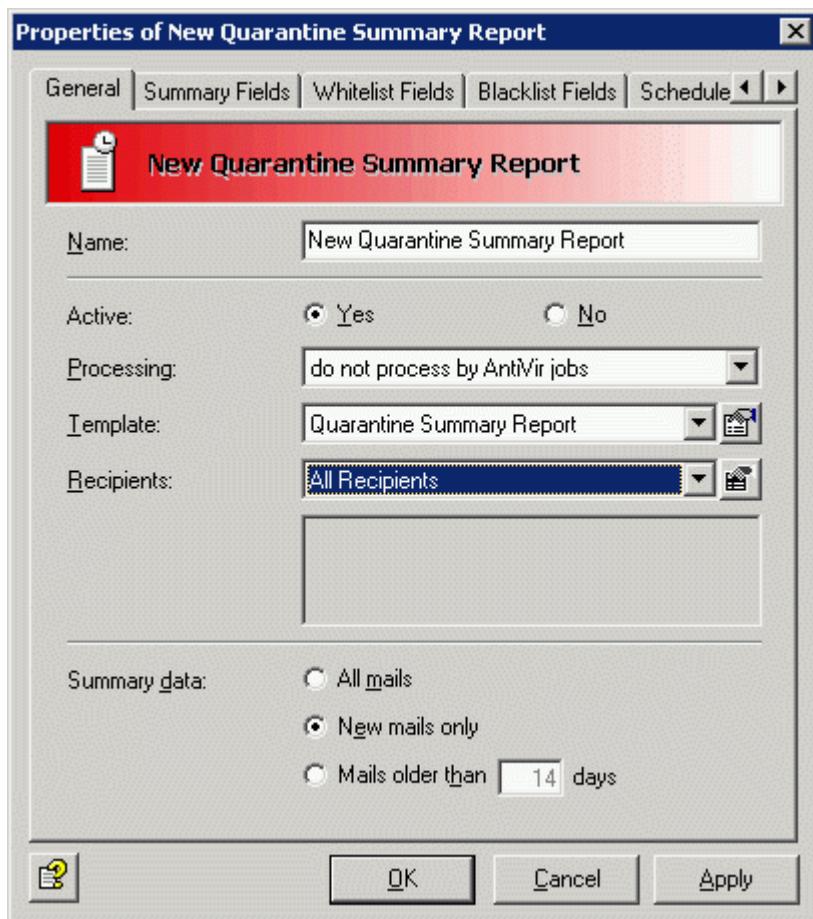
Summary reports are particularly intended for spam quarantines and the recipients of these spam mails. The standard case is for the users to receive a list of all new spam mails that were addressed to them and that are in a specific spam quarantine. This standard case is configured as follows:

1. Open **Basic Configuration - Folders - Quarantines**.
2. In the right-hand window, double-click the **Anti-spam: Medium** spam quarantine to open it.



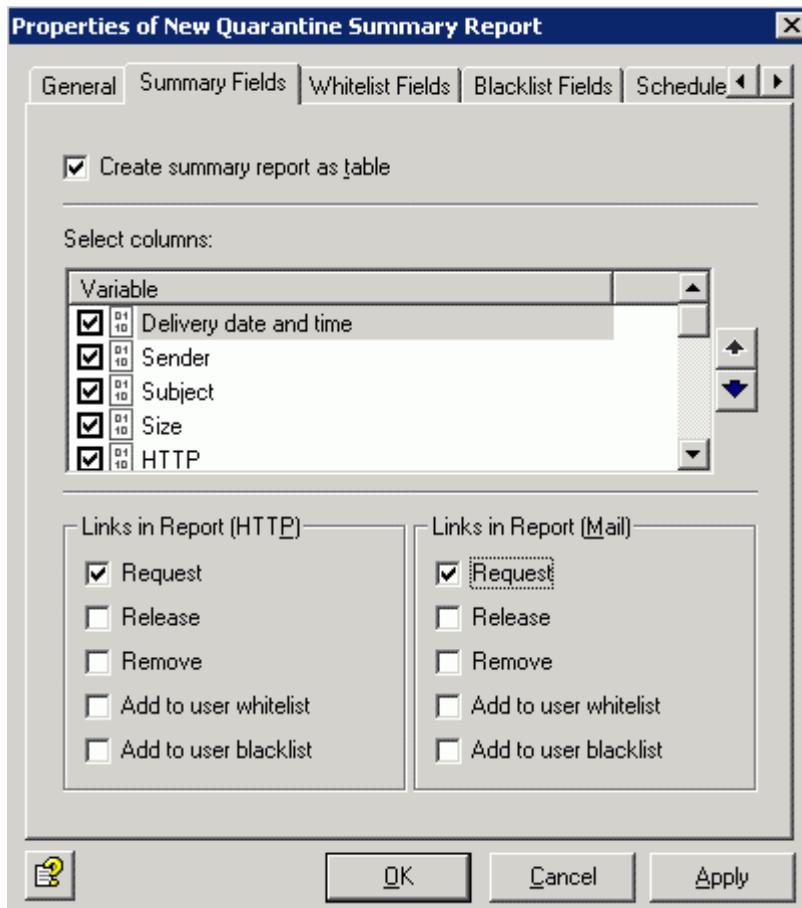
3. Click the **Summary Reports** tab.
4. Click **Add**.

5. Assign a name for the summary report on the **General** tab.



6. In the **Recipients** field, select the **All Recipients** entry. Recipients of the summary report are the original recipients of the quarantine emails. Select **User-defined recipients** if, for example, you want to restrict the group of recipients for a summary report. The selected recipients, senders, groups or other address patterns are then listed in the lower text box.
7. As a template, you can select a summary report that you defined yourself under **General Settings - Templates - Quarantines - Summary Reports**. The Avira AntiVir Exchange standard delivery includes the **Quarantine Summary Report** template, which already contains preconfigured settings. If you want to allow your users to place a sender from the summary report on their user whitelist, use the **Quarantine Summary Report with Whitelist Support** template.
8. For **Summary data**, select **New mails only**. In this way, the recipient of the summary report only receives the emails that came in since the last summary report in the quarantine.
9. **Processing: do not process by AntiVir jobs** means that the resent email that the user requested or released is no longer checked by the active AntiVir jobs. Each requested or released email is delivered unchecked to the recipient. See also the **Fields** tab.

10. In the **Fields** tab, select which fields from the quarantine emails are to be written to the list of quarantine emails of the summary report. If, for example, you select the **Subject** check box here, the subject of the quarantine email is listed in the email list of the summary report. The relevant check boxes for the standard case are already selected.



The recipient of the summary report can execute an action with the listed email by clicking the links in the report. Here, select the action that the user is permitted to execute:

Request: The email is delivered from the quarantine to the recipient of the summary report.

Release: The email is delivered to all original recipients of the email.

Remove: The email is marked for deletion in the quarantine.

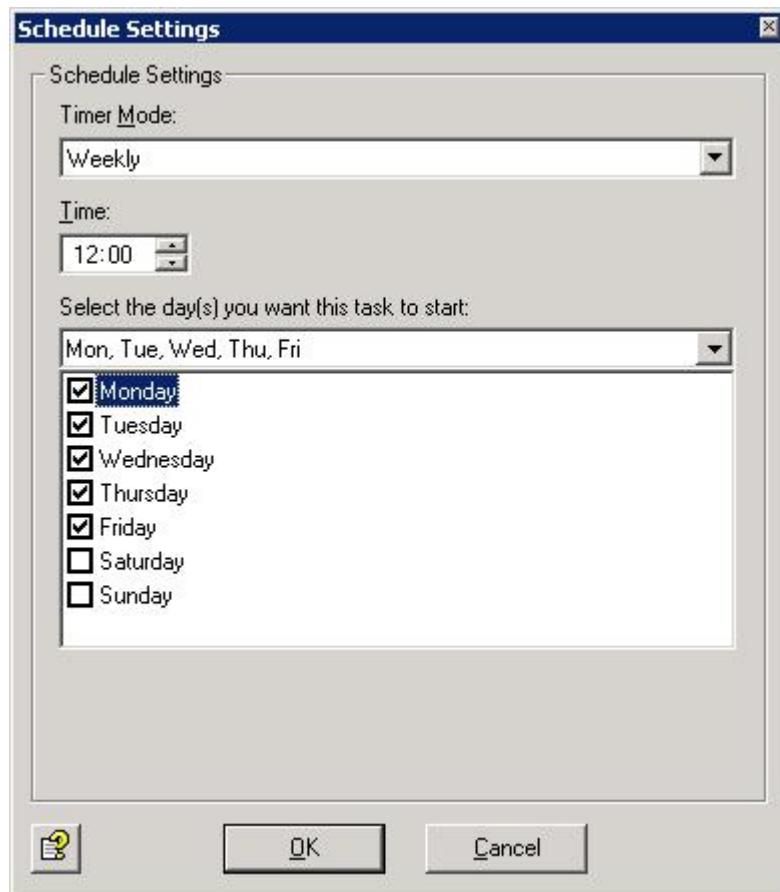
Add to user whitelist: The sender of the email is added to the user whitelist.

Add to user blacklist: The sender of the email is added to the user blacklist.

Note: If you select several check boxes, several links to an email will appear in the summary report.

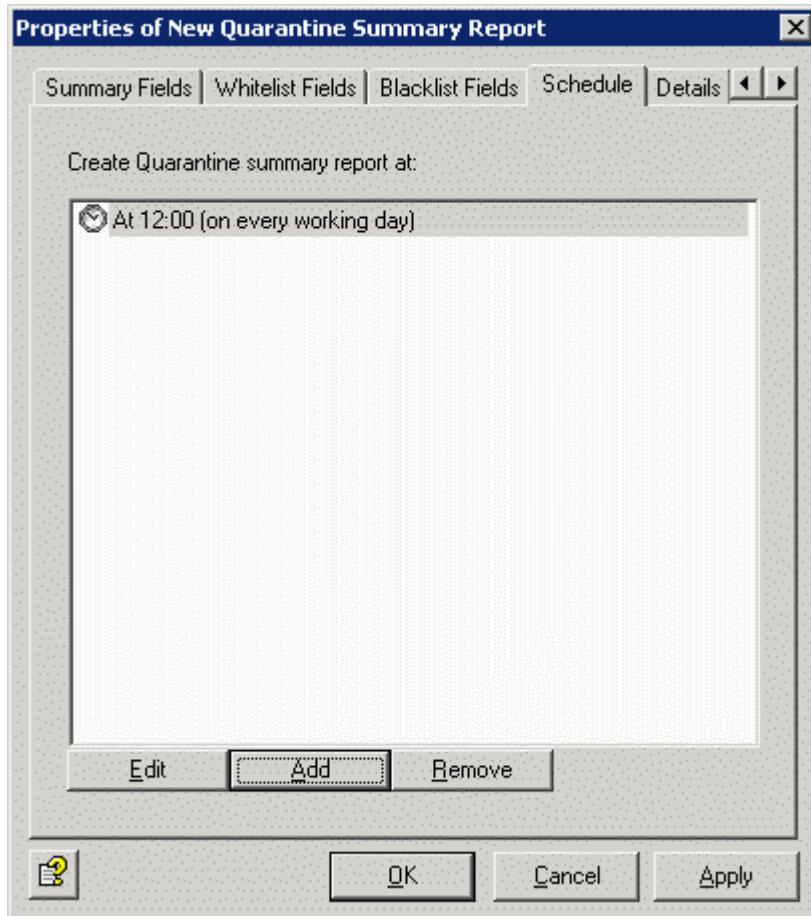
11. In the **Whitelist Fields** or **Blacklist Fields** tabs, select the fields from the quarantine emails that you want to appear in the whitelist or blacklist report.

12. Click the **Schedule** tab and then **Add**. A Schedule Settings window in which you can define the start of the summary report creation is displayed. In this case, a quarantine summary report is generated and sent to the recipients of the spam mails every workday at 12:00 a.m.



13. Click **OK**.

14. Your new quarantine summary report is now displayed in the **Schedule** tab. Clicking **Edit** allows you to change the time or the day of the week while clicking **Remove** deletes the summary report:



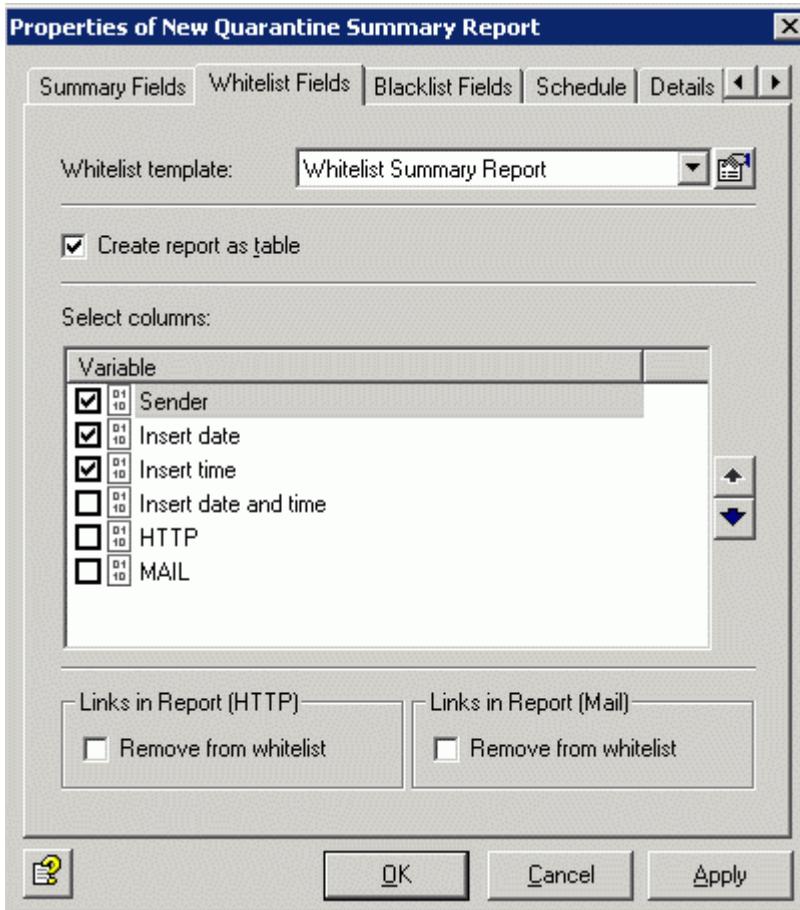
From now on, a summary report is sent to the recipients of spam mails of the **Anti-spam: Medium** quarantine at 12:00 a.m.

Note: You can create several different summary reports with different content for a quarantine. The emails for each summary report are "gathered" separately from the quarantine, even if the schedule for these summary reports is identical.

Note: You will find a list of all quarantines under **Basic Settings - Folders - Quarantines**. The Summary Report column allows you to see immediately the quarantines for which a summary report is configured (yes/no).

Whitelist report

Select the **Whitelist Support** template for the quarantine summary report so that the recipient of the quarantine summary report can manage the entries in his/her whitelist and can request a whitelist report.



Under **Whitelist Fields**, define the fields to be displayed.

Under **Whitelist template**, you can edit the existing whitelist template or create a new one. Configure the whitelist template with the variables as described under [List of template variables](#).

4.3.9 Utility settings

Fingerprints

AntiVir uses fingerprints for file type recognition. A comprehensive list of fingerprints is supplied with Avira AntiVir Exchange and these are divided into categories. It is generally not necessary to make changes initially. You will find more information about the configuration of fingerprints in [Configuring fingerprints](#).

Dictionaries

Here you can create dictionaries that contain word strings that you want to block during content and spam filtering with AntiVir Wall. We provide some dictionary categories, which you can adapt to your own needs. You will find the exact configuration of the dictionaries in [Setting up dictionaries](#).

AntiVir Scan Engine

For more information on configuring the virus scanner, see [Configuring and enabling the AntiVir Scan Engine](#).

4.4 Policy configuration

In the policy configuration, you define your AntiVir jobs based on your company's policies.

You can use various conditions (or also filters) to define which emails are affected, when specific actions should be executed, and in which sequence the jobs are to be processed (priority). All conditions can be configured within the job. The sum of the AntiVir jobs is the company policy.

4.4.1 Example of a company policy

Every incoming spam mail is to be detected, deleted or sent to quarantine.

The spam mails should not reach the recipient, but he should be informed that he has received spam and the spam should be named so that he can decide for himself which of these emails he wishes to receive.

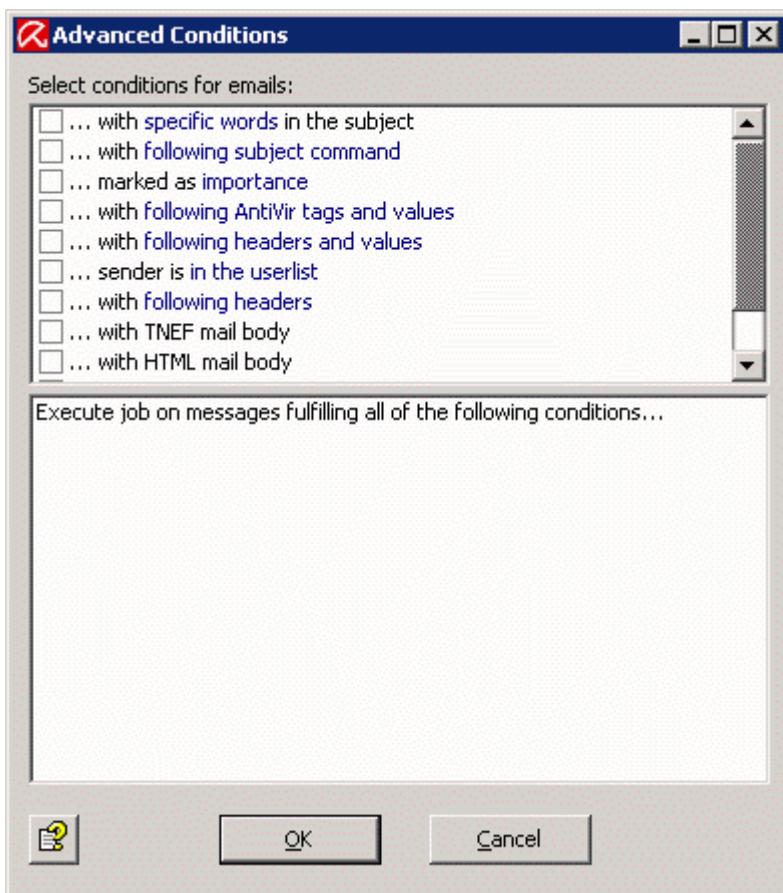
This is to be achieved with a daily summary.

All of this can be set up in the **Wall Spam Filtering** jobs.

4.4.2 Conditions

In each job you can define the properties that emails must have to ensure that a job is executed. You can define the conditional parameters yourself in accordance with your own requirements:

The processing of a job, e.g. scanning for viruses, is only initiated if all requirements for an incoming or outgoing email are met.



Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

Email processing can be controlled by means of the value of existing headers. External applications that process the emails prior to processing by Avira AntiVir Exchange can add certain X header fields with defined values to the emails, for example. The following AntiVir jobs can be configured with the condition ... **with following headers and values** so that job processing is initiated in accordance with the value of an X header field.

4.4.3 Job types

There are 9 different job types, which you can find under **Policy Configuration - Mail Transport Jobs - Right click - New:**

Job type	Meaning
AntiVir Scan	Job scans the emails for viruses.
AntiVir Email Size Filtering	Job checks the emails for a maximum permitted size (specified per email).
AntiVir Attachment Filtering	Job scans the emails for prohibited file attachments. The various file formats are identified using fingerprints.
AntiVir Attachment/Size Filtering	Job scans the emails for prohibited file attachments. The maximum permitted size for an attachment can be specified at the same time.
AntiVir Protected Attachment Detection	The job reacts to emails with password-protected archives and executes the job actions configured in the Actions tab. Password-protected archives can thus be handled in a rule-based way.
AntiVir Wall Content Filtering	Job scans the emails and attachments for prohibited text content.
AntiVir Wall Email Address Filtering	Job checks the emails for address restrictions.
AntiVir Wall Recipient Limit Filtering	Job checks the emails for a maximum permitted number of recipients per email (the recipients in the "To" field of an email are counted).
AntiVir Wall Spam Filtering	Job uses various criteria to scan emails for spam.

You can define your own conditions for each job type. All conditions must match before a defined action is executed. Address filters can be configured for all job types. For example, you can configure that all emails sent from the domains `*@gmx.net` and `*@hotmail.com`, that are larger than 500 KB, that contain the word "Look" and that belong to the Sound fingerprint category are to be deleted (and therefore not delivered to the recipient!) and that a copy of the email is to be placed in the quarantine. This case would be an **AntiVir Attachment/Size Filtering** job.

A series of standard jobs is provided with Avira AntiVir Exchange and you can modify these in accordance with your needs. Of course, you can also create your own jobs. The preconfigured jobs are available under **Policy Configuration – Job Templates**. Use the mouse to drag the required job into **Mail Transport Jobs**. Any number of jobs can be created. For the sequence of the processing, refer to **Mail Transport Jobs** from the order in the list of all jobs. Further information is available under [Processing sequence of jobs](#).

A job may be enabled or disabled. A disabled job is in the configuration but is not executed. If you want to disable jobs, you therefore do not need to permanently delete them from the configuration.

In each job, you can use the **Actions** tab to set which actions are to be executed if an email falls under the defined conditions or is infected with a virus.

4.4.4 Actions

In addition to the actions that belong to the function of a job, the following standard actions are also available:

Action	Meaning
Copy to quarantine	A copy of the email will be placed in the quarantine folder you have specified and can be viewed there at any time.
Delete email	The infected/blocked original email is permanently deleted from the server (the copy remains in quarantine if this option is set).
Delete attachment	The infected attachments are permanently deleted from the server.
Subject extension	A configurable extension is added to the subject line. This enables the recipient to see that this email has been scanned.
Send notifications to	Notifications can be sent to the following groups: <ul style="list-style-type: none"> • Administrators • Senders • Recipients • Others
Start external application	An external, freely selected application is run.
Add X header field	A field is added to the email header that can be filled with a value from the variables.
Redirect email	The email will be redirected to the specified recipients. Option: Original recipients also receive the email.

4.4.5 Processing sequence of jobs

The sequence in which a job is processed is displayed in the view of all jobs in **Policy Configuration - Mail Transport Jobs**.

New jobs are added to the end of the list. You can use the and arrow keys in the toolbar or right-click (**All Tasks - Up/Down**) to move the jobs to the required position.

4.5 AntiVir Monitor

AntiVir Monitor allows you to view the quarantine areas on every available server and to obtain detailed information about the emails contained there.

You can use AntiVir Monitor to observe all **Avira AntiVir Exchange Servers**, **quarantines** and **bad mails**. You can also access the **statistical evaluations**.

AntiVir Monitor lists all the servers configured under **Basic Configuration - AntiVir Server**. AntiVir Monitor uses SOAP/SSL encryption to access the server via the network.

To access a server, first enter it under **Basic Configuration - AntiVir Server** and refresh **AntiVir Monitor** in this view.

The procedure for adding a server can be found in the description [Settings for an individual AntiVir server](#). The configuration of the quarantine should also correspond in accordance with the description in the [Configure quarantine](#) section.

You can display detailed information about the AntiVir version and the configuration for every server. Right-click on the required server in **AntiVir Monitor** and select **Properties**.

To use AntiVir Monitor you must log on as an authorized user. If you are not logged on locally on the server, a login dialog will appear for you to enter your user name and the password for the relevant domain. The authorization for accessing AntiVir Monitor is entered in the properties of the file *access.acl* in the ... \Avira\Avira AntiVir Exchange\AppData\ folder.

Click on the **Security** tab and assign the relevant user at least read-only rights.

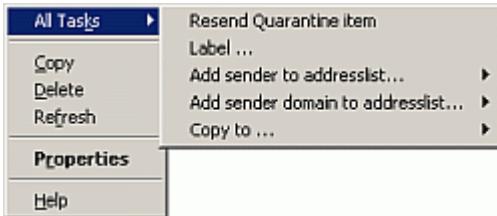
Observing the data in AntiVir Monitor:

1. Click the required server.
2. Authenticate yourself with a user name and password that has authorizations for the AntiVir data on the server's file system.
3. Click on the area you want to view, for example on **Default quarantine** or **Bad mail**. All existing emails will be displayed (limit 10,000 emails).
4. Filter the required emails with the **Filter Options** icon
5. Open an email with a double-click.
6. Send the email by clicking a second time if necessary.

4.5.1 Quarantines

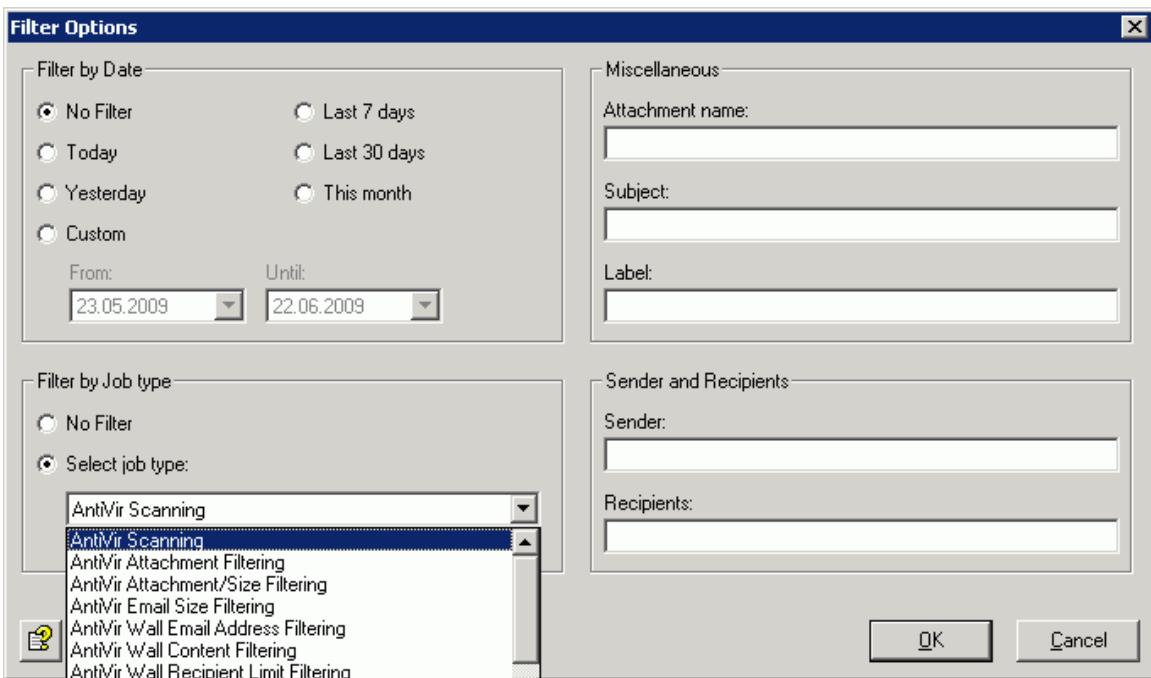
If you enabled the **Copy to quarantine** action in the job, then all affected emails are in a quarantine and all available information on the individual emails can be found in the AntiVir Monitor.

Click a quarantine. If you right-click an email, the following actions are available in the view:



You can also drag and drop to copy. Use your mouse to drag the selected email to another quarantine.

Within a quarantine, it is possible to filter emails according to numerous criteria. Right-click **View - Filter options** or on the icon. You will see the following dialog box:



There are three ways of resetting the options:

1. Enable the **No Filter** option in Filter Options.
2. Right-click **View - Show all objects**.
3. Use the icon in the toolbar.

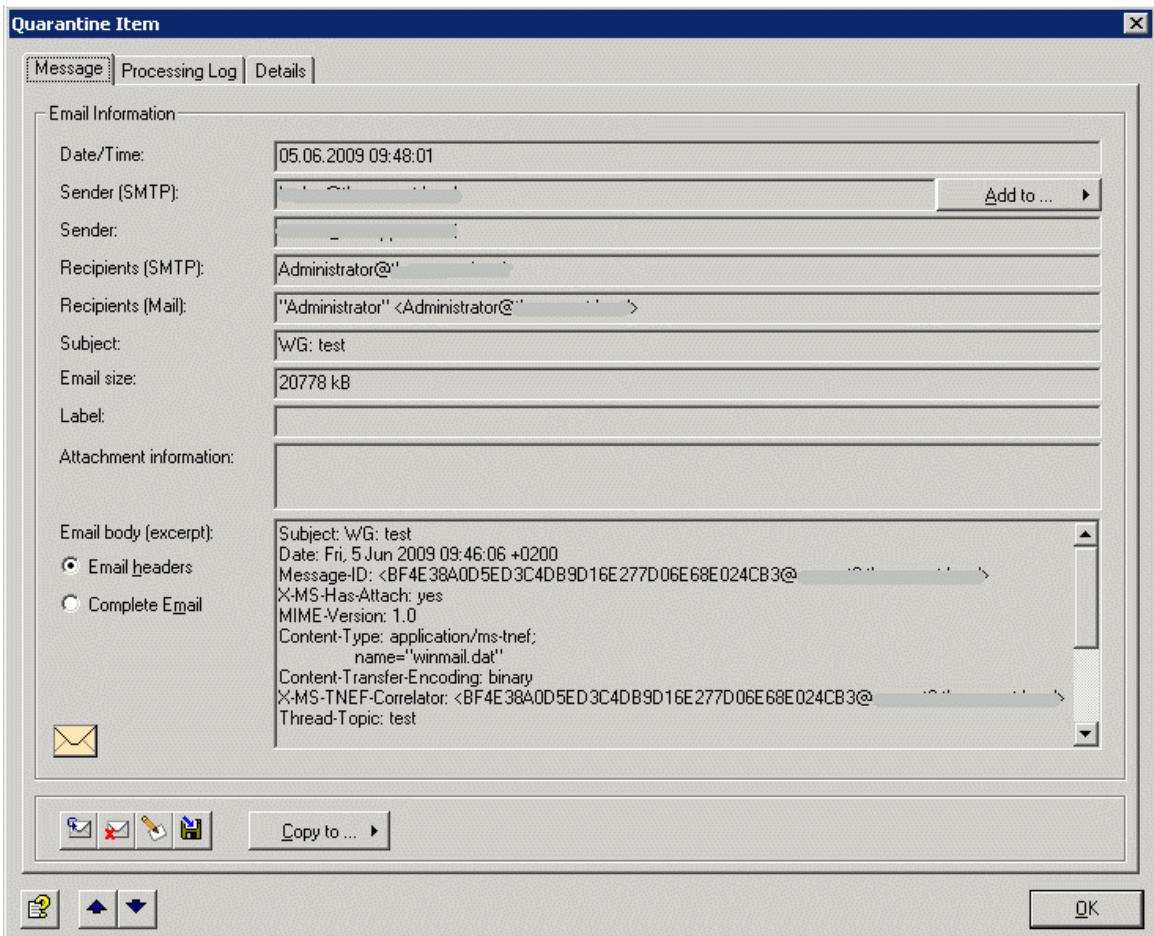
A maximum of 10,000 emails (the most recent) are displayed at any one time in the AntiVir Monitor. To obtain older emails that are no longer listed, restrict the view using a corresponding filter option.

Example of an email in quarantine

You receive this information if you double-click or right-click the properties of the email in the quarantine.

The most important information can be found at a glance on the Message tab.

Details on the Avira AntiVir Exchange Management Console



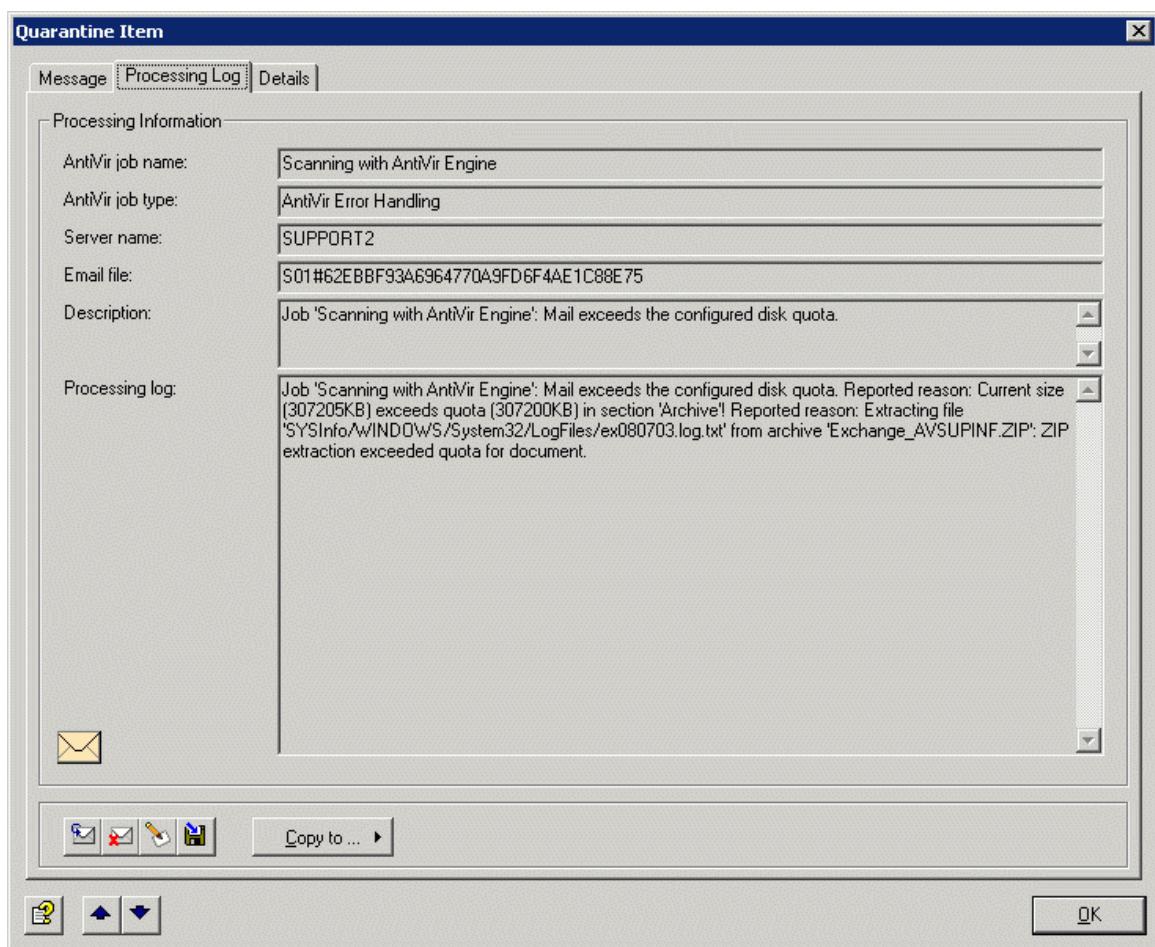
The icons used on these tabs:

	Send email from quarantine
	Delete email in quarantine
	Define, modify, delete the label for the email
	Save email as
	Open online help
	Next email in the quarantine / bad mail
	Previous email in the quarantine / bad mail

The **Add to** button allows you to add the SMTP sender of the email to the spam defense of a specific address list. You define for each individual address list which address lists are displayed under this button. See also [Address lists](#). Once the sender address has been added to the address list, you receive a message:

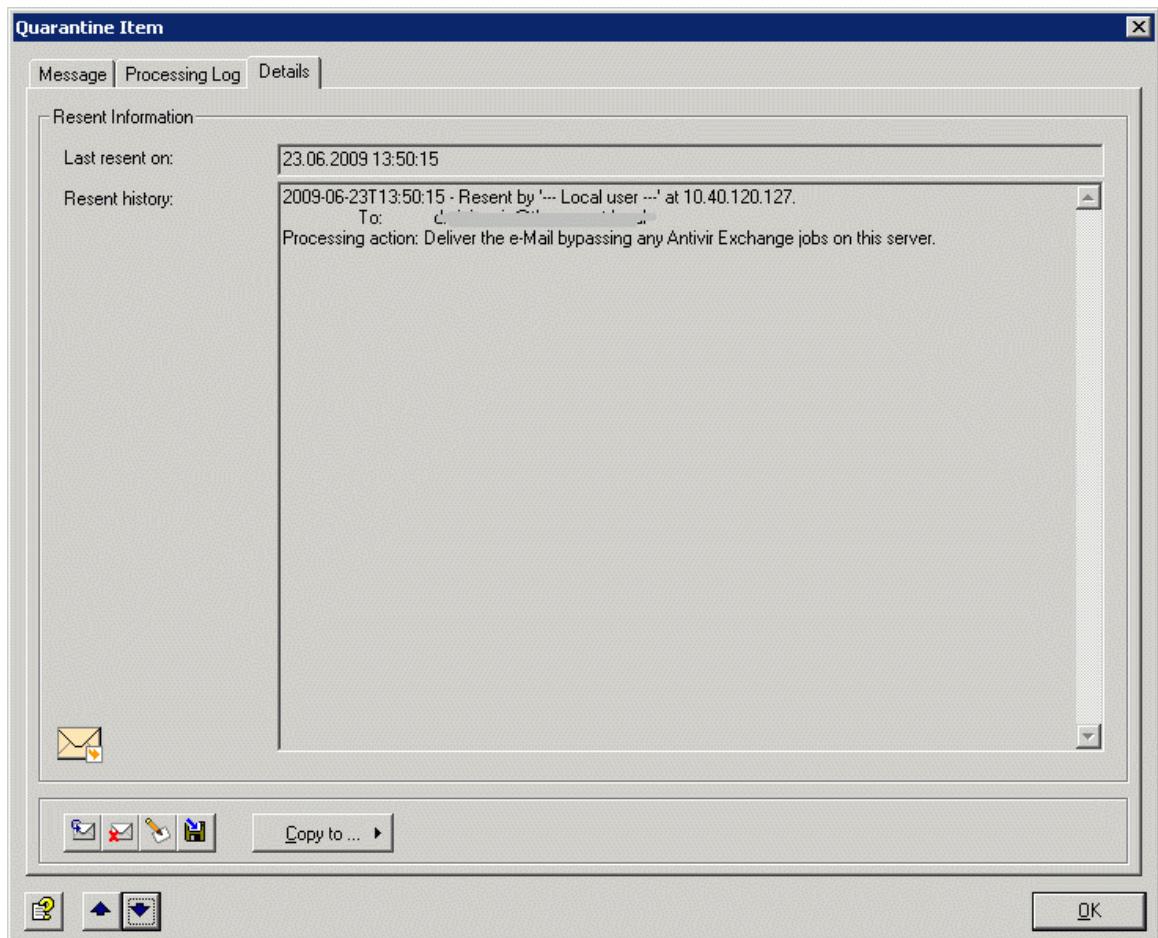


The name of the job that placed the email in quarantine, the job type, the server, information as to why the email fell under restrictions and was placed in quarantine, and further processing details are available under **Processing Log**:



Information about the resending of the email from quarantine is available under **Details**.

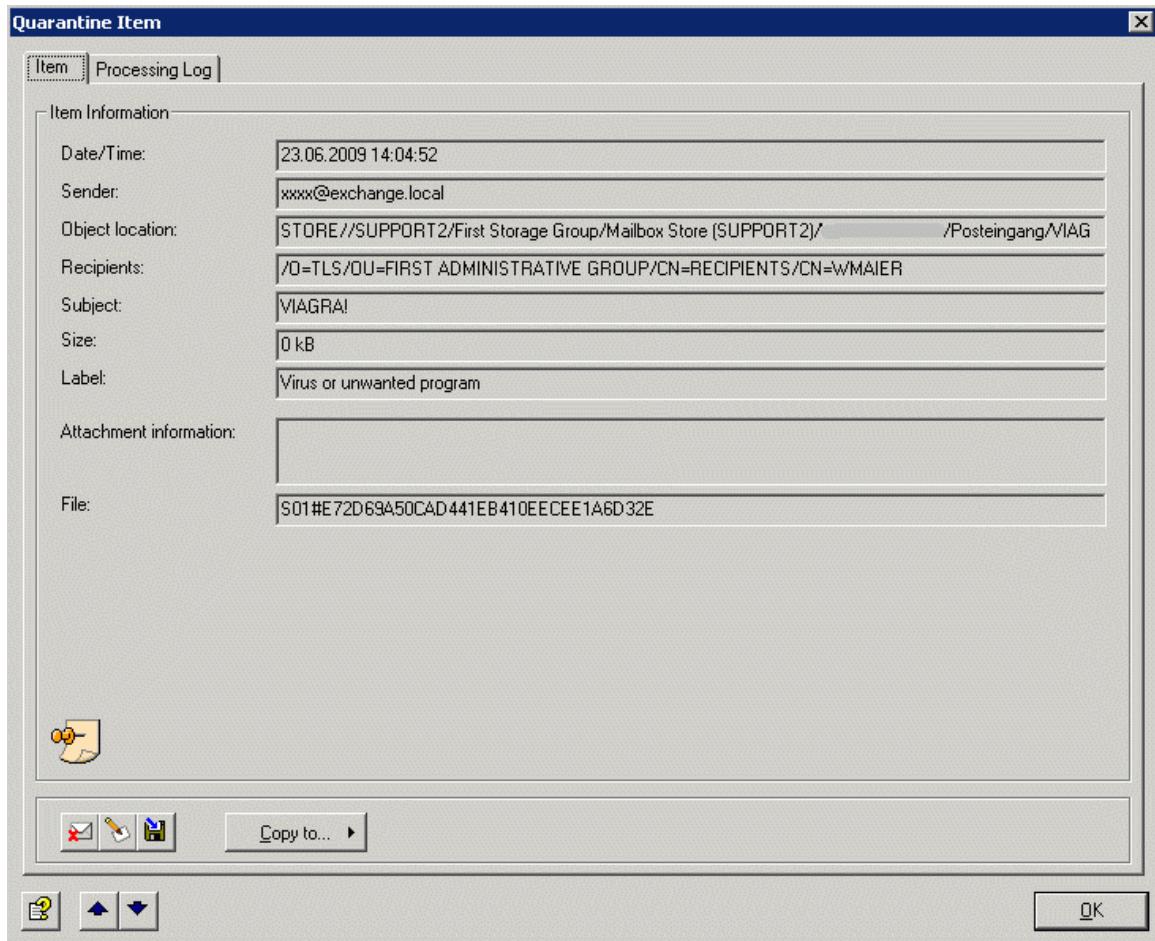
Details on the Avira AntiVir Exchange Management Console



Example of an email in the information store quarantine

You receive this information if you double-click or right-click the **properties** of the email in the information store quarantine.

The most important information can be found at a glance on the **Item** tab.



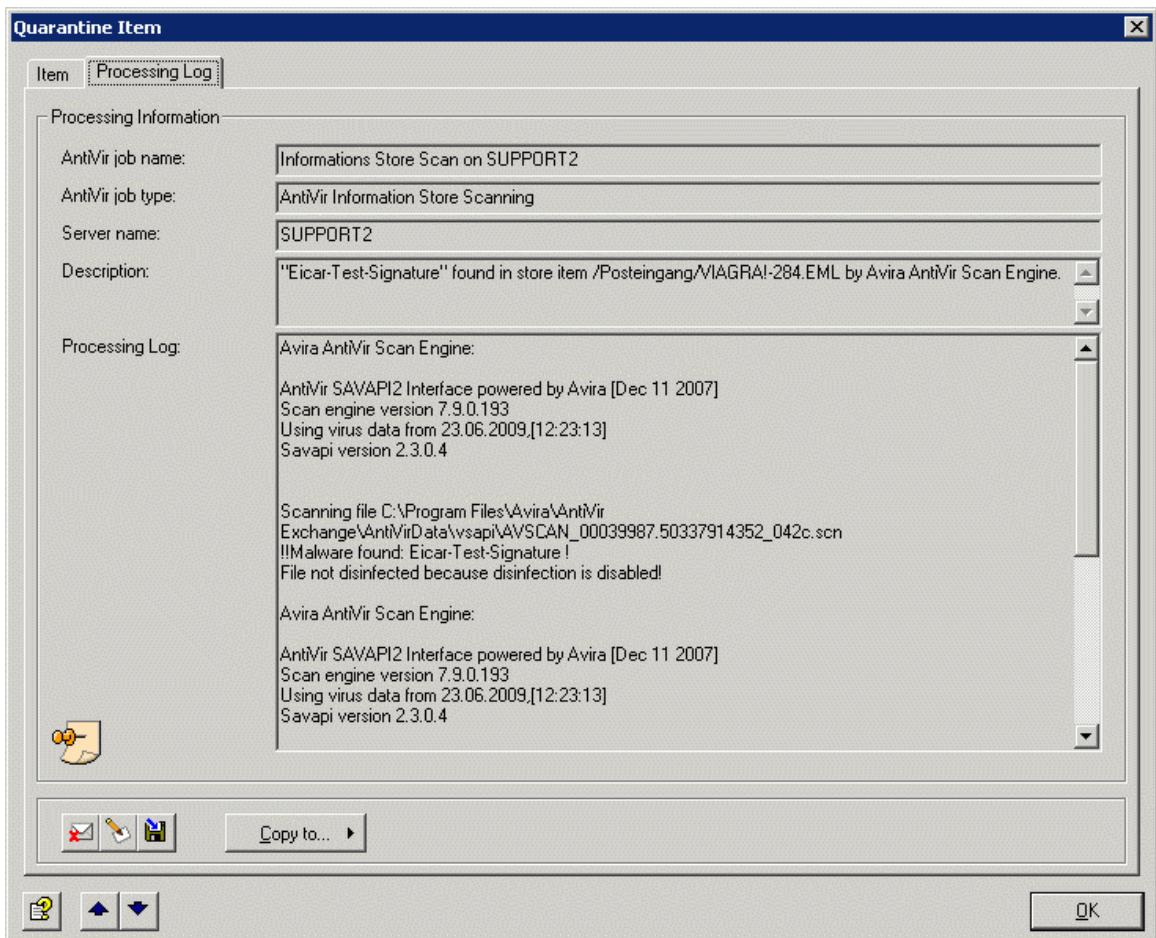
The icons used on these tabs:

	Delete item in quarantine
	Define, modify, delete the label for the item
	Save item in file system
	Next item in the quarantine
	Previous item in the quarantine

The **Copy** button allows you to copy the object to another quarantine on this server.

The next tab, **Processing Log**, shows the name of the job that placed the email in quarantine, the job type, the server, information as to why the item fell under restrictions and was placed in quarantine, and further processing details:

Details on the Avira AntiVir Exchange Management Console



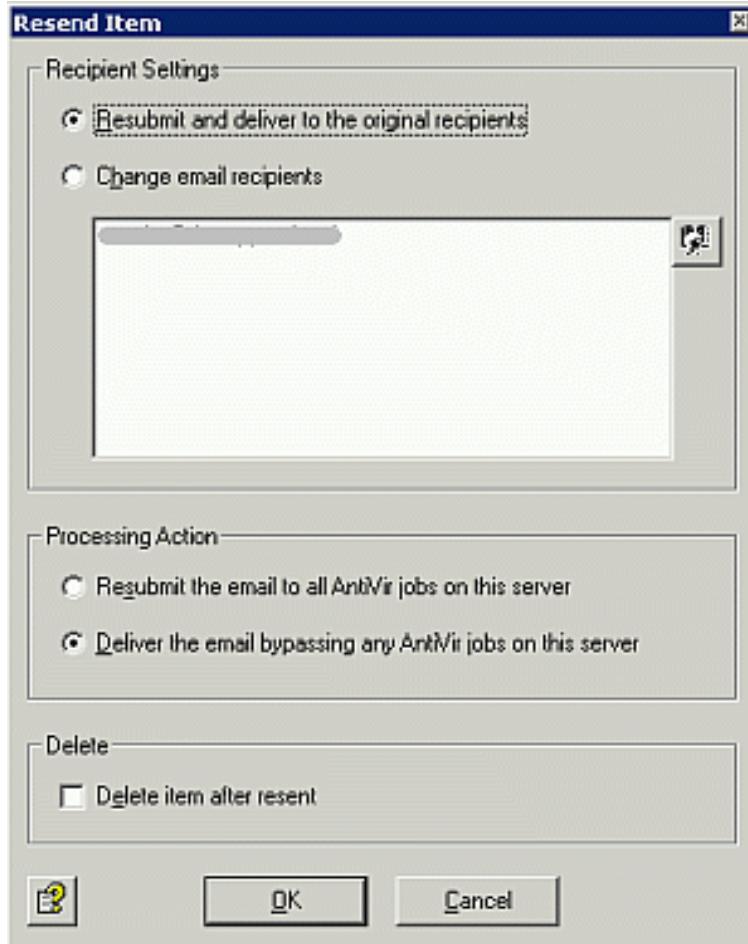
Sending emails from quarantine

If you want to have an email from quarantine delivered to its original or another recipient, you can send this directly from the quarantine without it having to be checked again by an Avira AntiVir Exchange job:

1. Open a list of emails of a quarantine in the AntiVir Monitor.
2. Right-click to select the required email and then select **All Tasks - Send from Quarantine**.

Note: Alternatively, you can also send the email directly from the Properties window by clicking the icon.

You will see the following dialog box:



The recipient sees the original sender in the "From" field of the email (i.e. not a forwarded mail).

3. You can change the recipient by enabling the **Change email recipients** option and then clicking the **Select address** icon: .

Note: When selecting addresses for the resending of emails from quarantine, no address lists are available. For more information on address lists, see [Address lists](#).

4. If you no longer want the email to be processed by the jobs, enable the **Deliver the email bypassing any AntiVir jobs on this server** option.

This will generally be the case if you want to have an email delivered from quarantine because a user urgently needs this email despite, for example, prohibited words or attachments.

Note: This is a universal setting. If you enabled jobs that are also to scan resent emails from quarantine, then set this setting to **Resubmit the email to all AntiVir jobs on this server**, as otherwise the **Check before sending** job setting will not take effect and all emails will be sent unprocessed.

Note: The **Resubmit the email to all AntiVir jobs on this server** instruction also applies only for the jobs for which the **Mails from quarantine: Check before sending** option was enabled. Even if you want to have the quarantine emails processed again, all jobs for which the **Ignore emails resent from quarantine** option is enabled are excluded.

Adding senders to an address list

If a sender's email was placed in quarantine but this sender's emails are in future to be identified as wanted, you can place the sender on one of your address lists, e.g. Antispam : Whitelist:

1. In the AntiVir Monitor, open the quarantine containing the required email.
2. Right-click to select the email and then select **All Tasks - Add sender to address list**.
3. Select the address list in which you want to include the sender.

If you want to ensure that all senders of a particular domain are to be identified as wanted and are to reach the user's mailbox, proceed according to the same principle but select the **Add mail domain to address list** option instead. In this way, if there are several email senders belonging to a mail domain, e.g. at a customer company, you do not need to enter all sender addresses individually in the address list. The address is added to the list in the form of *@samplecompany.com.

Note: In both cases, the **Allow adding addresses from quarantine** field must be enabled within the address list. Otherwise, the required sender address cannot be added to the list.

Bad mails

Bad mails are all emails that could not be processed by the AntiVir jobs, e.g. emails with formats that cannot be processed. Very little information exists about bad mails, as AntiVir could not inspect these emails. These emails may also contain an undetected virus.

There is only one folder for bad mails on each server. Also, no additional folders can be created. Apart from that, the same functions and options apply for bad mails as for quarantine mails.

4.5.2 Avira AntiVir Exchange reports

The report and statistics function in Avira AntiVir Exchange can be used to obtain detailed information about email processing.

Seven predefined statistical reports and one advanced report are available.

The extended statistical report can be defined on an individual basis. The reports can be accessed using AntiVir Monitor. The individual reports contain both the graphical presentation of detected policy violations (e.g. viruses, unwanted file attachments) as well as table information. A separate report exists that answers the most frequent questions. Data relating to AntiVir quarantines is also shown.

The reports can be produced for freely defined periods. Extensive printing and export functions allow the report data to be reused with ease.

The report data is cached during processing and is recorded in the evaluation database twice per hour. Processed emails do not generally appear immediately in the reports.

Click **AntiVir Reports** and open the required report in the right-hand window with a double-click. Enter the required period for the report in the new window that appears. Select  to export the evaluation for importing into another application; you can choose from a number of different formats.

5 AntiVir scan engine

5.1 Overview

AntiVir is used for scanning emails for viruses, for type and size of attachment and for the total email size.

5.1.1 Job types

- Virus scan of incoming and outgoing emails
Type: **AntiVir Scan**
- Virus scanning in MS Exchange databases (on access & proactive/background)
Type: **Information store scan**
- Blocking of specific file types in the attachment
Type: **AntiVir Attachment Filtering**
- Restriction of the email size
Type: **AntiVir Email Size Filtering**
- Restriction of type and/or size of attachments
Type: **AntiVir Attachment/Size Filtering**

Note: Create a separate job for every restriction type. The job types cannot be changed later.

For the exact procedure, please see the descriptions in [Activating virus scanning - sample job](#).

5.2 AntiVir Scan

You can configure the virus scanner under **Basic Configuration - Utility Settings - AntiVir Engine - Avira AntiVir Scan Engine - Properties**.

The **AntiVir Scan** job starts the virus scanner in accordance with the configured conditions. The conditions determine the emails for which a job is executed.

The following example illustrates how a virus scanning job works: The job scans an email with the result: Virus found. This triggers a virus alarm and a series of actions is started, which you can define yourself under **Actions** in the job.

You can define the following, for example:

1. If a virus is found, the original mail should be cleaned and then delivered to the recipient.
2. If the original mail cannot be cleaned, the affected email is copied to the folder selected by you (quarantine), the original is deleted and not delivered.
3. In this case, messages are sent to the administrator, sender and recipient. These messages contain the relevant information regarding the virus scanner and the AntiVir job.

The following actions are possible:

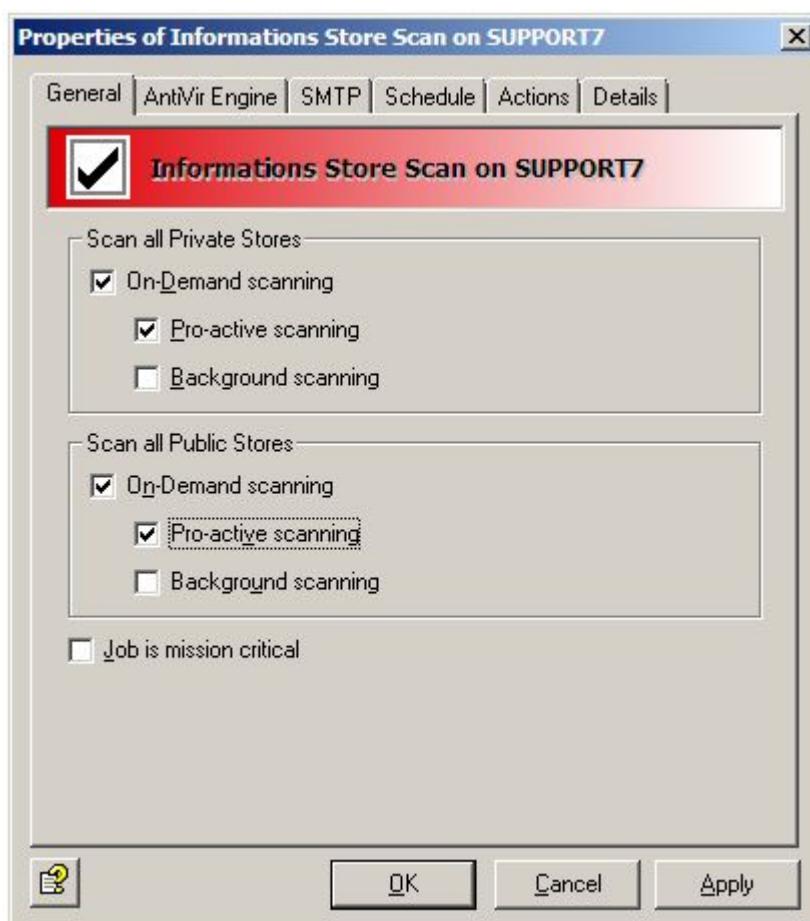
- Scan for viruses
- Remove viruses
- Subject extension

- Copy entire email to quarantine
- Remove affected attachments from the email
- Delete and do not deliver the affected email
- Run an external application
- Notify administrator, sender, and/or recipient
- Notify other freely selected persons
- Add X-header field
- Redirect email

5.3 Information store scan

In addition to the virus scan on transport level, Avira AntiVir Exchange can also scan data in the public or private information store of MS Exchange. This scan does not refer to the incoming or outgoing mail traffic, but instead to the mail files on the server or those that do not come into contact or have not come into contact with the transport agent, e.g. drafts.

Three main areas are covered with the information store scan:



- **On-demand scan**

If a client attempts to open a message, a comparison is carried out to ensure that the text body and the attachment were scanned by the current virus signature file. If the content was not scanned using the current virus signature file, the corresponding message component is sent to the virus scanner before being forwarded to the client. The on-demand scan is the most frequently selected option in the information store scan.

- **Proactive scan**

The proactive scan checks new incoming messages before access to a client via the on-demand scan takes place. The proactive scan is an addition to the on-demand scan that can ensure faster client access.

- **Background scan**

With the background scan, a complete scan of all elements of the information store can be started. This scan can be enabled separately for the public and private information store. All elements that have not yet been scanned with the current virus scanner signature file are included.

In addition to the scheduled scan, the background scan is also always executed when the databases are being loaded (e.g. when the server is started).

The settings for the information store scan are server-wide. That is why there is always only one information store scan job available for each server, and not any number like for AntiVir virus scanning.

If a virus is found in a message, various actions that are specially tailored for the information store scan can be carried out:

- **Block object:** Blocking prevents access to the entire message object. With current Microsoft email clients, a corresponding error message is displayed when an attempt is made to open such an e-mail message. With other/older email clients, there may be different feedback. However, the blocked messages can always be deleted via the client.
- **Replace with:** Replacement replaces the infected element of the message (e.g. file attachment) with a text comment. The infected element is deleted.
- **Mark as not infected:** In exceptional cases, it can be decided that the corresponding element is not to be marked as infected when a virus is found. Subsequent virus checks will again identify the element as infected. This action is only useful in test environments, as the user is not protected.

Note: The virus scan of the MS Exchange information store takes place using Microsoft Virus Scanning API 2.0/2.5. For further information, see <http://support.microsoft.com/kb/285667/EN/>

Warning: For messages that are blocked by the information store scan, there may be error messages during data back-ups of the information store.

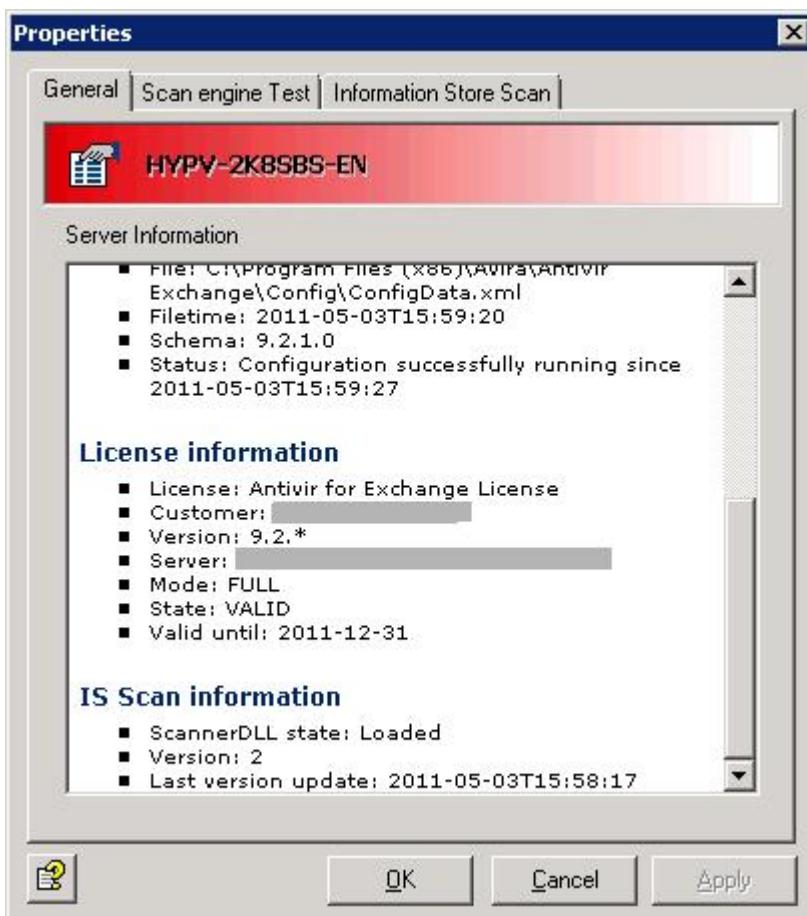
Warning: Exiting or uninstalling Avira AntiVir Exchange, as well as stopping the information store scan jobs, not only disables the active virus protection of the information store but also removes the blocking of infected content mentioned above.

5.3.1 Status of the information store

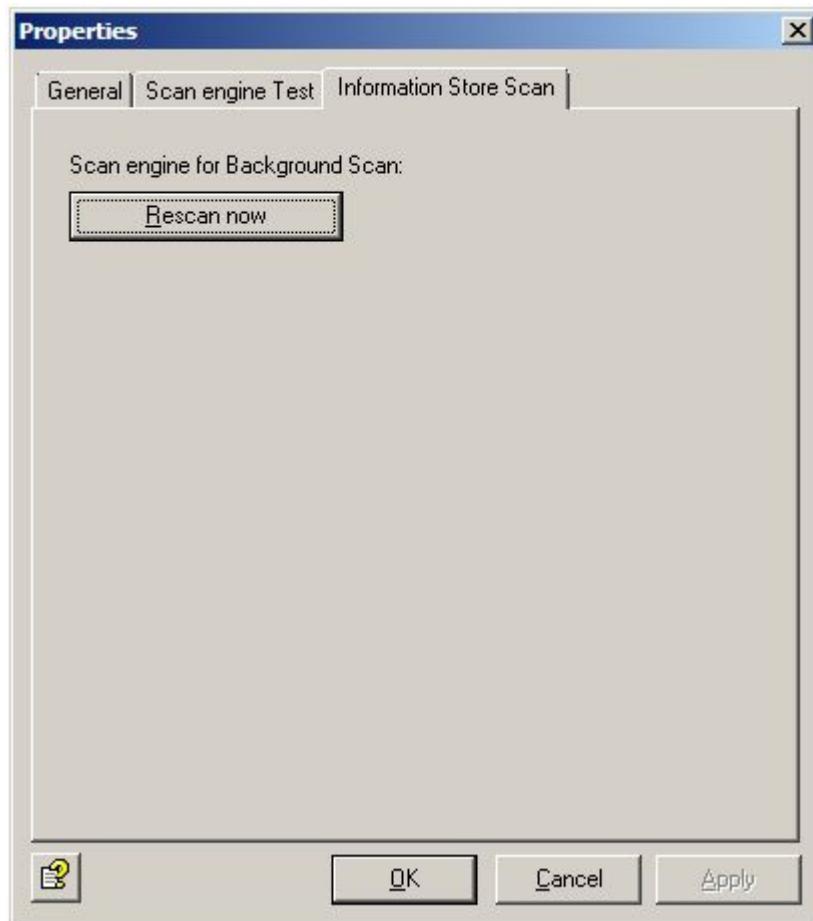
Click **AntiVir Monitor - Server - Server Status**. There you will find both the current status of the information store scans and the option for a manual restart.

If you click the **General** tab, you will see:

- whether the scanner DLL for the information store scan is loaded. As soon as the DLL shows Loaded, the information store scan is activated.
- the version of the information store scan. Each restart increases this value.
- when the last version update occurred and the time and date of the last restart.



Click the **Information store scan** tab. There you have the option of restarting the background scan.



Warning: When you restart the scan, all elements in the information store are scanned again. This applies to all three scan modes. If you have enabled the background scan, this scan can be very time and resource-intensive. It is therefore recommended that you restart at off-peak times and depending on the virus scanner update.

5.3.2 Virus scan in the information store - sample job

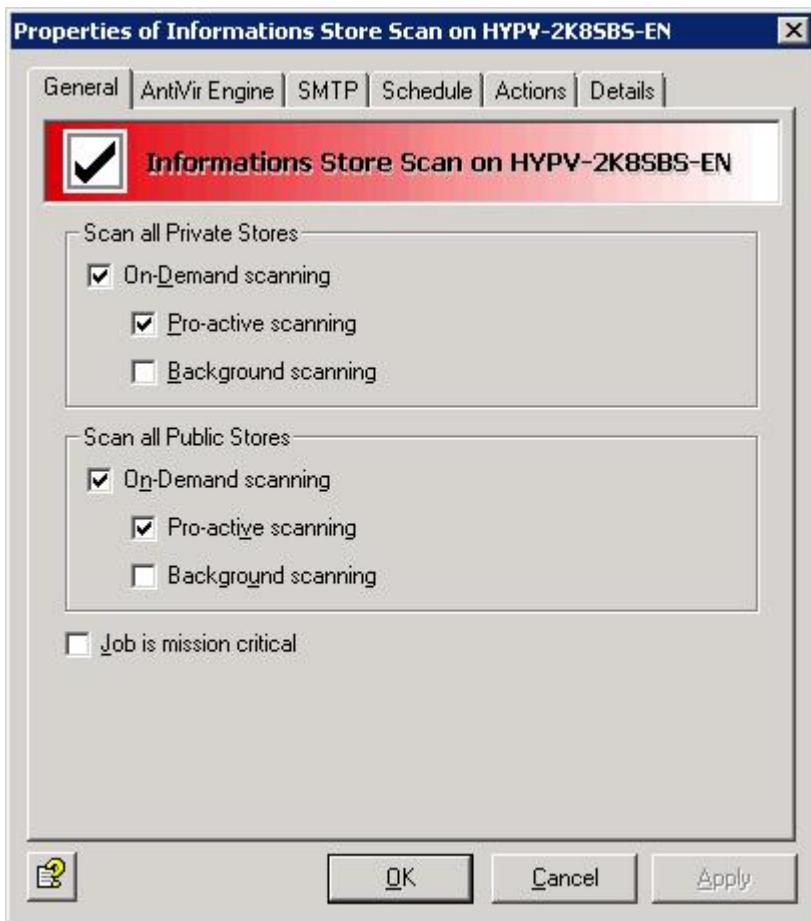
In the Information Store Jobs section under **Policy Configuration**, you will find an **Information Store Scan** per server. Open this job with a double-click.

Warning: When you enable/disable the information store scan job, it can take up to two minutes before the Exchange Store registers the change.

General settings

On the **General** tab, you can enable the on-demand scan for both the private and the public information store.

In addition to the on-demand scan, you can also enable the proactive scan and the background scan. For further information, see [Information store scan](#).

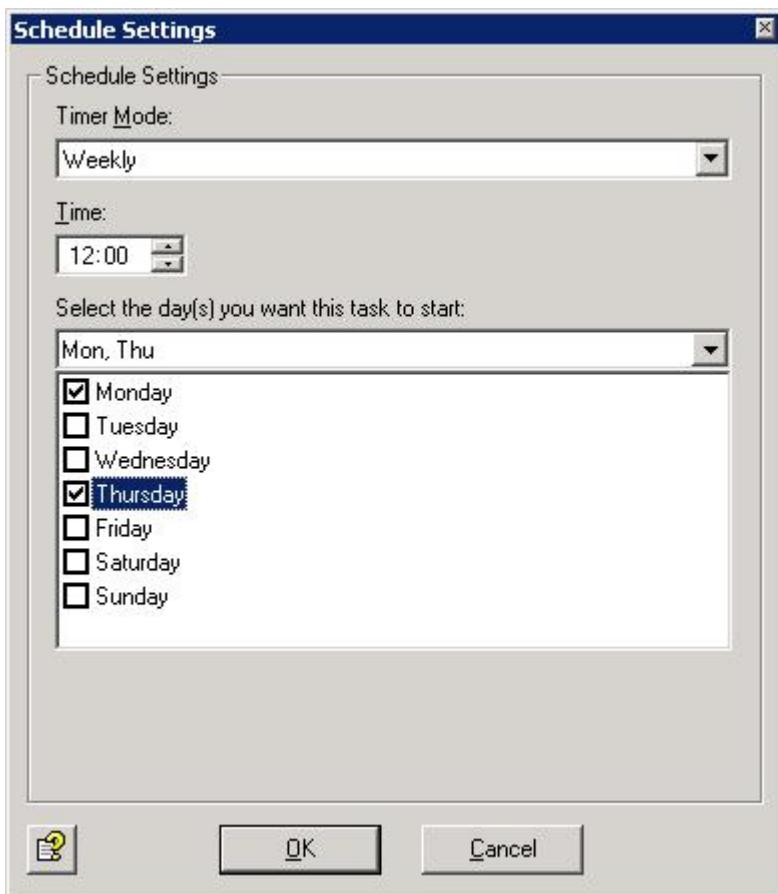


The mission critical option is explained in more detail in **Job is mission critical**.

Defining a schedule

You can create a schedule for restarting of the scan on the **Schedule** tab. When you restart the scans, all elements in the information store are scanned again. This applies to all three scan modes. If you have enabled the background scan, this scan can be very time and resource-intensive. It is therefore recommended that you restart at off-peak times and depending on the virus scanner update.

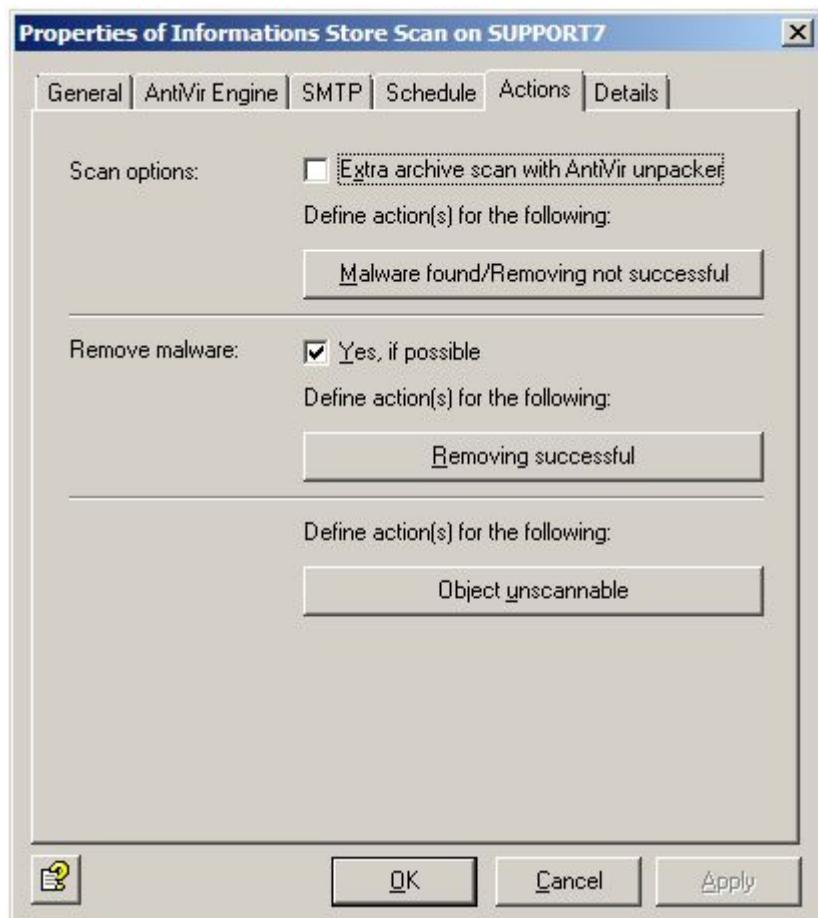
Click **Add** to create an entry in the schedule. Then select the start time and the days on which the restart is to be executed. The selection is added to the schedule when you click **OK**:



Defining actions

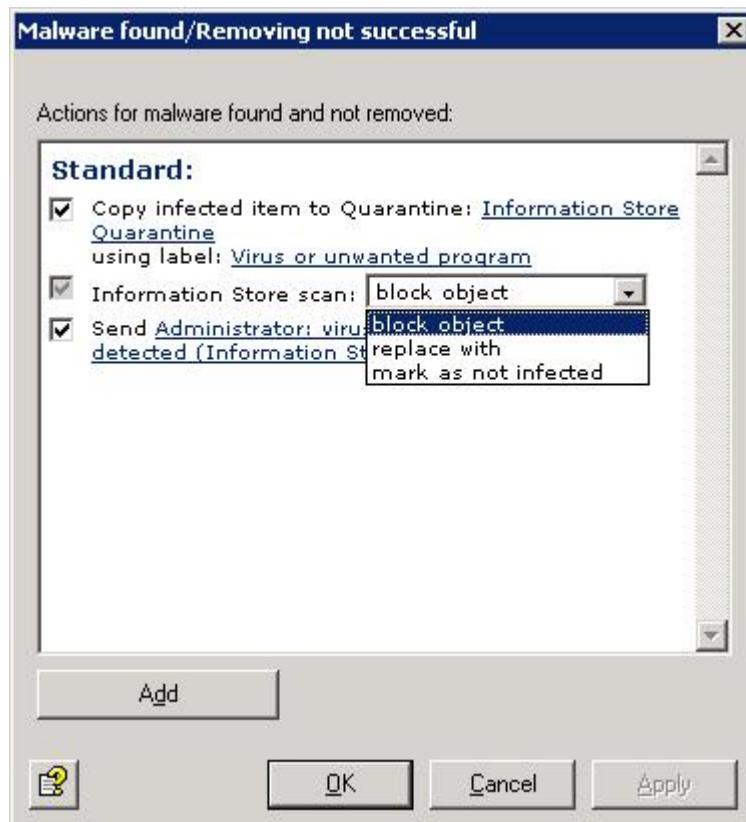
The **Actions** tab is used to define which actions are to be carried out when the job has found an infected mail.

Extra archive scan with AntiVir unpacker: Enable this option if you are using the virus scanner of another manufacturer and, unlike Avira products, this scanner does not have an integrated unpacker. When this option is enabled, an internal unpacker firstly extracts the packed files and then sends them individually to the virus scanner.



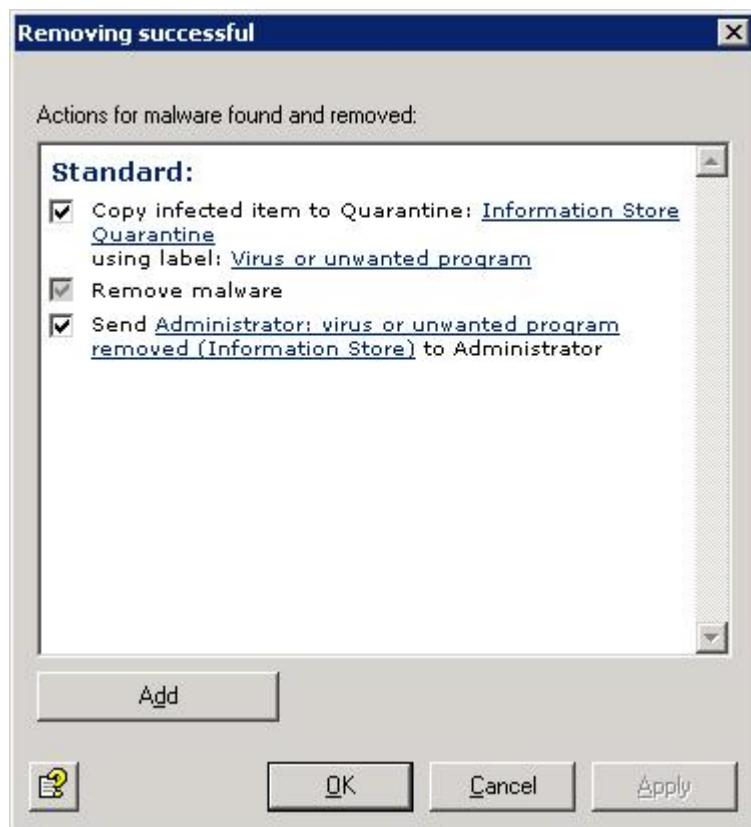
Three different actions are possible:

- A. **Malware found/Removing not successful:** Handles the case whereby a virus was found and the file could not be successfully cleaned.



- a. Firstly select whether a copy of the object is to be placed in a quarantine and labeled. A special default quarantine is available for the information store scan.
- b. The second option gives you the choice of blocking, replacing or ignoring/not marking the object. See also [**Information store scan**](#).
- c. Use the last default option to select whether a notification is to be sent to the administrator(s).
- d. You can use the **Add** button to select additional actions. In this way, it is possible, for example, to send notifications to any recipients or to start an external application.

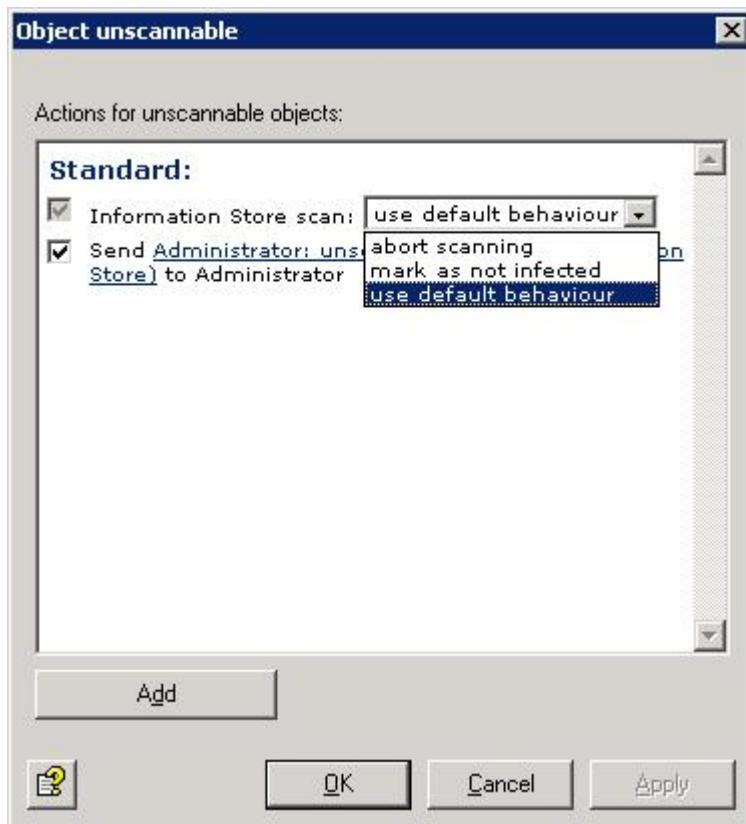
- B. **Removing successful:** Handles the case whereby the file was successfully cleaned and the virus was removed.



The following actions can be defined here:

- a. With the first option, select whether a copy of the object is to be placed in a quarantine and labeled. The copy is created before the object is cleaned, which means that the object is in its original state in the quarantine.
- b. In addition, you can choose whether a notification is to be sent to the administrator(s).

- C. **Object unscannable:** Handles the case whereby the files could not be scanned. This allows you to influence the behavior of Avira AntiVir Exchange when encrypted objects are found, which due to their nature cannot be viewed and therefore cannot be scanned for viruses.



Two options are available to you here. The first concerns the action of the information store scan:

- Abort scanning:** The object is scanned again during the next scan process. Access to this option is blocked if previous scan processes handled the object as virus-free.
- Mark as not infected:** The object is handled as if it were virus-free. It is only scanned again the next time the virus scan is restarted.
- Use default behaviour:** The object is handled according to the settings for **When e-mail is unscannable, then...** under **Basic Configuration - AntiVir Server - General**.

The second option concerns the possibility of sending a notification to the administrator as well as executing additional actions using **Add**.

Job details

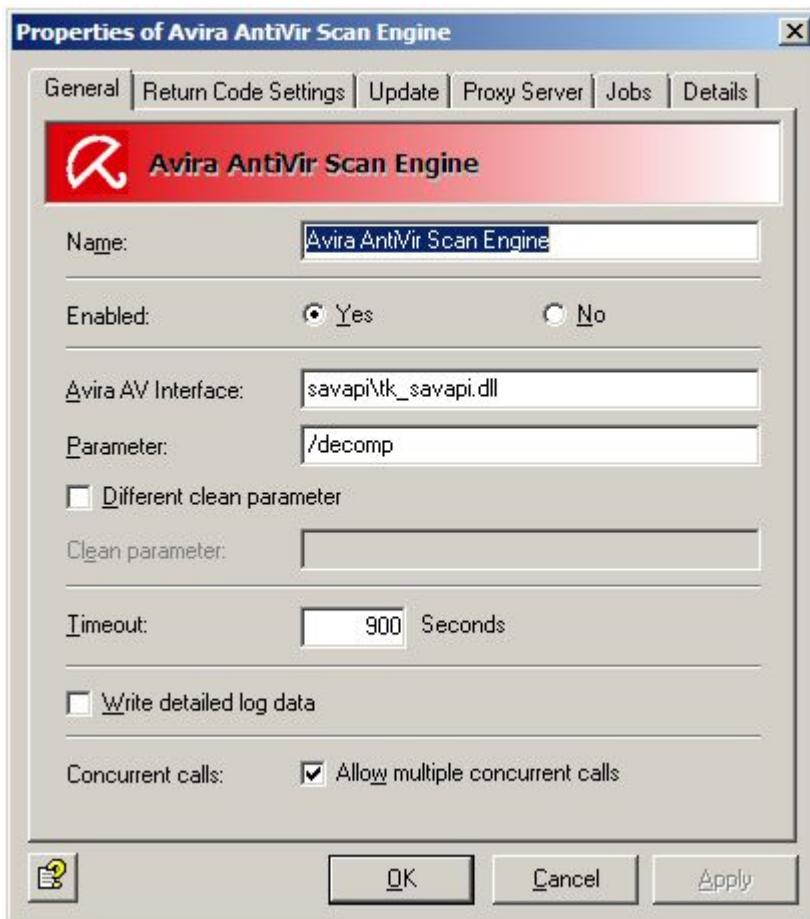
You can describe the job in more detail on the last tab entitled **Details**.

5.4 Configuring and enabling the AntiVir Scan Engine

Avira AntiVir Exchange accesses the virus scanner by means of the so-called **Avira AV Interface** - a DLL file.

Warning: You must disable any real-time or on-access scan functions of the virus scanners used for the directory ... \Avira\AntiVir Exchange\AntiVirData\

Test that your virus scanner is working correctly: Mark the required server name under **AntiVir Monitor** and click **Server Status** in the right-hand window. Under the **Search Engine Test** tab select **Virus Scanner Test**. If the test is successful you will get an OK and a message indicating that an EICAR test virus has been found.



You can configure AntiVir under **Basic Configuration - Utility Settings - AntiVir Engine - Avira AntiVir Scan Engine - Properties**.

- The name of the Avira Interface DLL must be entered in the **Avira AV Interface** field. This DLL file is the connection between Avira AntiVir Exchange and the virus scanner. This entry is preconfigured for every virus scanner and cannot be changed! In the next field specify the **parameter** to be used by the virus scanner to scan for viruses.
- To set the virus scanner so that emails or attachments are cleaned when a virus is found, enable the **Different clean parameter** field and specify the associated parameter in the subsequent **Clean parameter** field.

Note: The corresponding clean parameters can be obtained by email or telephone from the Support team.

Note: If you only want to use the virus scanner to scan for viruses, use the **Scan with AntiVir Engine** job. The **Remove Virus** field must be disabled in the **Actions** tab. If the virus scanner is also to be used to remove any viruses found, use the **Scan and Remove with AntiVir Engine** job. In this case, the aforementioned field must be enabled and the required actions in the event of a virus must be defined.

- **Timeout:**

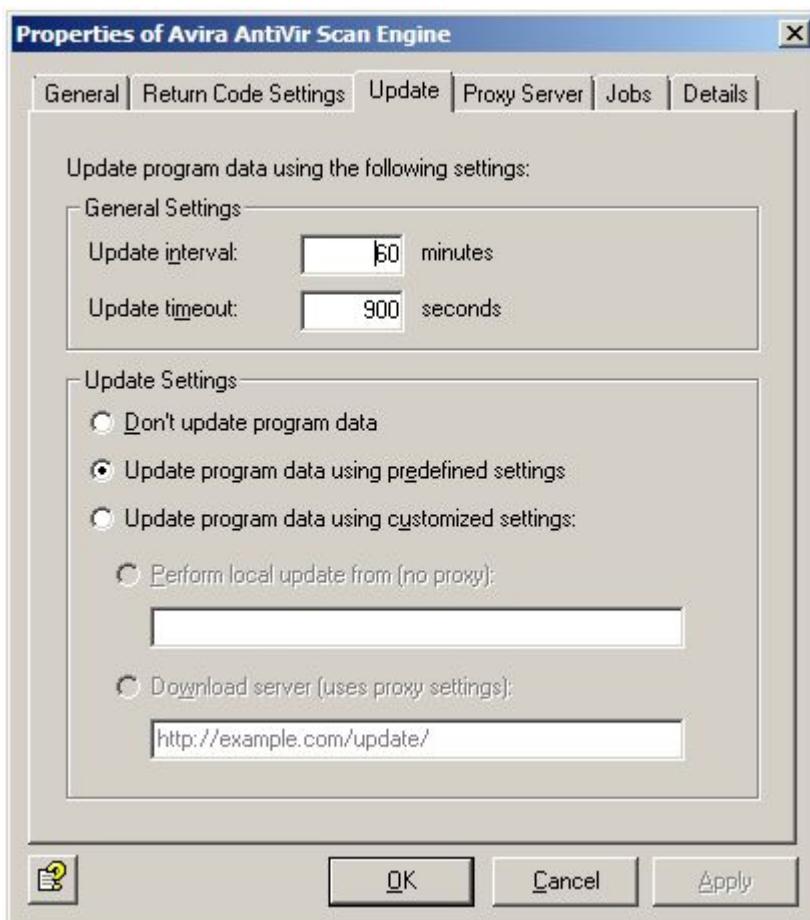
Specify the number of seconds after which an attempt to connect to the server is to be canceled (if the connection has not been established by then). When specifying a time, please consider the performance of your server. Minimum value: 60 seconds.

- **Allow multiple concurrent calls:**

means that several emails can be processed by this virus scanner at the same time. The number of calls is defined in **AntiVir Server - Properties - General tab: Number of threads**. See also the settings for an individual Avira AntiVir Exchange Server.

The preconfigured return codes can be processed in the **Return codes** tab. The **Details** tab indicates the meaning of the individual codes.

Update tab: The virus scanner has a mechanism that enables the latest patterns to be loaded from the Internet.



Update pattern database: Enable this switch.

- **Parameter:** This field specifies the directory in which the updated virus patterns are saved and contains a default setting (default: *Update\Extract*).
- **Interval:** Interval in minutes at which pattern update scanning takes place. Minimum value: 15 minutes.

- **Timeout:** The update procedure will be canceled after this time. Minimum value: 60 seconds.

You can use a **proxy server** to update the virus pattern. Select the required proxy server in the Proxy Server tab. To create a new proxy server, see the "Using proxy servers" section under [Settings for an individual AntiVir server](#).

The **Jobs** tab shows the jobs in which the virus scanner is incorporated.

Warning: To update Avira AntiVir Exchange please do not use this tab, but rather select the **Virus Scanner/Anti-spam Update** option on the **Search Engine Test** tab and click **Start**. After the update you will receive a detailed update report.

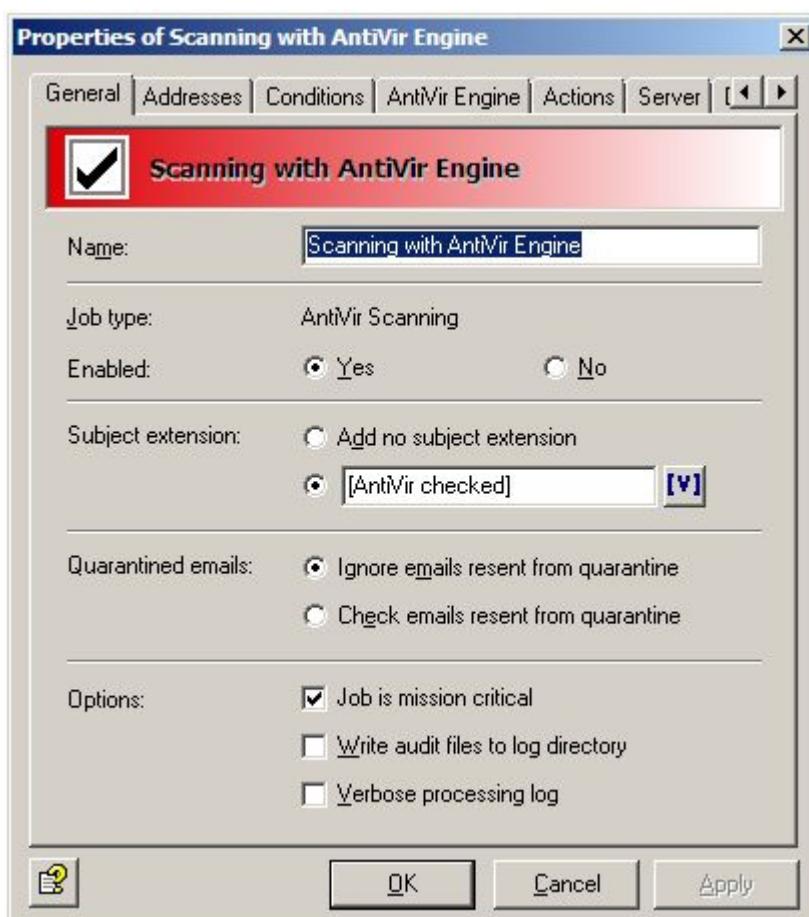
The **Details** tab contains a description of the default return values. If you make changes to the **Return Codes** tab, we recommend documenting these changes on the **Details** tab.

5.5 Activating virus scanning - sample job

In **Policy Configuration - Mail Transport Jobs**, you will find the job **Scan with AntiVir Scan Engine**. Open this job with a double-click.

5.5.1 General settings

You can assign a name of your own to the job on the **General** tab. Set the job to **Active**. The job is enabled as soon as you save your settings with **OK** and close the job. The check mark in the job icon immediately tells you the job is enabled.



The default for the **Subject extension** is **AntiVir checked**. This additional text is added to the subject line of every email checked by the job.

This job also processes emails sent from quarantine once again. The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend a mail with the **Quarantine Send** option **Deliver the email bypassing any AntiVir jobs on this server**, the mail will not be processed by any job. For this reason, when sending emails from quarantine, you should set the Send option to **Resubmit the email to all AntiVir jobs on this server**.

For more information about resending emails from Quarantine see [Sending emails from Quarantine](#).

5.5.2 Job is mission critical

A job is **mission critical** if the email is to be placed in the bad mail area in the event of a processing error, e.g. if the virus scanner is not found. Select this option for mission-critical jobs such as virus scans (place a checkmark in the box).

Warning: When this option is set, **every** email (incoming or outgoing) is transferred to the bad mail area for as long as the processing error is not fixed.

A job is **not mission critical** if the result of the job is to be ignored for the email in question if a processing error occurs. In this case, the email is transferred to the next job for processing. Every processing error is entered in the Windows Event Log. If the processing error occurs five times successively, the job is disabled. The disabled job is restarted automatically after 15 minutes. Select this option for jobs that are not mission critical.

The default setting for nearly all jobs is **not mission critical**. Which jobs are to be considered mission critical should be determined in the company policies.

Keeping a log of the processing

You use the processing log to observe the processing of the emails by the job. Activate this function if an obligation to produce verification may occur or if you want to test a job.

When you set the checkmark for this option, information as to whether and how the job processed the respective email is written to a text file for every email processed. This log text file is stored in the Log folder in the Avira AntiVir Exchange installation directory. The log is defined per job but the text file contains information on all jobs for which the **Write processing log** option is enabled. An extra text file is created for each day.

Name of the text file: *Audit_all_<Date of last change>.log*, e.g. *Audit_all_20050909.log*

The individual items of information regarding the processed email are separated by semicolons and can therefore be evaluated manually or automatically:

1. Date and time the email was processed.
2. Job ID
3. Job name
4. Message ID
5. SMTP sender
6. SMTP recipient
7. Result of the scan by Avira AntiVir Exchange
 - Restricted - email matches the defined restrictions
 - Restricted - email does not match the defined restrictions

Recipient groups are broken down. A separate line is written to the file for each recipient.

5.5.3 Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself. For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

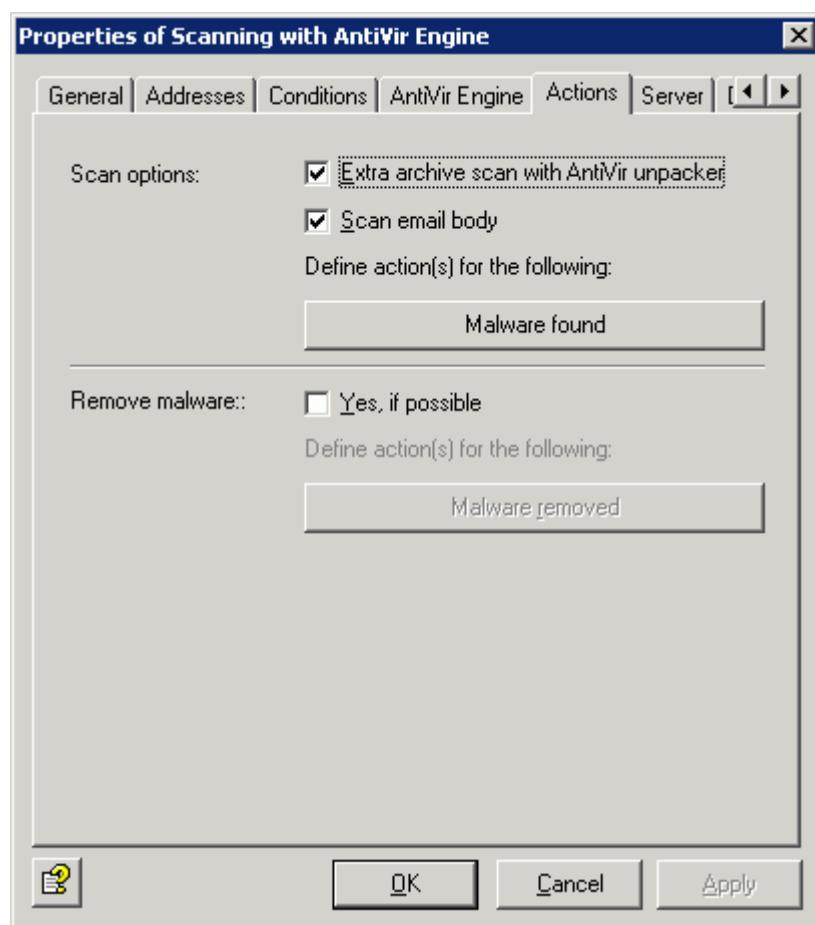
5.5.4 Setting content conditions

You can use the **Conditions** tab to set the conditions for executing a job. For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

5.5.5 Defining actions

The **Actions** tab is used to define which actions are to be carried out **when the job has found a virulent email**:



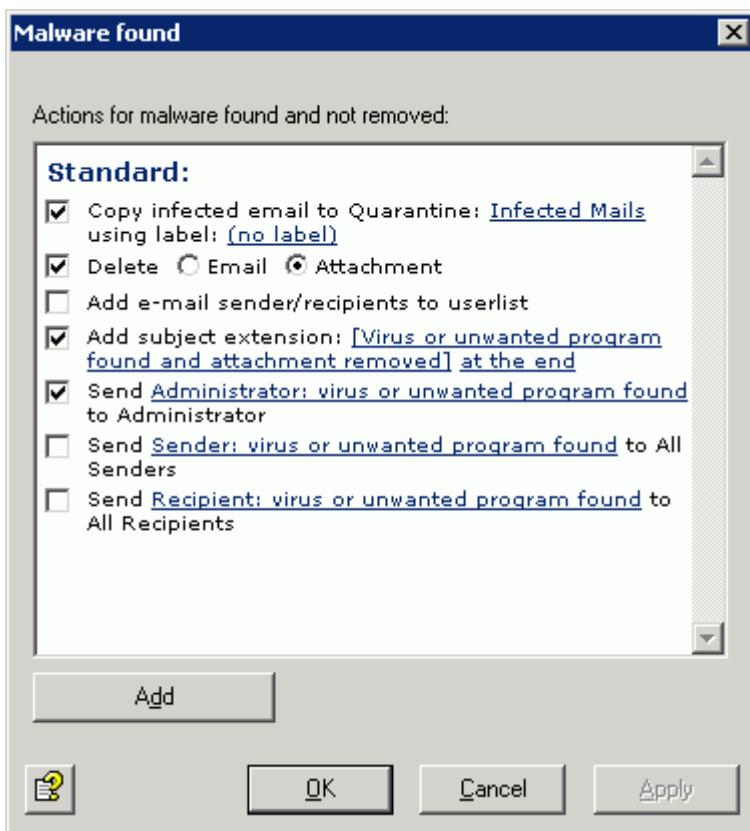
This job should scan the email for viruses but not attempt to clean the viruses from the email or attachment. All virus scanners are generally able to clean viruses. However, as it rarely happens in practice that known communication partners accidentally send viruses to one another (the viruses mostly originate from spam that contains viruses), it is more effective to place attachments with viruses into quarantine.

Note: As the job should only carry out one virus scan, you need to configure the AntiVir Scan Engine accordingly. In **Basic Configuration - Utility Settings - AntiVir Engine**, select the required engine and disable the **Different clean parameter** field. Enable this field if the job is to clean the email or the attachment if a virus is found.

Once you have defined what exactly is to be scanned, define two different actions:

1. For the event that a virus was found and the file could not be successfully cleaned.
2. For the event that the file was successfully cleaned and the virus was removed (if you selected this option).

The configuration of the actions is the same in both cases. The following example refers to the first case:

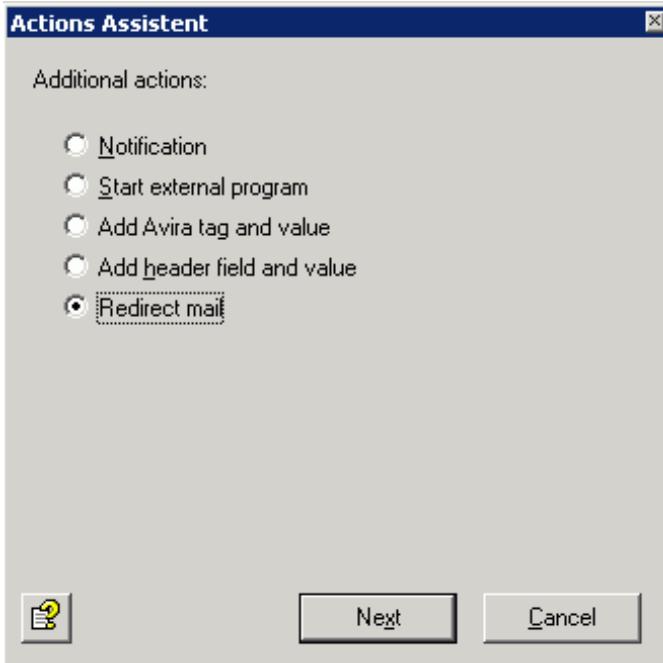


A copy of the email is placed in quarantine and the relevant attachments are deleted. Here, the email is only delivered to the recipient if the message text was virus-free and the attachment could be deleted. A notification regarding the virus is sent to the administrator. This notification is selected from the pull-down list of possible notifications; the list can be organized individually with the HTML toolbar or directly with HTML format commands.

Note: Check whether virus mails sent to your company are frequently also spam. If this is the case, it is best to immediately delete the entire email and not only the attachment. In this way, there is no need to also check the remainder of the message texts for spam.

Note: If you enabled the **Scan for viruses: Body** option and a virus is actually found in the text, the entire email, including the attachments, is deleted if the **Delete attachment** option was set (an attachment is not delivered without the message text). The email section affected is generally deleted individually. If only the attachment was virulent, then it is only the attachment that is deleted.

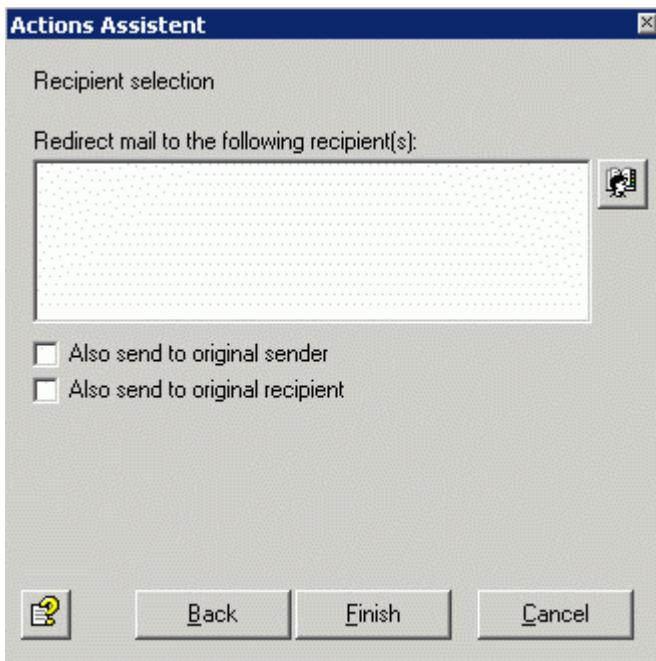
Click the **Add** button if you want to define further actions:



- **Notification:** Select the recipient of the notification from the address book.
- **Start external program:** A new program/application can be defined to have the actions of this application executed. To start an external application, specify the path and, if applicable, the necessary parameters.
- **Add Avira tag and value:** Mail header tags can be set during the Avira AntiVir Exchange processing process so that special Avira AntiVir Exchange actions can be executed. For example, additional details to be evaluated by a subsequent job can be added to an email. When the email is sent to the original recipient, the mail header tags are removed.
- **Add header field and value:** Define a new X-header field and select the variable to be inserted in order, for example, to output the result of a spam analysis as a value. Unlike the mail header tag, this information remains even when the email is sent to the original recipient.
- **Redirect mail:** Select the recipient of the redirected email from the address book. Redirect mail is not set by default but is simply proposed as an additional action.

Note: Special information with regard to **Redirect mail**: If you redirect a TNEF mail to an external address, an empty email will be received, possibly with a *winmail.dat* attachment. Exchange uses the TNEF format if an Outlook user (not Outlook Express!) sends an email within an Exchange organization. This format is not used for communication via the Internet or when using other email programs.

Click **Next** and make further configurations depending on the selected option. In the case of Redirect mail, you have the following options:

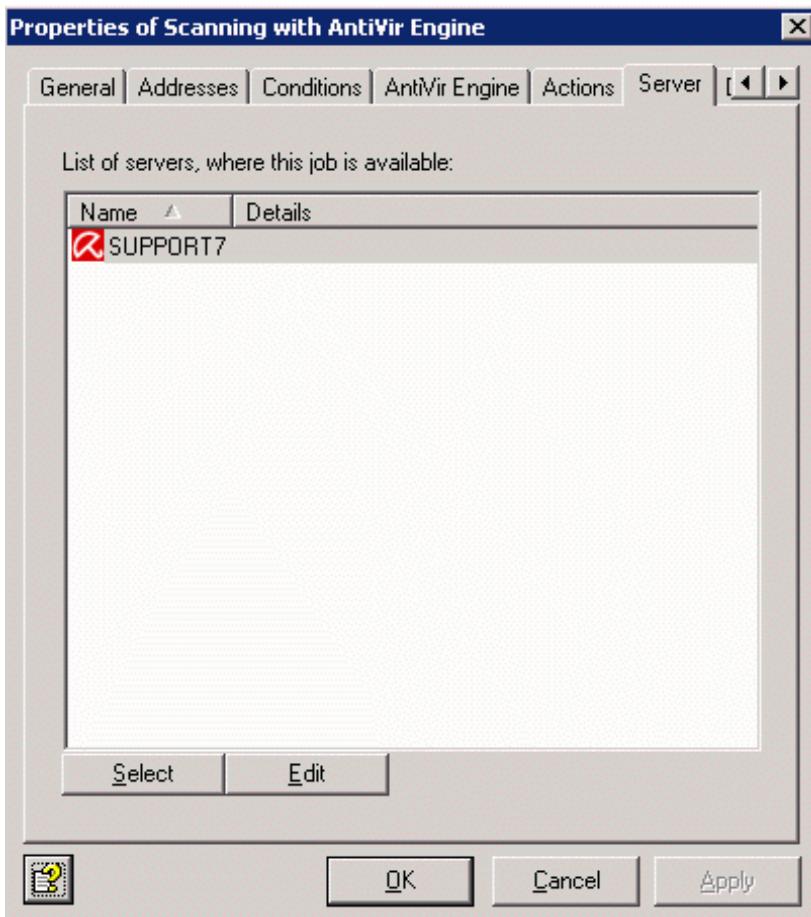


Click the address book icon  to select additional recipients or to define your own addresses. If you also want to deliver the email to the original recipient or the original sender, select the associated check box.

Click **Finish** when the recipient has been entered.

5.5.6 Selecting servers

On the **Server** tab, select the server(s) on which the job is to be active.



Click the **Select** button. A dialog box similar to the one for selecting virus scanners is displayed.

Note: The server must be configured correctly in order to appear in the selection list. For more information on the configuration of Avira AntiVir Exchange Servers, see [Settings for an individual AntiVir Exchange server](#).

5.5.7 Entering details for the job

You can describe the job in more detail on the last tab entitled **Details**.

5.5.8 Saving the configuration

Save the configuration of the Avira AntiVir Exchange Console every time you make changes. To do so, click the button. The configuration is saved in the *ConfigData.xml* file, which is stored in the *Avira\AntiVir Exchange\Config* directory. Open changes are indicated by (*) at the uppermost node.

5.6 Virus scan of password-protected archives

In order for AntiVir jobs to be able to process emails, the emails must be fully unpacked. Password-protected archives cannot be unpacked. Therefore, emails with such file attachments are by default blocked as "unscannable" by the virus scan job and are placed in the AntiVir bad mail quarantine.

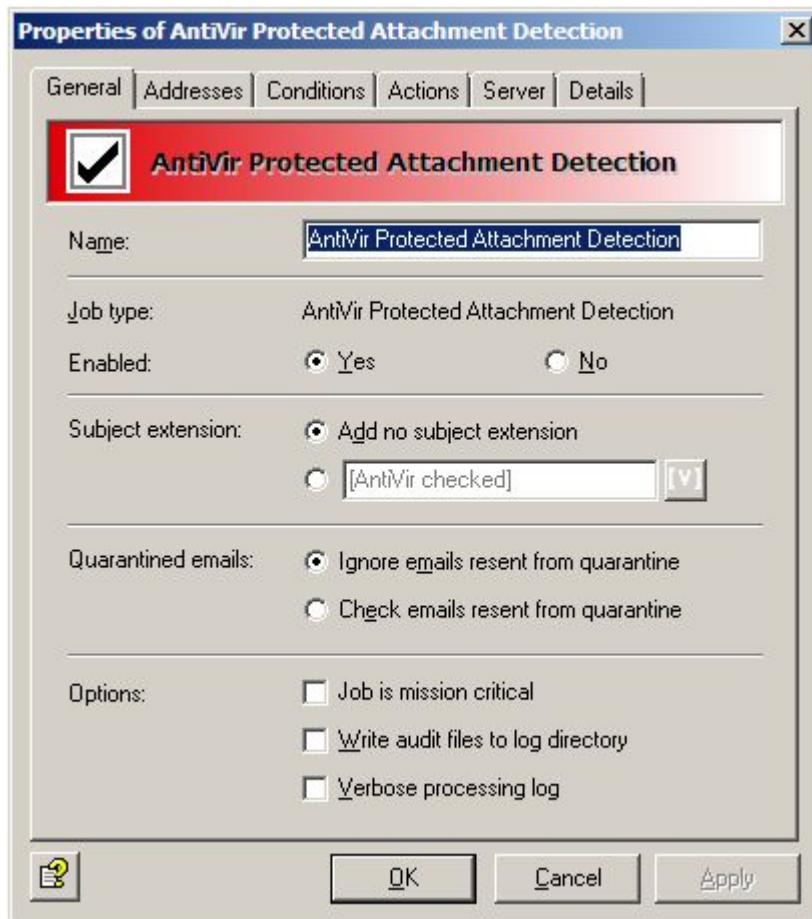
To prevent this action, use the **AntiVir Protected Attachment Detection** job. This job reacts to emails with password-protected archives and executes the job actions configured in the **Actions** tab. Password-protected archives can thus be handled in a rule-based way. For example, such emails can be blocked for certain individuals/groups but delivered to others.

As the emails would be delivered unscanned in the latter case, the emails need to be scanned by a virus scan job before delivery. The **AntiVir Scanner** job therefore marks emails that contain password-protected archives. Due to this marking, a subsequent virus scan job handles these emails as "normal" emails and can ignore processing errors (DENIED) that occur without this job.

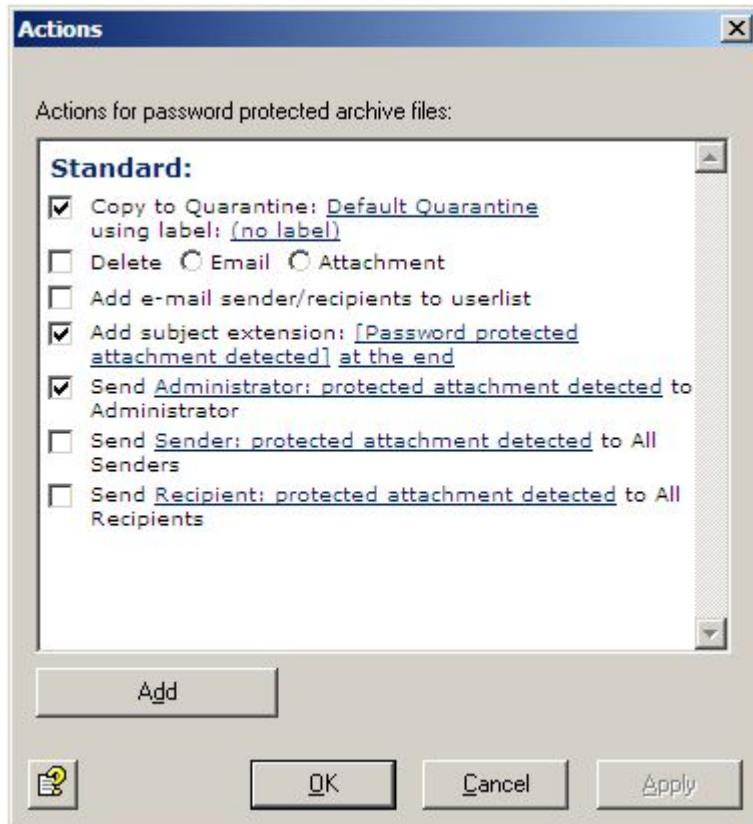
Warning: The virus scanner does not check the files contained in archives for virus infection.

5.6.1 Sample job

1. Right-click **Mail Transport Jobs**, select **New - AntiVir Protected Attachment Detection**.



2. Enable the job. In the example, only the job-specific details are explained.



3. With the default setting for the job, an extension is inserted in the subject of the email and a notification is delivered to the administrator. An email copy is stored in the standard quarantine but the email is not blocked (the **Delete email** option is disabled). Depending on the configuration, it is transferred to a subsequent virus scan job and then delivered to the recipient.
4. If emails are blocked and are not to be delivered to the recipients, enable the **Delete email** option. The email remains in the default quarantine until it is checked and released by the administrator.

5.7 File restrictions for the attachment

Files can be restricted according to the type and size criteria. To begin with, certain types of files cannot be permitted. You can also define the maximum size of an email and the maximum size of email attachments. The attachment size and type can also be checked in a shared job.

5.7.1 By type

The file must be identified by AntiVir. For this, the fingerprint of the file is checked. The fingerprint contains the binary file pattern, e.g. for *.exe files and/or the file extension, e.g. for *.vbs files.

The result of this check is compared with the prohibited/permited fingerprints under AntiVir restrictions and is excluded or admitted accordingly. The actions from the job are then executed for rejected files, e.g. in the case of an email with a prohibited attachment:

- The prohibited attachment is copied to quarantine.
- The message text is delivered to the recipient.
- Notifications are sent to the administrator and the sender.

The following actions are possible for an **AntiVir Attachment Filtering** job:

- Place entire email in quarantine
- Remove affected attachments from the email
- Delete and do not deliver the affected email
- Add sender or recipient to whitelist
- Subject extension
- Notify administrator
- Notify sender
- Notify recipient
- Notify other freely selected persons
- Run an external application
- Add Avira header field
- Add X-header field
- Redirect email

5.7.2 By email size

Emails can be analyzed and also rejected based on their total size. You can set limit per email in the **Email size** tab.

The following actions are possible for an **AntiVir Email Size Filtering** job:

- Place entire email in quarantine
- Subject extension
- Delete and do not deliver the affected email
- Add sender or recipient to whitelist
- Notify administrator, sender, recipient
- Notify other freely selected persons
- Run an external application
- Add Avira header field
- Add X-header field
- Redirect email

5.7.3 By attachment type and/or size

Emails can be analyzed and also rejected based on the size of their attachments. You can set the maximum size of an attachment per email in the **Fingerprint/Size** tab. In this job, you can also restrict the type of attachment at the same time.

The action options for an **AntiVir Attachment/Size Filtering** job are the same as for an Attachment Filtering job.

5.7.4 Configuring fingerprints

A fingerprint comprises a name pattern and/or a binary pattern.

- Name pattern: This can be used to configure fingerprints using the file name and file extension (*.exe, etc.).
- Binary pattern: This can be used to configure fingerprints using unique binary file information.

With the name pattern, manipulations are of course possible, as (if the users are aware of it) the extension can simply be changed. The binary pattern is a unique assignment to a format and cannot be manipulated so easily in the file. Therefore, the secure way to identify a file format is to enter a binary pattern.

However, with name patterns it is possible to react quickly to virus attacks:

As soon as the attachment name with which the virus is spread is known (example: Nimda virus = readme.exe), the virus attacks can be prevented even before a virus pattern update is available from the anti-virus manufacturer. The file name is simply created as a new fingerprint with the name pattern.

It is also possible to block individual files:

If a company is using customized software that generates its own file format, a fingerprint can also be created for this and it is therefore possible, for example, to prevent such files leaving the company by email. You can organize fingerprints and group them in a logical category.

A series of predefined fingerprints for standard files is automatically provided with the program. For help with creating individual fingerprints, please contact support.

5.7.5 Blocking file attachments by type - Sample job

You will find different jobs for blocking various file formats under **Policy configuration - Sample jobs**.

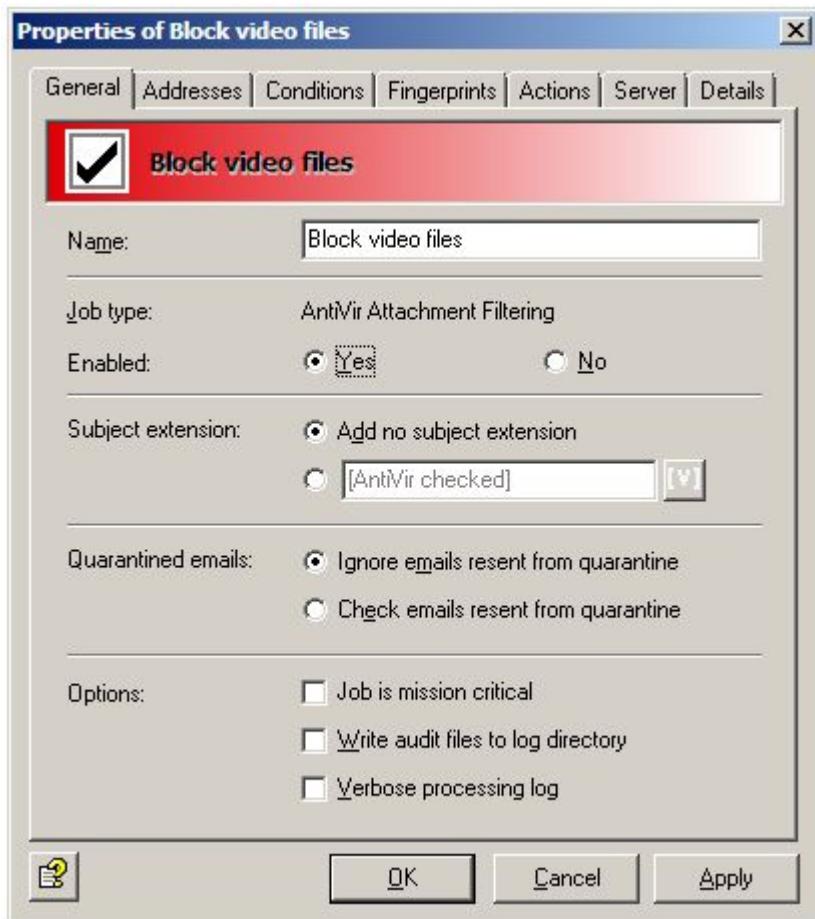
- **Block archives, except ZIP files**
All compressed formats except ZIP files
- **Block suspect attachments**
Known harmful attachments, such as Nimda, etc.
- **Block video files**
Video formats
- **Block sound files**
Sound formats
- **Block executable files**
Executable files (exe, com, etc.)

The following example is based on **Block video files**. Drag and drop this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General settings

1. You can assign a name of your own to the job on the **General** tab.
The check mark in the job icon immediately tells you the job is active.
2. **Enable** the job.

3. The job is enabled as soon as you save your settings with **OK** and close the job.



The default for the **Subject extension** is **AntiVir checked**. This extension is added to the subject line of every email scanned by the job.

This job also processes emails sent from quarantine once again. The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend a mail with the **Quarantine Send** option **Delivery without further AntiVir check on this server** the mail will not be processed by any job. For this reason, when sending emails from quarantine, you should set the Send option to **Recheck email with AntiVir jobs**.

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply.

Select all addresses from existing address lists or from lists you have created yourself.

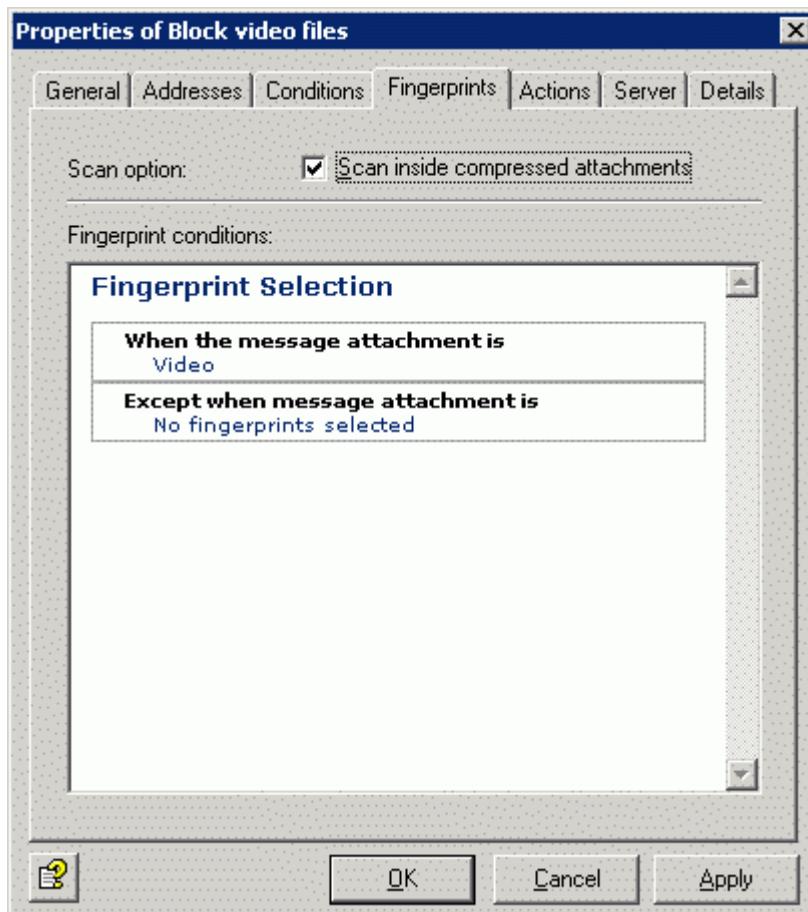
Setting content conditions

You can use the **Conditions** tab to set the conditions for executing a job.

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

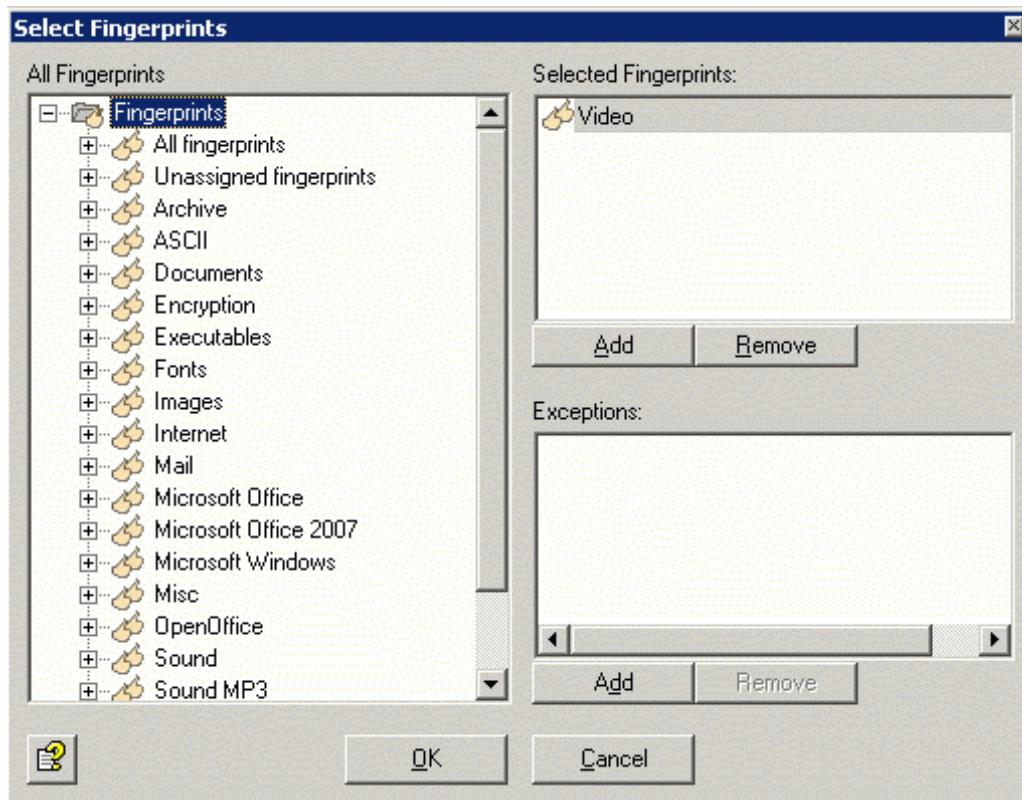
Select fingerprints

1. Select the prohibited fingerprints from the **Fingerprints** tab:



Unpack compressed attachments means that the internal unpacker will open archives and check the files they contain for the specified fingerprints. If this checkbox is not enabled, only the archive will be checked as the highest file and will simply be recognized as a packed format.

2. Fingerprint conditions: Click **Video** and **no fingerprints selected** to select a fingerprint category or an individual fingerprint from a fingerprint list.
You will see the following view:

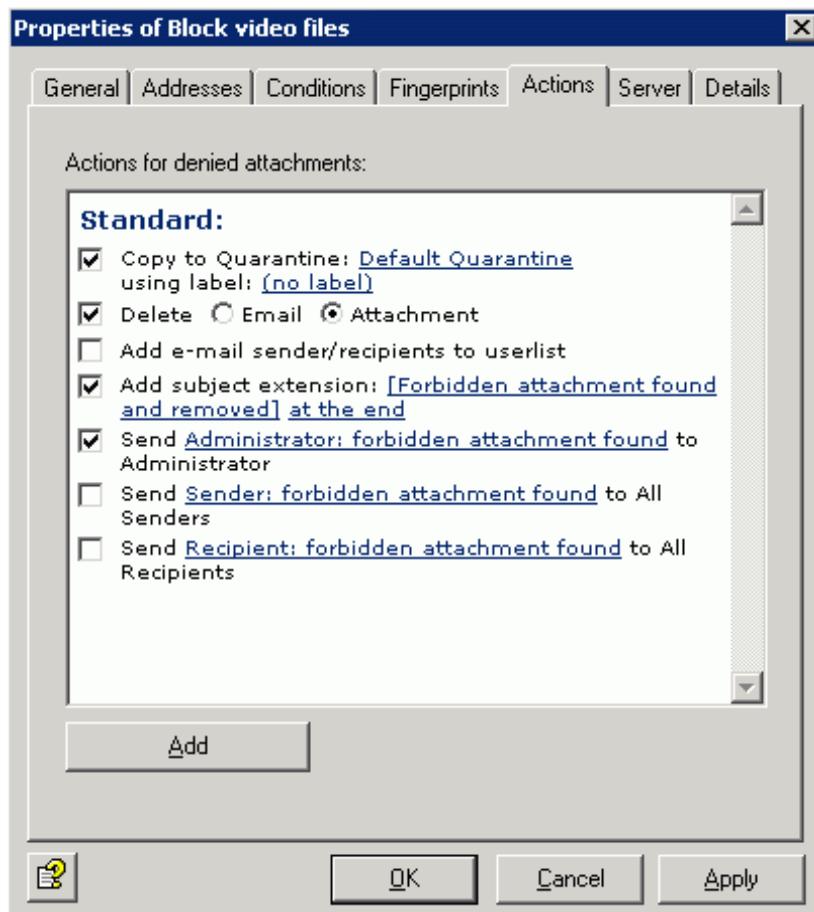


3. You can use the **Add** and **Remove** buttons to assign whole categories or individual fingerprints to the list of blocked and/or permitted fingerprints. Open the category in the left window by double-clicking or by clicking on the +.

Note: You can select a category, such as Video under **Selected Fingerprints** and enter one or more fingerprints for this category under **Exceptions**. For a better overview, avoid having too many categories checked by a single job.

Defining actions

- The **Actions** tab is used to define which actions are to be carried out **when the job has found a prohibited fingerprint as an attachment**:



A copy of the email is placed in quarantine and the relevant attachments are deleted. Consequently, the email is delivered to the recipient, but the prohibited attachments are removed. A warning is sent to the administrator notifying him/her of the fingerprint detected. This notification is selected from the pull-down list of possible notifications; the list can be organized individually with the HTML toolbar or directly with HTML format commands.

- The **Add** button allows you to define more actions.

5.7.6 Restricting email size - sample job

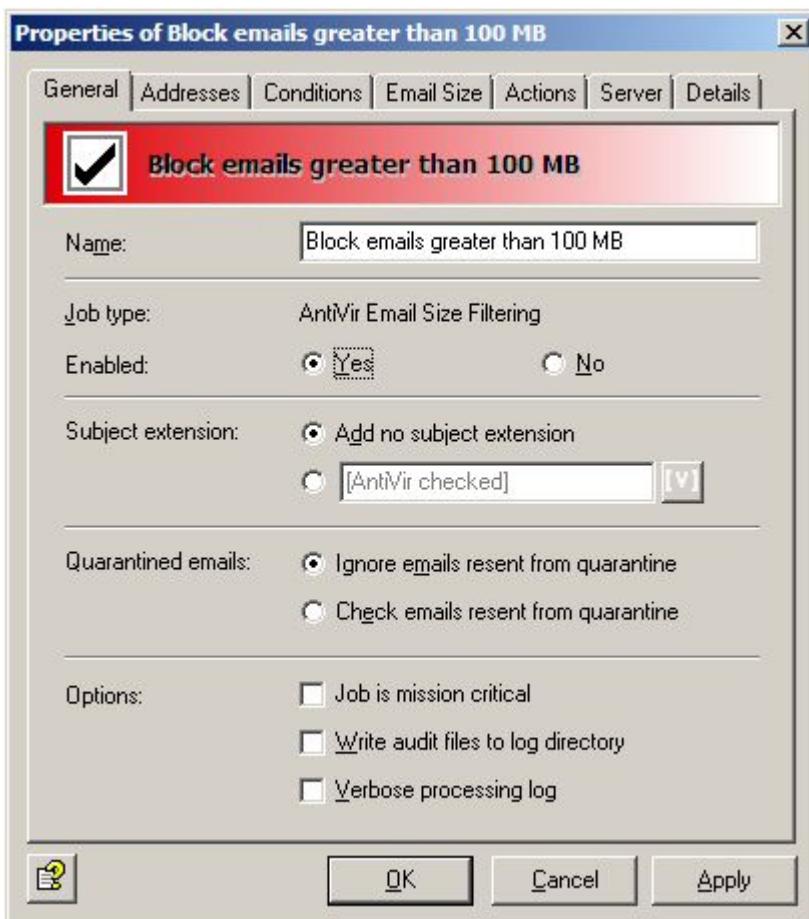
Under **Policy configuration - sample jobs** you will find the **Block emails greater than 100 MB** job

Note: The email size restriction relates to the entire email, including the subject, message text, header and attachment.

Drag and drop this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General settings

You can assign a name of your own to the job on the **General** tab. **Enable** the job. The job is enabled as soon as you save your settings with **OK** and close the job. The check mark in the job icon immediately tells you the job is enabled.



The default for the **Subject extension** is **AntiVir checked**. This extension is added to the subject line of every email scanned by the job.

This job also processes emails resent from quarantine. The Send option in **Send from quarantine** applies to all jobs and has priority. Accordingly, if you resend a mail with the **Quarantine Send** option **Deliver the email bypassing any AntiVir jobs on this server**, the mail will not be processed by any job. For this reason, when sending emails from quarantine, you should set the Send option to **Recheck email with AntiVir jobs**.

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself.

For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

Setting content conditions

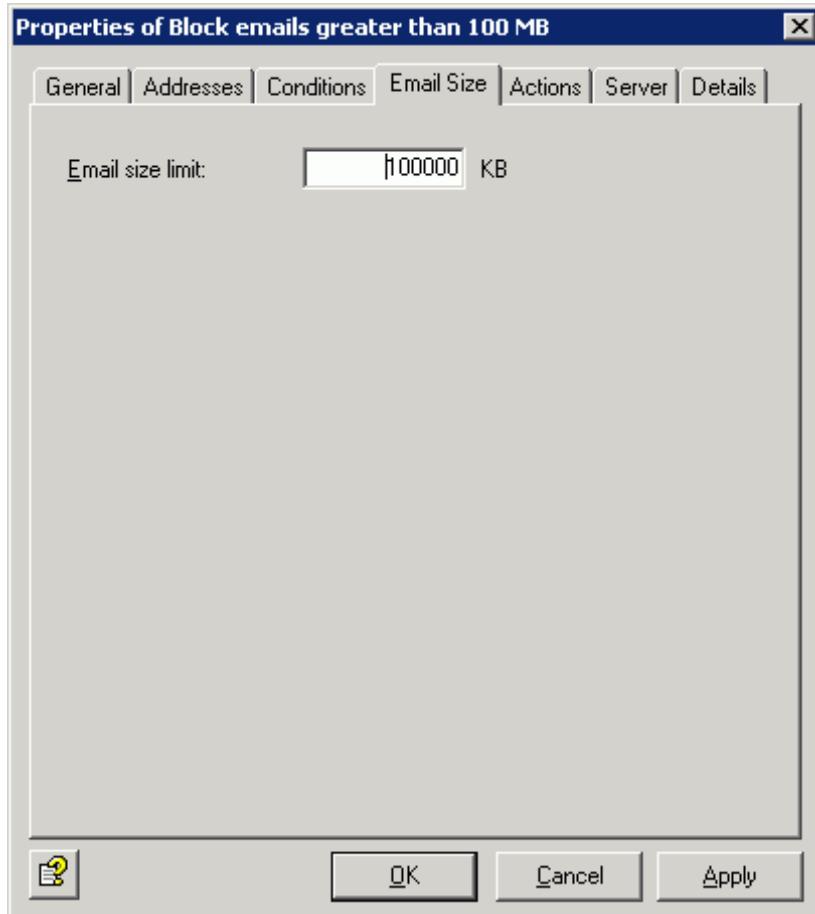
You can use the **Conditions** tab to set the conditions for executing a job.

For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

Defining email size

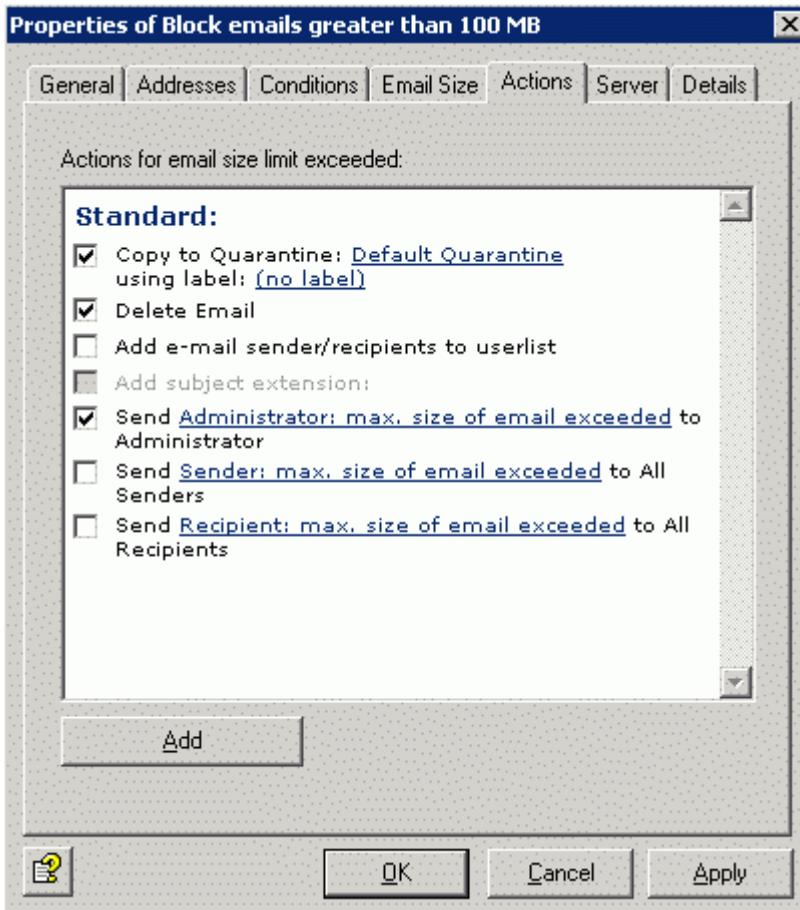
The **Email size** tab is used to define the required maximum email size in Kilobytes:



Each incoming and outgoing email may therefore only be a maximum of 100,000 Kilobytes in size.

Defining actions

The **Actions** tab is used to define which actions are to be carried out when the job has found an email that is too large.



As the action, a copy of the email is placed in quarantine and the relevant email is deleted. Consequently, the email is not delivered to the recipient. A warning is sent to the administrator notifying him/her of the excessively large email. The notification is selected from the pull-down list of possible notifications; the list can be organized individually with the HTML toolbar or directly with HTML format commands.

The **Add** button allows you to define more actions.

The procedure is described under [Defining actions](#) in "Enabling virus scanning - sample job"

Selecting servers

Servers are selected as described in [Selecting servers](#).

Saving the configuration

Save the configuration of the AntiVir Exchange Management Console every time you make changes. To do so, click the button. The configuration is saved in the ConfigData.xml file, which is stored in the Avira\AntiVir Exchange\Config\ directory. Open changes are indicated by (*) at the uppermost node.

5.7.7 Blocking attachments types and sizes - sample job

You will find different jobs for blocking various file formats and corresponding sizes under **Policy Configuration - Job templates**.

- **Block Office Files > 10 MB**
Microsoft Office files larger than 10 MB
- **Block Sound Files > 5 MB**
Sound files larger than 5 MB

- **Block Video Files > 5 MB**

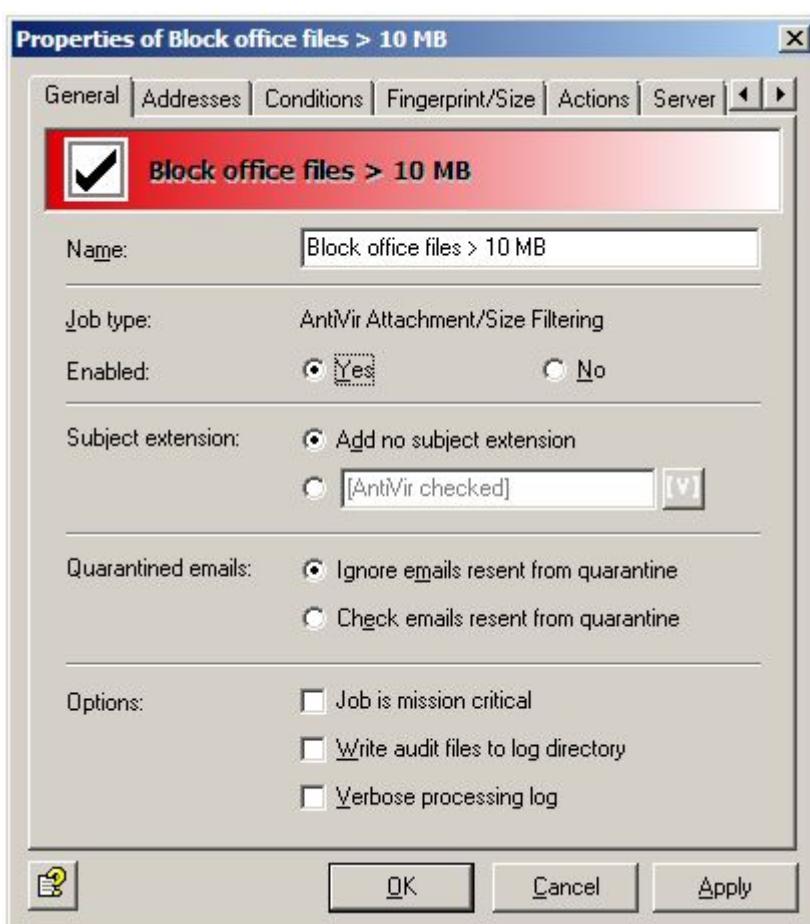
Video files larger than 5 MB

Note: Unlike the scan for email size, the scanning of the attachment format and size only applies to the attachments. The subject line, message text and header data of the email are ignored in this scan.

The following example is based on **Block Office Files > 10 MB**. Drag and drop this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General settings

You can assign a name of your own to the job on the **General** tab. **Enable** the job. The job is enabled as soon as you save your settings with **OK** and close the job. The check mark in the job icon immediately tells you the job is enabled.



The default for the **Subject extension** is **AntiVir checked**. This extension is added to the subject line of every email scanned by the job.

This job also processes emails resent from quarantine. The Send option in **Send from quarantine** applies to all jobs and has priority. Accordingly, if you resend a mail with the **Quarantine Send** option **Deliver the email bypassing any AntiVir jobs on this server**, the mail will not be processed by any job. For this reason, when sending emails from quarantine, you should set the Send option to **Recheck email with AntiVir jobs**.

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself.

For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

Setting content conditions

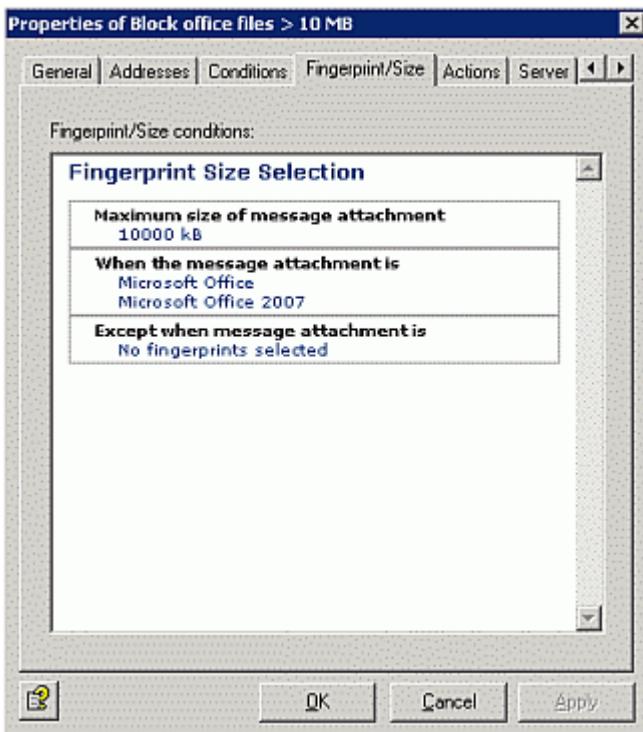
You can use the **Conditions** tab to set the conditions for executing a job.

For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

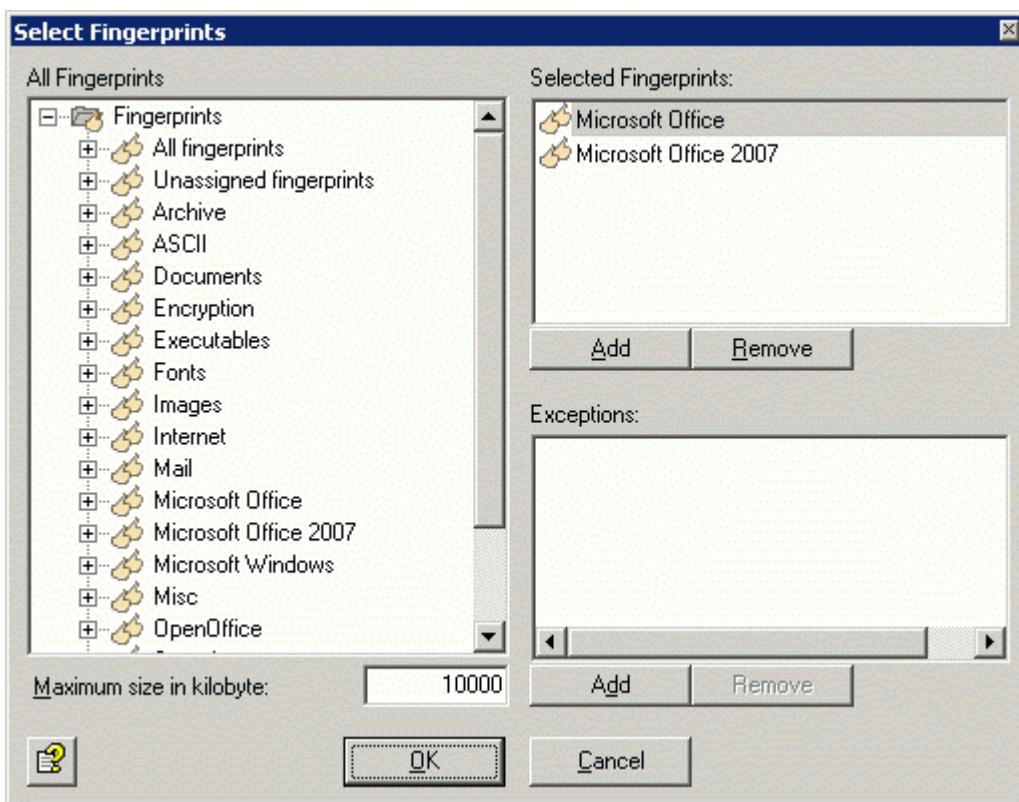
Setting the fingerprint/size

The **Fingerprint/Size** tab is used to define the required maximum email size and the fingerprint format:



Note: Unlike the simple fingerprint check, the **Unpack compressed attachments** option is not available here. If you wish to restrict the size of compressed files, just specify the relevant formats in this job.

Fingerprint/size conditions: Click **10,000** to set the size in kilobytes or on Microsoft Office to select a fingerprint category from a fingerprint list, an individual fingerprint or maximum size. You will see the following view:



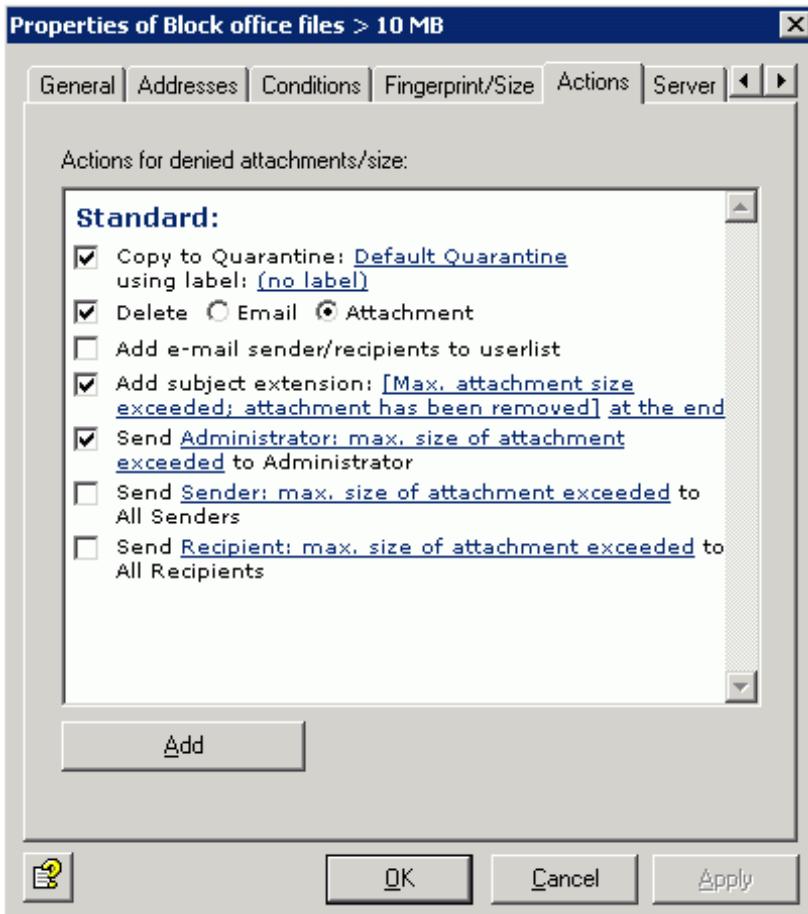
You can use the **Add** and **Remove** buttons to assign whole categories or individual fingerprints to the list of blocked and/or permitted fingerprints. Open the category in the left-hand window by double-clicking or by clicking on the +.

Note: You can select a category, such as "Microsoft Office" under **Blocked Fingerprints** and enter one or more fingerprints for this category under **Permitted Fingerprints as Exceptions**. For a better overview, avoid having too many categories checked by a single job.

You will find more information about fingerprints and about entering name and binary patterns under [Configuring fingerprints](#).

Defining actions

The **Actions** tab is used to define which actions are to be executed **when the job has found an email that has been blocked by an attachment/ size job**.



A copy of the email is placed in quarantine and the relevant attachments are deleted. In other words, the email is delivered to the recipient without its attachment. The administrator is notified of the restriction found. This notification is selected from the pull-down list of possible notifications; the list can be organized individually with the HTML toolbar or directly with HTML format commands.

The **Add** button allows you to define more actions.

The procedure is described under [Defining actions](#) in "Activating virus scanning - sample job"

Selecting servers

Servers are selected as described in [Selecting servers](#).

6 AntiVir Wall

AntiVir Wall allows you to check the text contained in emails or attachments, scan images for offensive content, classify emails according to content, restrict email addresses in input/output or limit the number of recipients per email.

6.1 Job types

- Address scan
Job: **AntiVir Wall Email Address Filtering**
- Content scan
Job: **AntiVir Wall Content Filtering**
- Anti-spam scan
Job: **AntiVir Wall Spam Filtering**
- Scanning for the number of recipients
Job: **AntiVir Wall Recipient Limit Filtering**

Note: Create a separate job for each restriction type. The job types cannot be changed later.

The exact procedure for creating a job can be found in the sample job descriptions, e.g. [Blocking senders and/or recipients - Sample job](#).

6.2 Address check

Address scanning concentrates on the senders and recipients of an email. You can block certain senders, so that your users no longer receive any email from them, as well as certain recipients, so that none of your employees (or only a select group) can send emails to certain recipients.

The following objects can be used in address scanning:

- Mail-enabled Active Directory users
- Mail-enabled Active Directory groups
- Mail-enabled Active Directory contacts
- Freely definable SMTP addresses, incl. wildcards
- [INTERNAL] = Internal domains as defined in Avira AntiVir Exchange
- [EXTERNAL] = All addresses that are not [INTERNAL]
- "Administrator" = The email addresses defined in Avira AntiVir Exchange as administrators.

The entry in the relevant email fields determines whether the user in question is a sender or a recipient. A sender can be either an employee of your company who sends an external email or an external person who sends an email to an employee of your company. You can define senders and recipients both as individuals or as groups.

The following wildcards can be used during address scanning:

- Asterisk (*)
The asterisk symbolizes the placeholder for one or more letters and/or numbers. The asterisk can be used any number of times within the keyword.

- Question marks (?)

The question mark is used as a placeholder for a single character. The question mark can also be used any number of times within the keyword.

When you specify a prohibited sender, you can use tom*@*. instead of individual email addresses. This means that all emails sent by a Tom followed by any extension (including last names) will be blocked, irrespective of the domain they are sent from. This group also includes your own employee, Tom Jones, who is therefore also restricted and whose emails are covered by the defined actions. You can define a specific domain, for example as *@domain.com. This prohibits all senders and recipients of this domain. An address scanning job with a block on a whole domain should only be applied to all users on a cross-server basis with great care. It is not always clear which addresses are private and which are for business purposes. Remember that smaller business partners may have email addresses under domains such as @tonline.de or @aol.com.

Address scanning is a simple way to filter out known spam addresses. The "usual suspects" can be intercepted by the job on the server and are immediately deleted.

Note: Because the initial restriction corresponds to the job restriction condition in address scanning jobs, a configured **Subject extension** when the condition is met is also added when the initial condition is not met, contrary to the other job types.

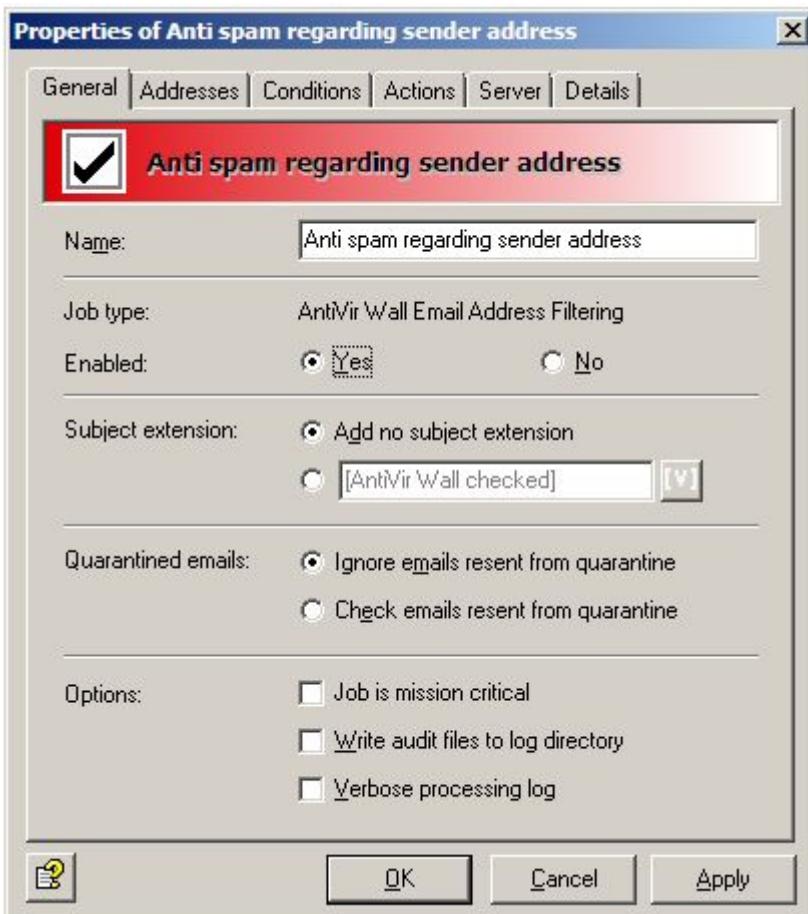
- Copy entire email to quarantine
- Subject extension
- Delete and do not deliver the affected email.
- Notify administrator
- Notify sender
- Notify recipient
- Notify other freely selected persons
- Run an external application
- Add Avira header field
- Add X header field
- Redirect email

6.2.1 Blocking senders or recipients - sample job

You will find a preconfigured job for scanning addresses under **Policy configuration - Sample jobs**. Copy the job labeled **Anti-Spam using Email Addresses** under **Mail Transport Jobs** and double click to open it.

General settings

You can assign a name of your own to the job in the **General** tab. **Enable** the job. The job is enabled as soon as you save your settings with OK and close the job.



The default for the **Subject extension** is **AntiVir Wall checked**. This extension is added to the subject line of every email scanned by the job.

This job will not process mails resent from Quarantine, even if the **Resubmit the email to all AntiVir jobs on this server** send option has been activated when sending emails from **Quarantine (AntiVir Monitor - <Select Email> - All Tasks - Send from Quarantine)**. The Ignore emails resent from quarantine option means that this job is generally skipped when mail is sent from Quarantine.

For more information about resending emails from Quarantine see [Sending emails from Quarantine](#). The **AntiVir** chapter explains the **Job is mission critical** option in more detail.

Save the configuration of the Avira AntiVir Exchange Console every time you make changes. To do so, click the button. The configuration is saved in the ConfigData.xml file, which is stored in the Avira\AntiVir Exchange\Config\ directory. Open changes are indicated by (*) at the uppermost node.

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself.

For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

Setting content conditions

You can use the **Conditions** tab to set the conditions for executing a job.

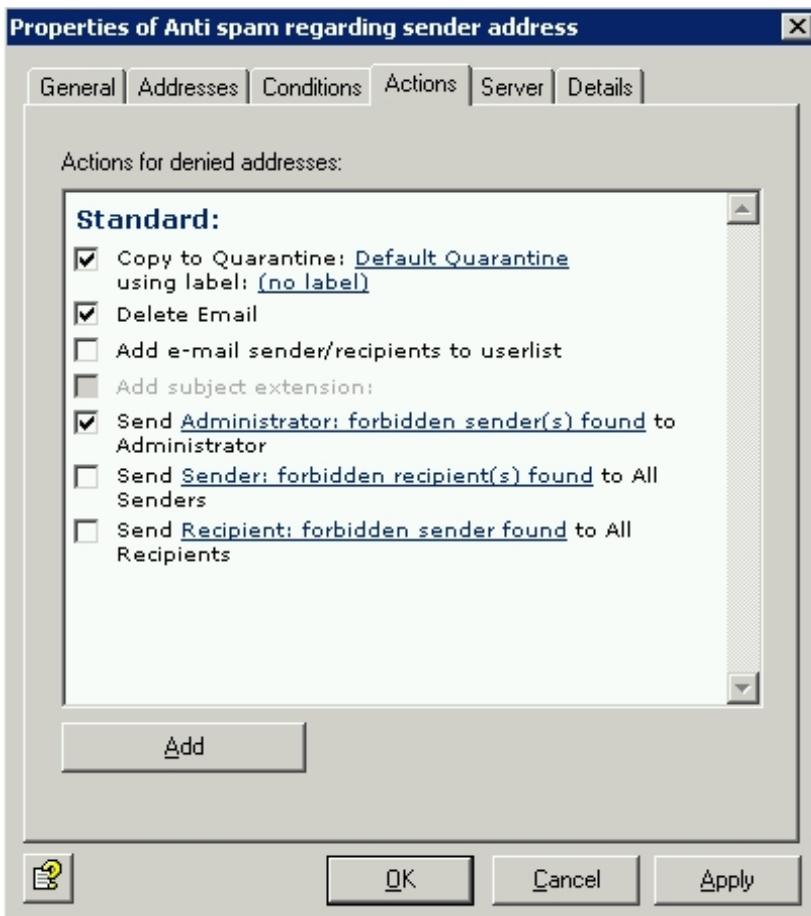
For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

Defining actions

The **Actions** tab is used to define which actions are to be carried out when the job has found an email with prohibited addresses.

As the action, a copy is placed in quarantine and the relevant email is deleted. Consequently, the email is not delivered to the recipient. A warning is sent to the administrator notifying him that the address policies have been violated. The notification is selected from the pull-down list of possible notifications; the list can be organized individually with the HTML toolbar or directly with HTML format commands.



The **Add** button allows you to define more actions.

The procedure is described under [Defining actions](#) in "Activating virus scanning - sample job"

Selecting servers

Servers are selected as described in [Selecting servers](#).

6.3 Content check with dictionaries

AntiVir Wall uses predefined dictionaries to check for unwanted text content.

The following components of the email can be checked:

- Subject
- Message text
- Attachments

The content search can be restricted to certain senders or recipients. In this way, it is possible to examine only incoming external emails for pornography, racism, etc. On the other hand, you can have emails from internal senders to outside the company scanned for company-internal information. The emails are scanned with the dictionary to be used and, as soon as this dictionary is enabled in the job, the words or sentences specified by you are deemed prohibited from a certain threshold. The character conversion is also defined in the job. When the threshold is reached, the job starts the actions that you had previously defined in the **Actions** tab.

Example of how a job for checking content works:

The job scans an email with the result: Prohibited content found. This triggers an alarm and a series of actions is started, which you can define yourself under Actions in the job. We assume that you have defined the following:

1. The email is moved to the folder selected by you (quarantine) and is not delivered to the recipient.
2. Messages to the administrator, sender and recipient are created and these contain the relevant information of the wall job.

The possible actions are the same as for the address check.

6.3.1 Setting up dictionaries

1. Click **Basic Configuration - Utility Settings - Dictionaries**
2. Double-click a dictionary to open it in the right-hand window.
3. Assign a name for the dictionary on the **General** tab.
4. Assign the dictionary a **Value rating** from 1 to 200.

This value rating applies per word or phrase and determines both the relationship to other dictionaries and the extent to which the dictionary is taken into account in the job.

For more information on value ratings, see [Checking and blocking text content - sample job](#).

5. Click the input field for words and add the words/phrases that you want to prohibit.
The individual words/phrases are separated from one another with a carriage return (Enter key).

The following wildcards can be used in dictionaries:

- Asterisk (*)

The asterisk means that the word/phrase searched for can also be a part of a bigger word but does not have to be. Examples:

check finds the individual word "check" but also the words "checkpoint", "intercheck" or "intercheckpoint".

check* finds "check" as well as "checkpoint".

The asterisk must be placed at either the start or the end of a word/phrase.

- Plus sign (+)

The plus sign means the same as the asterisk with the difference that the word/phrase searched for must be a part of a bigger word. Examples:

+check+ finds only "checkpoint", "intercheck" or "intercheckpoint" but not "check".

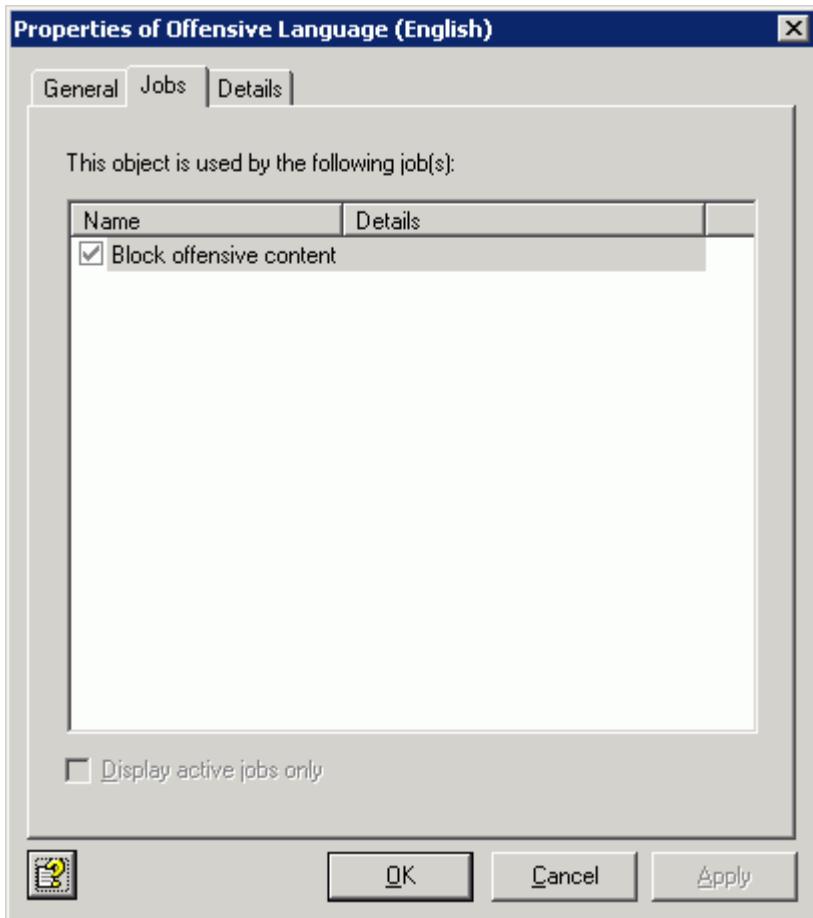
check+ only finds "checkpoint".

The plus sign must also be placed at either the start or the end of a word/phrase.

Note: If you do not insert an asterisk or a plus sign in your words/phrases, the word must be found exactly as entered. Therefore: if you enter check, only the individual word "check" will be found.

6. If required, you can sort the dictionary in ascending or descending order by clicking  for ascending and  for descending.
7. You can create a new dictionary by right-clicking **Dictionaries** and selecting **New - Dictionaries**.

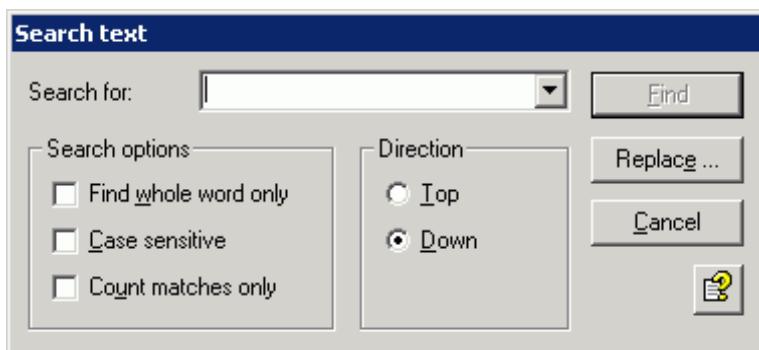
The **Jobs** tab shows the jobs in which the dictionary is incorporated:



Note: To use the dictionaries in the job, select a Content-Filtering job in the Policy Configuration, enable the corresponding dictionary and define an overall threshold (from 1 to 10,000). As soon as this threshold has been reached by adding up all the value ratings (found words) of the active dictionaries, the defined actions come into effect. For more information, see [Checking and blocking text content - sample job](#).

Text search in dictionaries

1. You can search for terms in dictionaries and delete them if required. Double-click the dictionary to open it and then click the text search icon



If you do not specify any additional option, the string will be found everywhere, also in parts of a word or a phrase.

- **Find whole word only:**
All non-alphanumeric characters, including carriage or line returns, are valid separators between words.
- **Case sensitive:**
Takes upper and lower case into account during the search.
- **Count matches only:**
The hits are not "jumped to" directly but are instead counted and the result is output in the form of a message:



2. Click the **Replace** button if you want to replace a specific term with another one:



You can also use the text search for searching and replacing in your own addresses. For more information, see [Address lists](#).

6.3.2 Checking and blocking text content - sample job

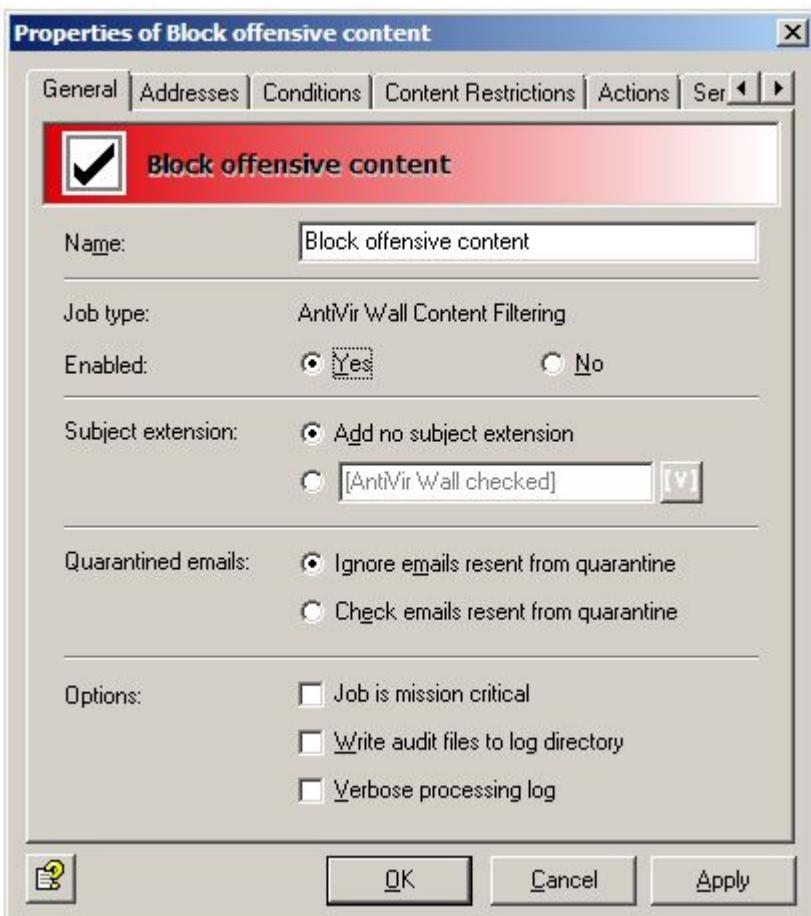
You will find various jobs for checking content with dictionaries under **Policy Configuration – Job Templates**.

- **Block offensive content**
Scan emails for ordinary and pornographic language
- **Block script commands**
Scan email for script commands that could cause damage
- **Block e-mails with resumes**
Scan email for terms from resumes
- **Block emails with "Nigeria connection"**
Scan email for special terms in the "Nigeria" emails

Block offensive content is taken as an example here. Drag and drop this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General settings

You can assign a name of your own to the job on the **General** tab. Set the job to **Active**. The job is enabled as soon as you save your settings with OK and close the job. The check mark in the job icon immediately tells you the job is active.



The default for the **Subject extension** is **AntiVir Wall checked**. This additional text is added to the subject line of every email checked by the job.

This job will not process mails resent from Quarantine, even if the **Resubmit the email to all AntiVir jobs on this server** send option has been activated when sending emails from **Quarantine (AntiVir Monitor - <Select Email> - All Tasks - Send from Quarantine)**. The **Ignore emails resent from quarantine** option means that this job is generally skipped when mail is sent from Quarantine.

For more information about resending emails from Quarantine see [Sending emails from Quarantine](#). The **AntiVir** chapter explains the [**Job is mission critical**](#) option in more detail.

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself.

For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

Setting content conditions

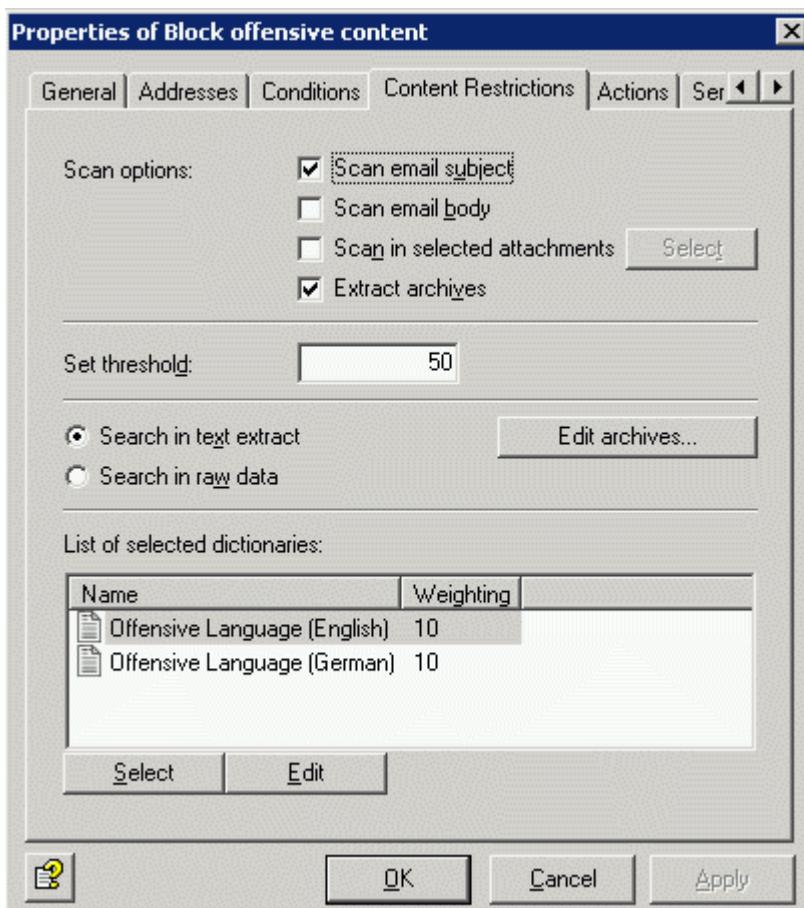
You can use the **Conditions** tab to set the conditions for executing a job.

For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

Selecting dictionaries

In the **Content Restrictions** tab, set which dictionaries are to be called with this job.



This job scans the subject. The overall threshold is defined as 50. The defined actions are therefore executed if 5 words/phrases from the **Offensive Language (English)** or the **Offensive Language (German)** dictionary are found.

The calculation: Each word or each phrase from the **Offensive Language** list has a value rating of 10. The actions are therefore executed if at least 5 words/phrases from these lists are found.

Explanation: Each word or each phrase from the **Offensive Language** list has a value rating of 10. Each word/phrase from this list is counted, the number of words/phrases found from the list is multiplied by the value rating, and the email is compared with the threshold value.

Therefore, in this case: 5 words that are on the list were found in the email. This gives a value of 5 words x 10 (value rating): $5 \times 10 = 50$. Comparison with the threshold value of 50 = Action is triggered. If only 4 words from the list are found in the email, the total value is only 40 (4×10), the threshold is not reached and no action is initiated.

Another example:

You are using **two different dictionaries** to scan the subject and the message text of an email for prohibited content.

The **overall threshold** is defined as 20 in the job and the first dictionary (A) specified in the job has a value rating of 20. The second dictionary (B) specified in this job has a value rating of 1. The defined actions are therefore executed if 1 word/phrase from dictionary A is found, or alternatively if 20 terms from dictionary B are found.

The calculation: Each word or each phrase from dictionary A has a value rating of 20. Therefore, if a single phrase from this list is found, the job threshold has already been reached and the action is carried out.

Each word or each phrase from dictionary B has a value rating of 1. Each word/phrase from this list is counted, the total number of words/phrases is multiplied by the value rating, and the email is compared with the threshold value. If 21 words that are on list B are found in the email, these are multiplied by the value rating of 1: $21 \times 1 = 21$. Comparison with the job threshold value of 20 = Action is triggered.

Note: If you want to detect content from different languages, create the corresponding dictionaries and set up one job per language. For languages such as French and Spanish, define a user-defined character conversion. For this configuration, please contact Avira support.

Defining actions

The **Actions** tab is used to define which actions are to be carried out **when the job has found an email with prohibited content**.



As the action, a copy is placed in quarantine and the relevant email is deleted. Consequently, the email is not delivered to the recipient. A warning is sent to the administrator notifying him/her that the company policies have been violated. The notification is selected from the pull-down list of available notification templates; the list can be organized individually with the HTML toolbar or directly with HTML format commands.

Save the configuration of the Avira AntiVir Exchange Console every time you make changes. To do so, click the  button. The configuration is saved in the *ConfigData.xml* file, which is stored in the *Avira\AntiVir Exchange\Config* directory. Open changes are indicated by (*) at the uppermost node.

6.4 Limiting the number of recipients

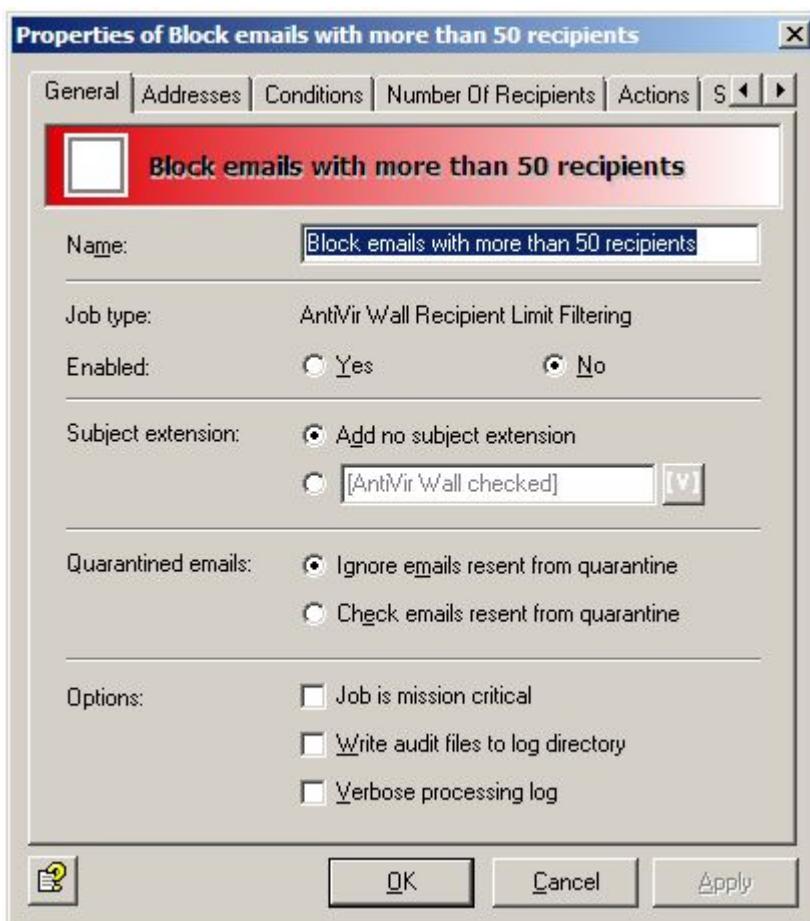
This job type allows you to restrict the number of recipients per email. If this job is enabled, it is not possible to send unnecessary mass mailings to all employees of the company.

6.4.1 Restricting the number of recipients - sample job

In **Policy Configuration – Job Templates**, you will find the job **Block emails with more than 50 recipients**. Drag and drop this job to the **Mail Transport Jobs** folder and open it there with a double-click.

General settings

You can assign a name of your own to the job on the **General** tab. Set the job to **Active**. The job is enabled as soon as you save your settings with OK and close the job.



The default for the **Subject extension** is **AntiVir Wall checked**. This additional text is added to the subject line of every email checked by the job.

This job will not process mails resent from Quarantine, even if the send option **Resubmit the email to all AntiVir jobs on this server** has been activated when sending emails from **Quarantine (AntiVir Monitor - <Select Email> - All Tasks - Send from Quarantine)**. The **Ignore emails resent from quarantine** option means that this job is generally skipped when mail is sent from Quarantine.

For more information about resending emails from Quarantine see [Sending emails from Quarantine](#).

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself.

For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

Setting content conditions

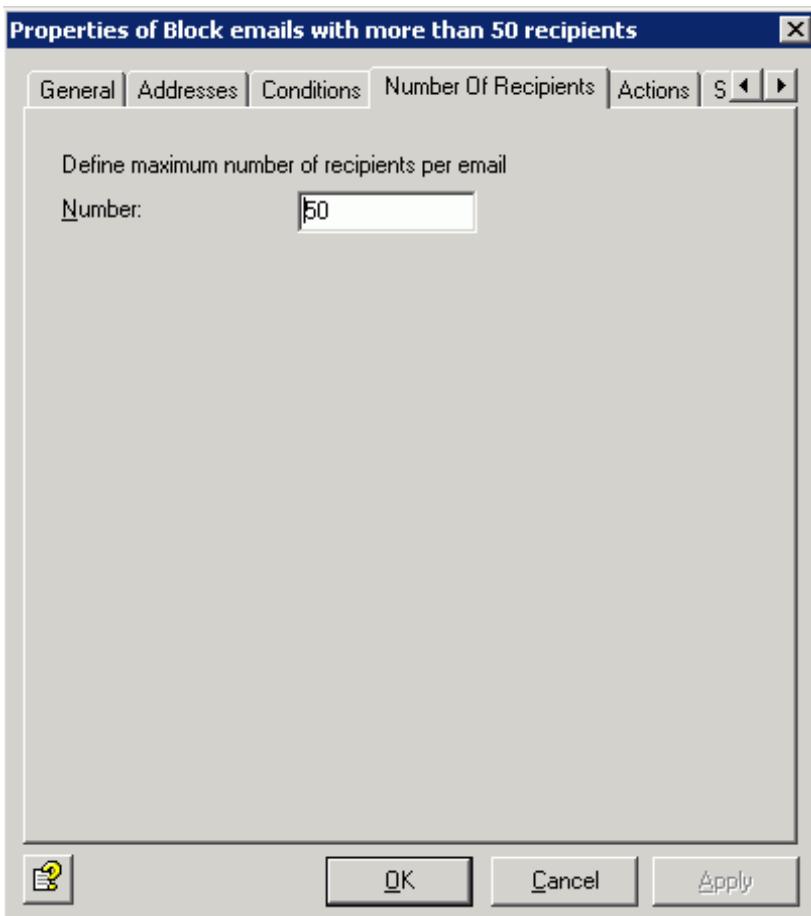
You can use the **Conditions** tab to set the conditions for executing a job.

For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

Defining the number of recipients

Enter the maximum number of recipients per email in the **Number of recipients** tab:

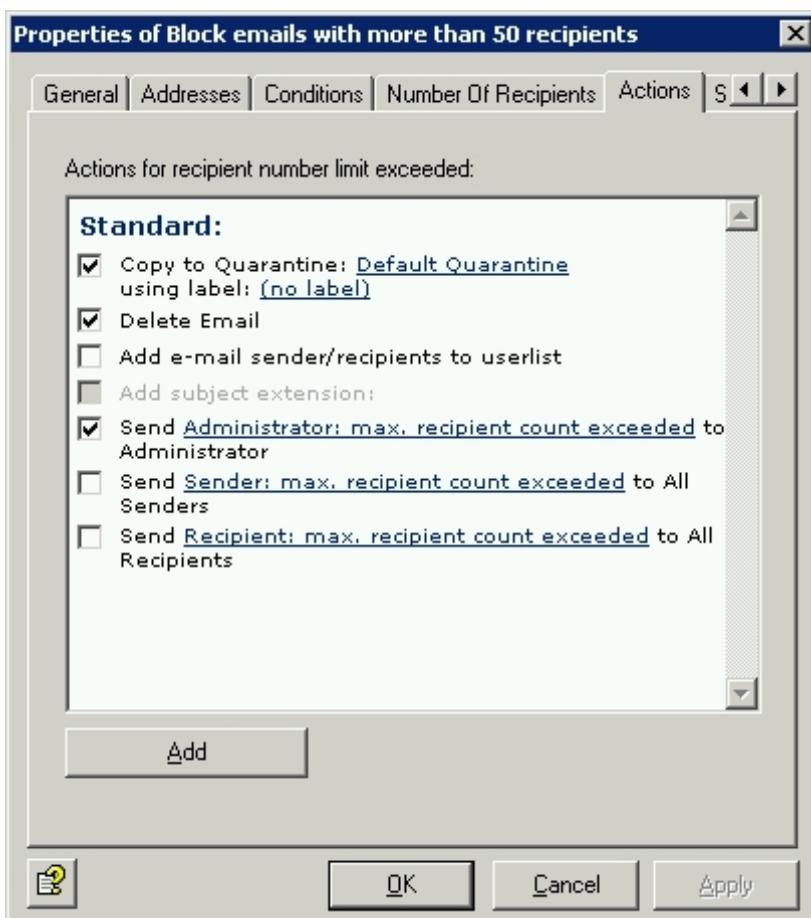


Each incoming and outgoing email may therefore only be addressed to a maximum of 50 recipients. As soon as an email is addressed to 51 recipients, the defined action is triggered.

Note: If the emails are addressed to a list of recipients that are grouped in a single address, the Exchange server must be able to break down the list into the various recipients so that it can identify the number of recipients. An address that is actually a mailing list is considered a single recipient if it is outside the range of the Exchange server.

Defining actions

The **Actions** tab is used to define which actions are to be carried out when the job has found an email with too many recipients.



As the action, a copy of the email is placed in Quarantine and the relevant email is deleted. Consequently, the email is **not** delivered to the recipients. A warning is sent to the administrator notifying him/her about the number of recipients. The notification is selected from the pull-down list of available notification templates; the list can be organized individually with the HTML toolbar or with HTML format commands.

The **Add** button allows you to define more actions. The procedure is described under [Defining actions](#) in "Activating virus scanning - sample job"

Selecting servers

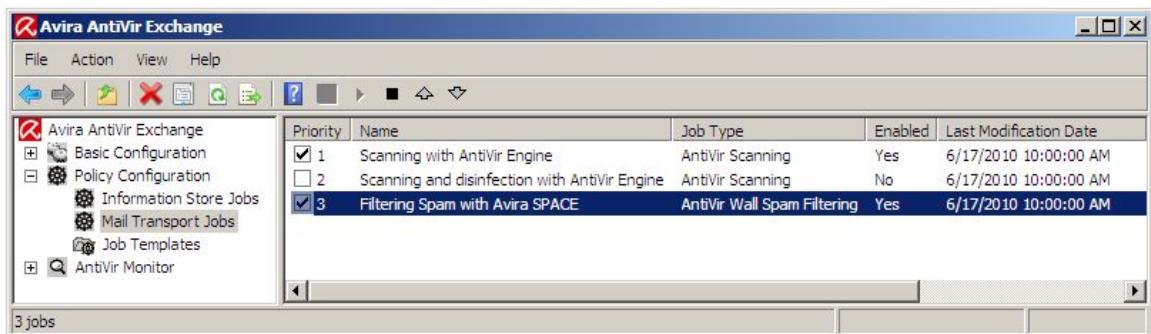
Servers are selected as described in [Selecting servers](#).

7 Anti-spam

The anti-spam check involves scanning emails for special features that indicate spam. Unlike viruses, spam is not always immediately recognizable as such. Spammers send a wide variety of content in a broad spectrum of forms, always with the intention that their emails should not be recognized for what they are: namely spam. Spammers are constantly coming up with new tricks for getting past spam filters.

This means that an anti-spam job must also consider that emails cannot always be definitively identified as spam. That's why the spam filtering job uses a wide variety of spam criteria, which are divided into definite and combined criteria.

The **Filter for Spam with Avira AntiSpam** job is preconfigured and pre-enabled for your own security. This job can be found under **Mail Transport Jobs**.



7.1 Avira AntiSpam Engine

AntiSpam is a type of anti-spam engine used to detect spam and phishing emails. AntiSpam is part of AntiVir Wall Spam filtering jobs and is the default anti-spam engine.

The **Avira AntiSpam engine** uses the information from a periodically updated local database and various RBL DNS servers (Realtime Black Lists) to analyze emails.

The result of this check is a value that is used to calculate the spam probability as part of the extended spam filter job.

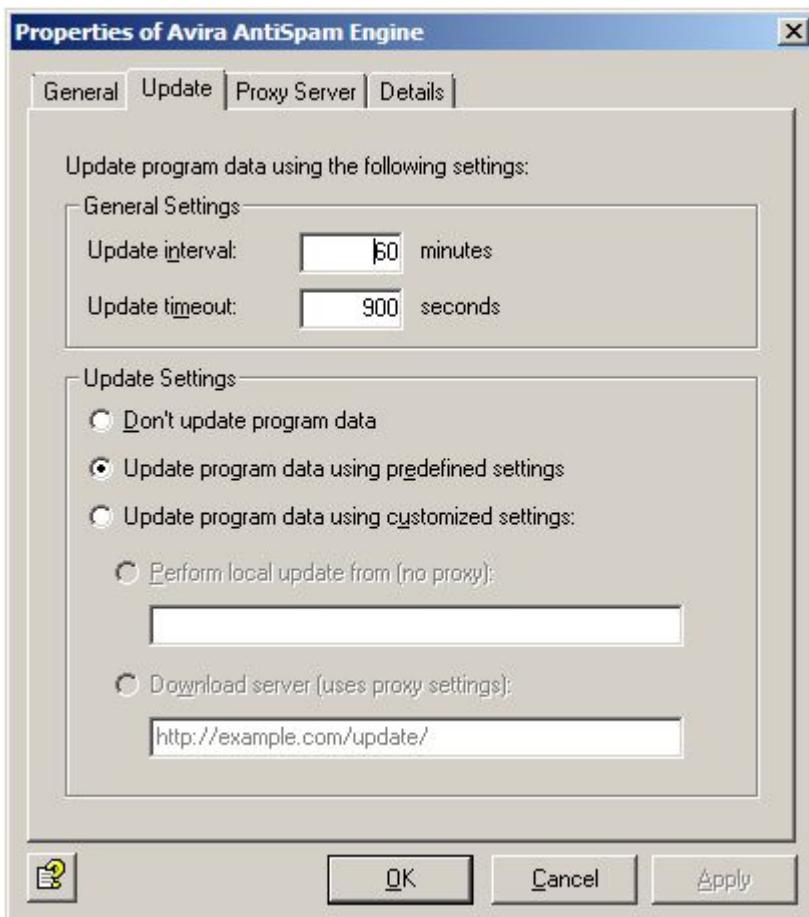
7.1.1 Configuring AntiSpam Engine

If you are using AntiSpam for combating spam, firstly configure the AntiSpam Engine for regular pattern updates. The configured engine is automatically used as soon as a spam filtering job with the SPACE criterion enabled is activated.

Open **Basic Configuration - Utility Settings** and click **AntiSpam Engine**. Double-click **Avira AntiSpam Engine** to select it or right-click **Properties**.

It is possible to duplicate AntiSpam, e.g. if you want to use different configurations or intervals.

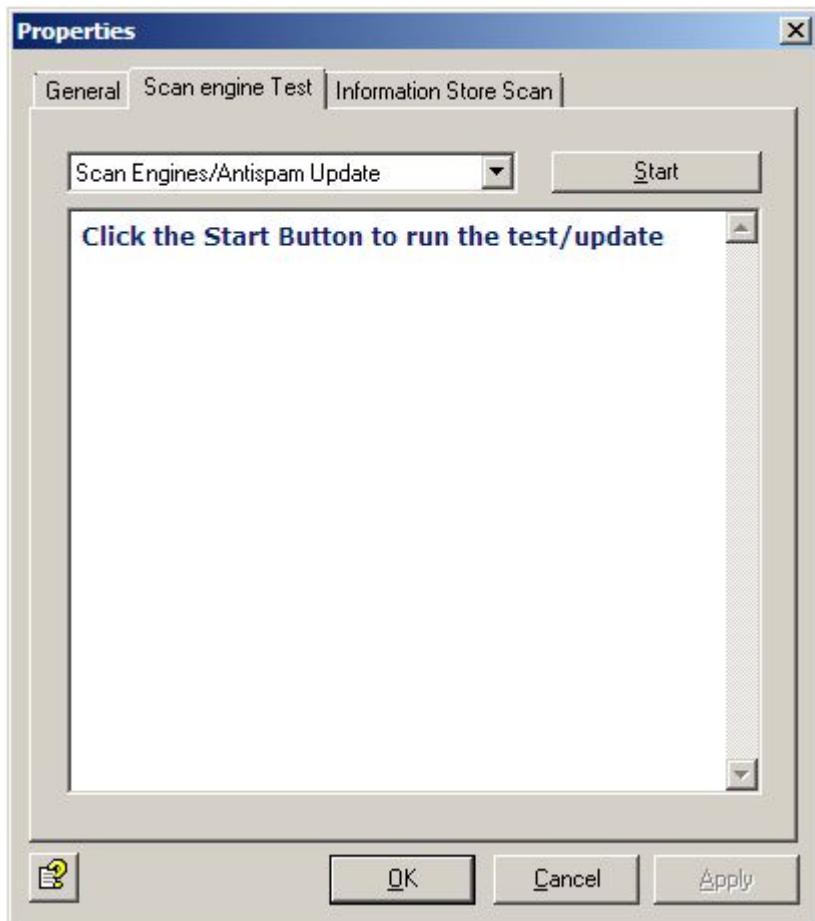
Setting an AntiSpam update



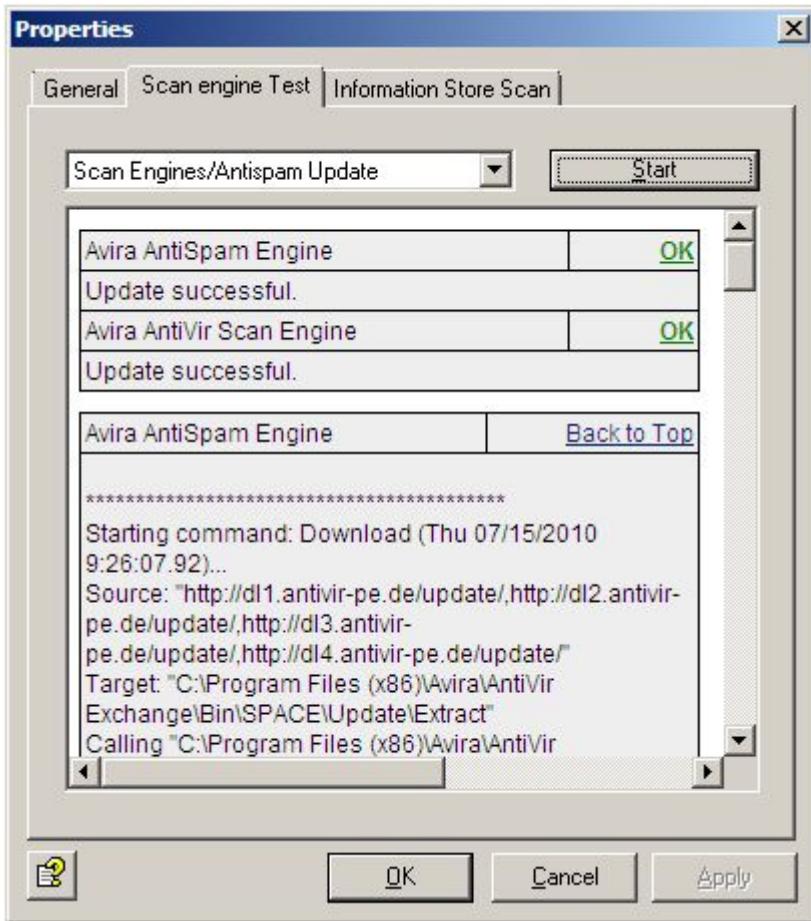
For the standard case, it is sufficient if you just enter the interval for the pattern update in this tab:

- **Parameter:** This field specifies the directory in which the updated patterns are saved. You only need to change the details if you selected other directories when setting up AntiSpam.
- **Interval:** Interval in minutes at which pattern update scanning takes place. Minimum value: 15 minutes.
- **Timeout:** For access to the server in seconds. The update procedure will be cancelled after this time.

If you are using a proxy server for the updates, click the **Proxy server** tab and select the server. To manually update AntiSpam, click **AntiVir Monitor - Server - <server> - Server Status** in the navigation area:



On the **Search Engine Test** tab, select **Virus Scanner/Antispam update** and click **Start**. After the update you will receive a detailed update report.



7.2 Wall spam filtering jobs

7.2.1 AntiSpam with Wall Spam Filtering jobs

This job uses the definite criteria to scan the email for absolutely unambiguous spam features and, following the scan, decides: 100% spam or 100% no spam. The combined criteria are used to check the "gray zone" to calculate the probability that the scanned email is spam (= spam probability). The spam probability of the definite criteria is always 0% or 100%, while the combined criteria can range from 1 to 99. A preconfigured **Wall Spam Filtering Job** can be found in the **Policy Configuration**. The job contains a number of analyses and checks the following components of the email:

- Email headers
- Subject
- Message text

Here too - as in normal content checks - predefined dictionaries with widely divergent content are used to scan for spam text content.

A number of the combined criteria occur frequently in spam mails in the "gray zone" and other criteria are more indicative of no spam mails. In itself, each combined criterion is normally just one indicator of whether an email has particular features that indicate spam. The more criteria with a high value for spam in an email, the more certain it is that this is indeed a spam mail. The combination of the individual results of these criteria (hence "combined criteria") yields a measure in the job that expresses the level of certainty that this email is spam (= spam probability).

The preconfigured job is set so that an email can only attain a high **spam probability** of over 91%, for example, if clear indicators of spam have been found for several combined criteria.

Up to four ranges of this spam probability are differentiated in the job. You can define the limits between four ranges (spam probability = threshold values) using sliders and define the actions for each defined range which the job is to perform on the emails whose spam probability falls in the relevant range. This enables you to choose a configuration so that

- definite "no spam" with a spam probability of 0% is delivered in the normal way,
- emails with a spam probability of less than 10% are also delivered in the normal way. One option might be to place these emails for classification in the quarantine **Email: Low**,
- between 10% and 50% spam probability the **SCL field** is evaluated in Exchange 2003 so that the email is automatically moved to the recipient's junk mail folder, or the emails are placed in the **Email: Medium** quarantine and recipients receive a summary report on the emails sent to quarantine and can request these as necessary,
- emails with a spam probability of over 50% are immediately deleted. Here too you can place the emails for classification in quarantine under **Email: High**.

The following actions are possible:

- Copy the entire email to quarantine
- Subject extension
- Delete and do not deliver the affected email.
- Add sender or recipient to white list
- Notify administrator
- Notify sender
- Notify recipient
- Notify other freely selected persons
- Run an external application
- Add Avira header field
- Add X header field
- Redirect email

The individual threshold ranges are:

1. **Spam probability: None.** Preconfigured: 0
2. **Spam probability: Low.** Preconfigured: 0 - 19.
3. **Spam probability: Medium.** Preconfigured: 20 - 74.
4. **Spam probability: High.** Preconfigured: 75-100.

The ranges **Low, Medium and High** can be defined by means of a slider and associated actions can be configured. Depending on the range assigned to the email after scanning, the action defined for this threshold range will be triggered. You can configure a subject extension for spam probability **None**.

The important point for a good email solution is also the effective avoidance of incorrectly classified emails (false positives) and the efficient use of the computing capacity available for spam checking in productive mode. The **definite exclusion criteria** (= Definite Criteria) thus precede the combined criteria so that there is no need to perform further spam checks on the email once these criteria are met. The exclusion criteria are used to restrict the spam checks to those emails that cannot already be excluded as spam, for example because of the sender.

Note: When a definite criterion is met, the spam probability is always 0% or 100% and always occurs in the **None** or **High** probability range with the corresponding actions.

Note: Naturally, these criteria do not affect scanning by differently configured and active email scanners, such as the scanning of file attachments by AntiVir. Accordingly, if you have enabled the definite "no spam" criterion **Emails with attachments** and have set the threshold (**minimum number**) to 2, this simply means that the spam filtering job will immediately assign these emails to the spam probability range **None** and not that a watchdog job will suddenly allow these two attachments to reach your network without any checking.

Note: It is not usually necessary to modify the combined criteria. If the spam detection rates are unsatisfactory, try to optimize the definite spam criteria (exclusion criteria) (see below).

7.2.2 Definite no-spam criteria

The following criteria can be configured in the job as the basis for automatically identifying emails as non-threatening or as no-spam:

Criterion	Description
Emails from these trusted senders (Whitelist)	Whitelist: Addresses of all known senders who are always permitted and who definitively do not send spam. In principle, these are all regular communication partners and the domains of customers and suppliers. The more complete this list, the less the system will have to carry out unnecessary checks.
Emails from Active Directory users	Other trusted addresses are all users and contacts entered in the Active Directory.
Emails from senders in user whitelist	Email addresses contained in the user whitelist are allowed through without being scanned for spam.
Emails with attachments	Emails with file attachments Most unwanted emails do not have attachments. As an option you can enter a threshold value here. Example: Minimum value = 2, i.e. all emails containing only 2 attachments are delivered without a spam check.
Emails with a minimum size of	Spam mails are generally small. Accordingly, large emails are not usually spam. You can set a threshold value here, so that larger emails do not get checked for spam.
Emails are in TNEF format	TNEF emails. This Exchange-specific format has not been used by spammers to date.

Emails are encrypted or signed	Encrypted and/or signed emails. At present, spammers do not send encrypted or signed emails.
Microsoft Exchange "No-Spam" SCL Value See also Write Spam result in Exchange SCL field	Spam Confidence Level (SCL), Spam Filter (Intelligent Message Filter (IMF) Exchange 2003 and higher. SCL can accept integers between -1 and 9. -1 is assigned by Exchange for emails from senders in the same Exchange organization. This value is evaluated by the Wall Spam filtering job as a definite "no spam" criterion.

7.2.3 Definite spam criteria

Likewise, the following exclusion criteria can be defined to ensure that an email is always filtered and intercepted if necessary.

Criterion	Description
Emails from the following senders (Blacklist)	Blacklist: Addresses from all senders who are always identified as spam senders. The default configuration already contains a list of known addresses. You can define additional addresses of your own.
Emails with this character set	This function checks the "charset" field in the email headers for character sets contained in the specified list. Emails using such character sets are immediately classified as spam.
Exchange SenderIDResult = "FAIL" You will find more information about the SenderID under Details: SenderID	If you enable this criterion, the sender ID of the email is also evaluated. This prevents "spoofing" in other words the falsification of sender mail address domains. Evaluation is based on entries in a DNS. This DNS can be used to determine from which IP addresses emails from particular domains can/cannot be sent. The result of the sender ID is supplied with the email. Wall checks the sender ID of the email and evaluates the result "FAIL" as spam. To be able to use the SenderID function you must enable a number of functions on the server, e.g. the associated filters for SenderID on the server. These are enabled under Server - Logs - SMTP - Properties in the Identification field. In addition, both server and client (Outlook) must be configured.

Note: If emails are only to be deleted directly when they are definitely identified as SPAM, you must set the **Spam probability** for **High** to 100 percent and define a corresponding action. This ensures that only the emails in which the definite criteria (= the black list of character set) have clearly identified SPAM come under this category. With a setting of 91 to 100, for example, emails with a high spam probability from other criteria also come under this category.

7.2.4 Practical tips

Depending on the operational environment, it can happen that the job also finds spam indicators for normal and wanted emails and therefore incorrectly treats these as spam. If such cases occur, we recommend the following configuration settings:

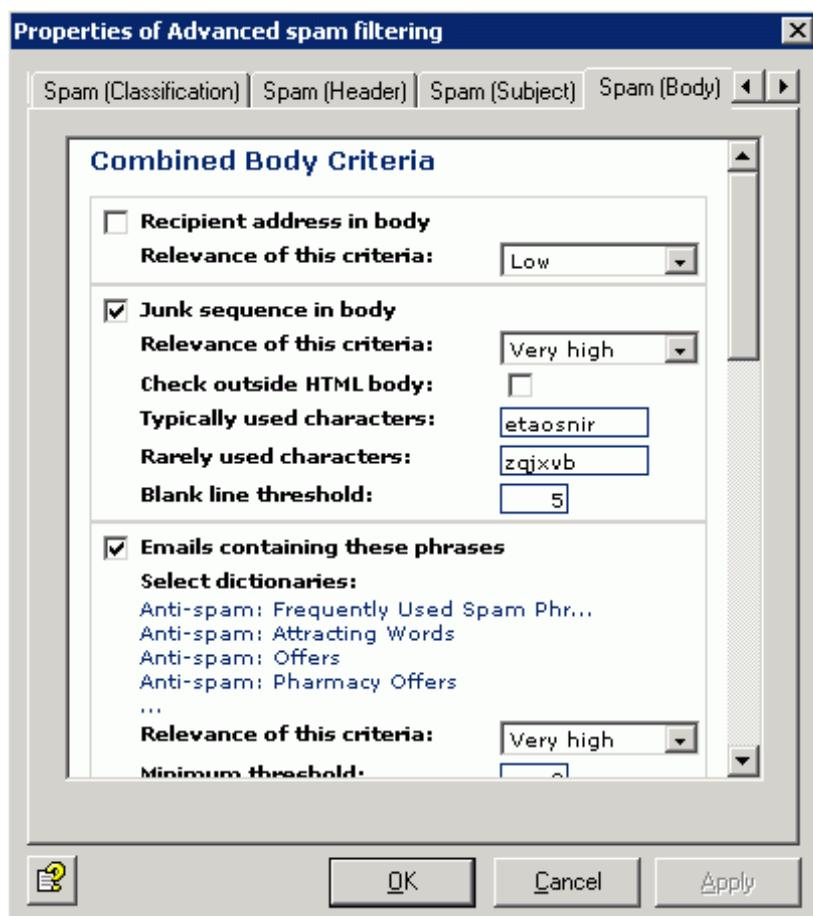
1. If the affected emails always lie just above the spam probability threshold, you should firstly set this threshold a little higher to avoid the incorrect classification in the future.
2. If you are regularly in contact with the sender of incorrectly classified emails, you should create the sender as a contact in the Active Directory or enter the sender in the whitelist (**Definite Criteria - Definite "No Spam"-Criteria**) so that these emails can be omitted from the check in the future.
3. Try to identify typical business terms for your operational environment in the emails affected and enter these terms in the Business Words dictionary. In future, the job will take these words into account using the **Ham phrases in message text** "no-spam" combined criterion and will consider emails that contain these words as less likely to be spam.
4. If despite the adjustments in points 1-3, the incorrect classifications are still not at an acceptable level, you should use the cause description in the quarantine or also the **Spam analysis details** notification variable to find out which criteria in the incorrectly classified email returned spam indicators. If this is repeatedly the same criterion, then this criterion is probably not meaningful enough for your operational environment: You should therefore lower its significance by reducing the **Relevance of this criterion** under **Combined criteria** by one level. The job then does not attach as much significance to this criterion when determining the spam probability.
5. If you are very familiar with the features of your usual email (spam and no-spam), you can use the **Combined Criteria in Advanced Configuration** to optimize the individual criteria to your operational environment. This can be particularly useful if you want to greatly reduce the relevance of a criterion or you need to disable a criterion completely in order to exclude incorrect classifications. The downside is a noticeable reduction in spam detection. For more information on this subject, see [Anti-spam for experts](#).

7.3 Anti-spam for experts

Definite and combined spam criteria can be set in the spam filtering job. The **definite criteria** imply an immediate decision one way or the other (spam or no spam) and are immediately assigned the label "Spam Probability is 0% = **None**" or "Spam Probability is 100% = **High**". The **combined criteria** are only applied if the definite criteria were not met. Several analysis mechanisms (criterion tests) are implemented in parallel for actual spam detection with combined criteria and are then "combined" after the email has been analyzed. Each criterion has a relevance of its own for the overall result (the individual value of this criterion); this relevance can range from **Low** to **Very High**. The criterion is disabled by clicking in the checkbox. In addition, most criteria can also be assigned an individual value for **Minimum** and **Maximum**. These two values relate to the word lists that the criterion uses to scan emails, for example. If the minimum value is not reached, this criterion is ignored for the relevant email in the overall evaluation. If the maximum value is reached, **this criterion** decides: "This is spam!".

Warning: The message "**This is spam!**" only applies to the specific individual criterion, whose maximum value is achieved by analyzing the email. Because this spam analysis always involves an analysis with combined criteria, the other criteria can also "decide differently" and can "out-vote" the original criterion when taken in combination. You will find more information in the example below.

7.3.1 Combined criteria - example



In the **Emails containing these phrases** combined criterion in the **Spam (Body)** tab, you are using the **Anti-spam: Frequently Used Spam Phrases** dictionary, among others, to scan the message text of all incoming emails for spam. This dictionary is set with a value rating of 5. If a word/phrase from this dictionary, e.g. "check it out", is found in an email, then this word/phrase is evaluated and counted with 5. You then specify the number of words from which this criterion is to be taken into account in the overall evaluation (**Minimum value**) and when your individual "spam measurement" for this criterion is full (**Maximum value**). For this, add together the value ratings of the words to be found. If you specify a value of 30 here (as in our preconfigured job), then 6 different words from the dictionary must be found in the email in order to be fully classified as spam for this criterion, as the value rating of the dictionary and the words contained in it = 5. If, for example, only 3 different words are found here, this email is not "fully" spam for this criterion but the probability is fairly high. From another dictionary with the value rating = 10, 3 hits would of course be enough for the "full" spam indicator.

Note: If the same word occurs several times, it is only counted once. Therefore, in this example, if the phrase "check it out" occurs three times in the email, this term only counts as 5 in total and not 15 (unlike in a normal Wall Content Filtering job).

Also specify the **Relevance of this criterion**. If you have set this to **Very high**, the criterion will be taken into account accordingly in the overall evaluation.

7.3.2 Combining the information on spam probability

The individual value ratings of all combined criteria are then weighted according to their set relevance and an overall value rating is calculated. The job compares this overall value rating (= spam probability of the email) at the end of the scan with the three threshold values to be set individually and assigns the email to one of the four spam probability ranges (**None to High**). Together with other combined criteria, our sample mail with the 3 words found from the dictionary with a value rating of 5 can therefore still fall into the "That is spam" range in the overall calculation.

In this example, our email with the 6 words found from the dictionary with a value rating of 5, which in this criterion received the "That is fully spam" stamp could also have received the spam probability **None** or **Low** when calculated together with other criteria and therefore have received the "That is probably not spam" stamp as an overall result at the end.

The overall rating is derived only from the criterion relevance, the minimum and maximum values and the individually set e-mail.

The individual combined criteria can be found on four tabs under **Advanced Configuration**.

The following tables provide an overview of the combined criteria contained in the job.

Note: For further information on combined criteria, please contact Avira support.

Combined no-spam criterion

Criterion	Description
Ham phrases in the message text	Checks whether words from the typical business vocabulary of the user are found in the message text of the email.

Combined classification criteria

Results from other spam detection products are included here and often only one spam detection feature of each product is used. The specific disadvantages of the individual products are eliminated through combination with other criteria in the Wall Spam Filtering job.

Criterion	Description
Exchange SCL value	<p>See also Definite "no spam" criteria and Write spam result in Exchange SCL field</p> <p>The Intelligent Message Filter (IMF) determines the probability of an email being spam. The result of this calculation is the so-called Spam Confidence Level (SCL). It can have integer values between -1 and 9. The higher the SCL, the greater the probability of spam. With this criterion, the SCL value of an email can be included in the spam evaluation of the iQ.Suite.</p> <p>For further information, see also http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/Avira</p>
Avira AntiSpam results	To detect spam, Avira AntiSpam conducts a comparison between known patterns and the incoming email.

Combined header criteria

Criterion	Description
Suspicious sender properties	Checks whether the "From" header exists and contains an entry and whether it matches the sender of the SMTP protocol.
Suspicious recipient properties	Checks whether the "To" header exists and contains an entry and whether at least one of the SMTP recipients is in the "To" or "Cc" header.
Numbers in sender address(es)	Checks whether one of the sender addresses (SMTP or email header) contains numbers.
Number of recipients per e-mail	Checks the number of recipients for an email.
Known spam X-Mailer	Checks whether the X-Mailer entry in the email is a known spam mail client.
Known spam results	Takes the result of a previous spam analysis for the classification of emails as spam or no-spam into account. The result (number of spam indicators found) is written to the X-header of the email. Avira AntiVir Exchange evaluates the X-header and writes the number of spam indicators to the criterion. The evaluation takes place using the minimum/maximum number of possible spam indicators. The result may originate from an external system or may have been calculated from the Avira AntiVir Exchange of another server.

Combined subject criteria

Criterion	Description
No subject	Checks whether the subject field exists and contains an entry.
Recipient address in the subject field	Checks whether the subject of the email contains the part of the recipient address before the @.
Junk string in the subject field	Checks whether long strings of hidden characters (spaces) and meaningless junk strings occur in the subject of the email.
Phrases in the subject field	Checks whether words from the typical spam vocabulary are found in the subject field of the email.
Disguised words in the subject field	Checks whether disguised words from the specified dictionary (dictionaries) are found in the subject field of the email.

Combined message text criteria

Criterion	Description
Recipient address in the message text	Checks whether the message text of the email contains the part of the recipient address before the @.
Junk string in the message text	Checks whether long strings of hidden characters and meaningless junk strings occur in the message text of the email.
Phrases in the message text	Checks whether words from the typical spam vocabulary are found in the message text of the email.
Disguised words in the message text	Checks whether disguised words from the specified dictionary (dictionaries) are found in the message text of the email.
Suspicious HTML code	Checks whether HTML constructs are found in the message text of the email.
Suspicious HTML links	Checks whether spammer links are found in the message text of the email.
A large number of HTML links	Checks whether the message text of the email contains a large number of HTML links relative to the size of the text.
Embedded images	Spam content that is transported by means of embedded images (internal reference to attachments) can be detected with this criterion. For example, it is therefore possible (in configurations without AntiSpam) for all emails with embedded images to be considered spam if embedded images are not a component of the regular email communication of the operational environment.

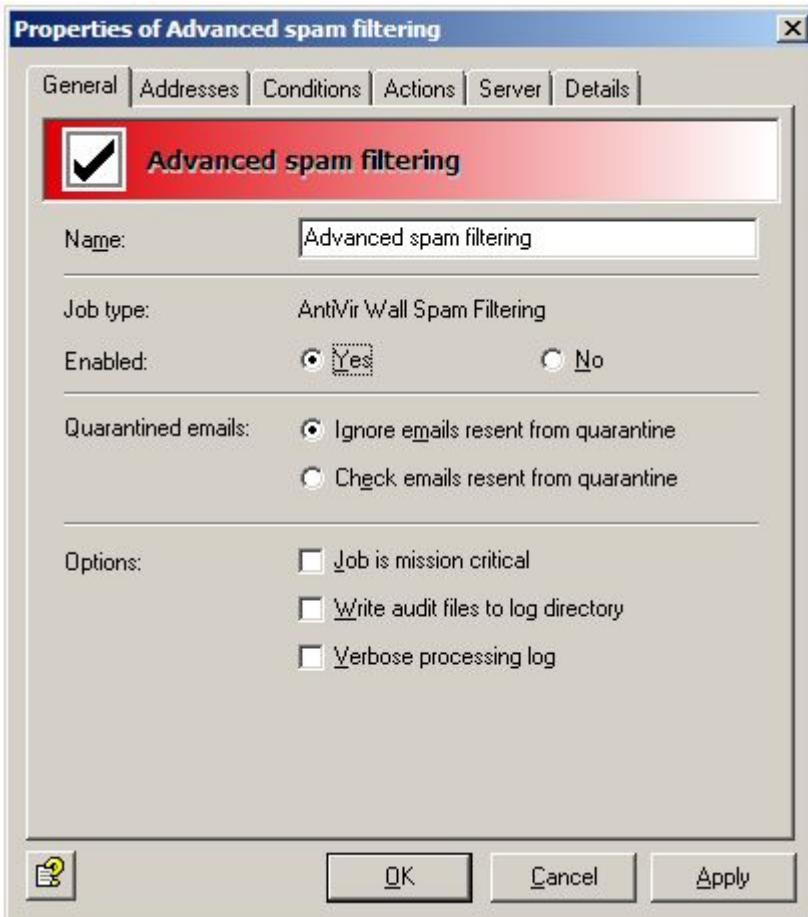
7.3.3 AntiSpam scanning - Sample job

Warning: For your own security, the **Filtering for Spam with Avira AntiSpam** is preconfigured and preactivated. This job can be found under **Mail Transport Jobs**.

You will also find a job for anti-spam scanning under **Policy configuration - Sample jobs**. Copy the **Advanced Spam Filtering** job to **Mail Transport Jobs** and double-click to open it. This job examines emails on the basis of special spam instructions.

General AntiSpam scan

You can assign a name of your own to the job in the **General** tab. **Enable** the job. The job is enabled as soon as you save your settings with OK and close.



This job will not process mails resent from quarantine, even if the send option **Recheck email with AntiVir jobs** has been activated when sending emails from **Quarantine (AntiVir Monitor - <Select Email> - All Jobs - Send emails from quarantine)**. The **Ignore emails resent from quarantine** option means that this job is generally skipped when mail is sent from quarantine.

For more information about resending emails from Quarantine see [Sending emails from quarantine](#). The "AntiVir scan engine" chapter explains the [Job is mission critical](#) option in more detail.

Note: This job contains the **Subject extension** on the **Actions** tab.

Setting address conditions

You can use the **Addresses** tab to restrict the senders and recipients for whom this job is to apply. Select all addresses from existing address lists or from lists you have created yourself.

For the best way to use address lists and for a precise description of the procedure see [Address lists](#).

Setting content conditions

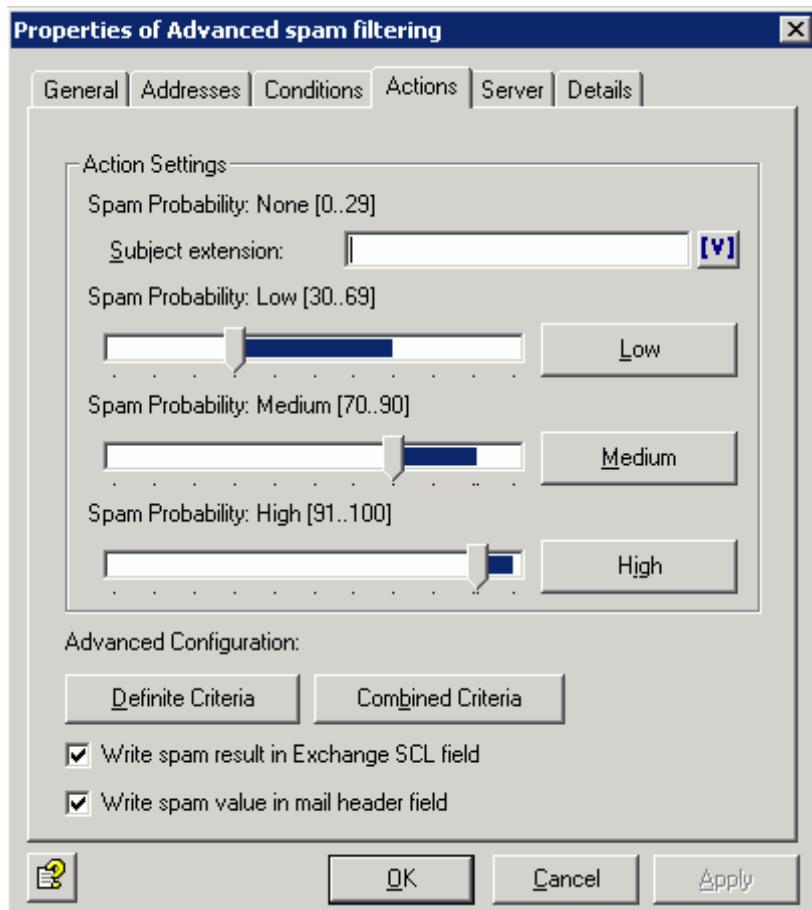
You can use the **Conditions** tab to set the conditions for executing a job.

For the best way to use conditions, see [Conditions](#).

Warning: In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (AND connector).

Defining actions

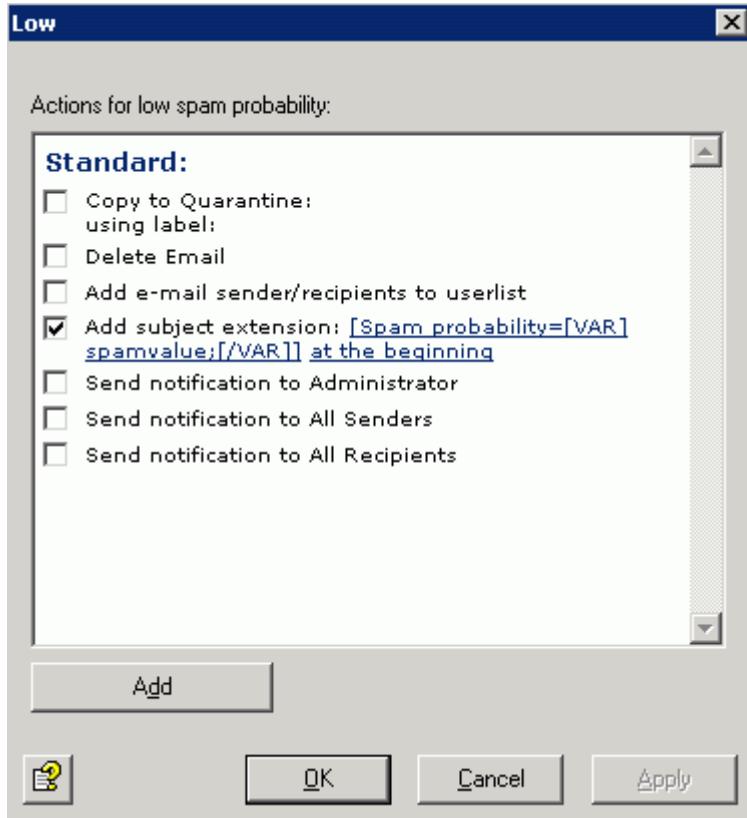
The **Actions** tab is used to define the spam probabilities and what is to be done with any detected spam.



The following spam probabilities will be defined in this example:

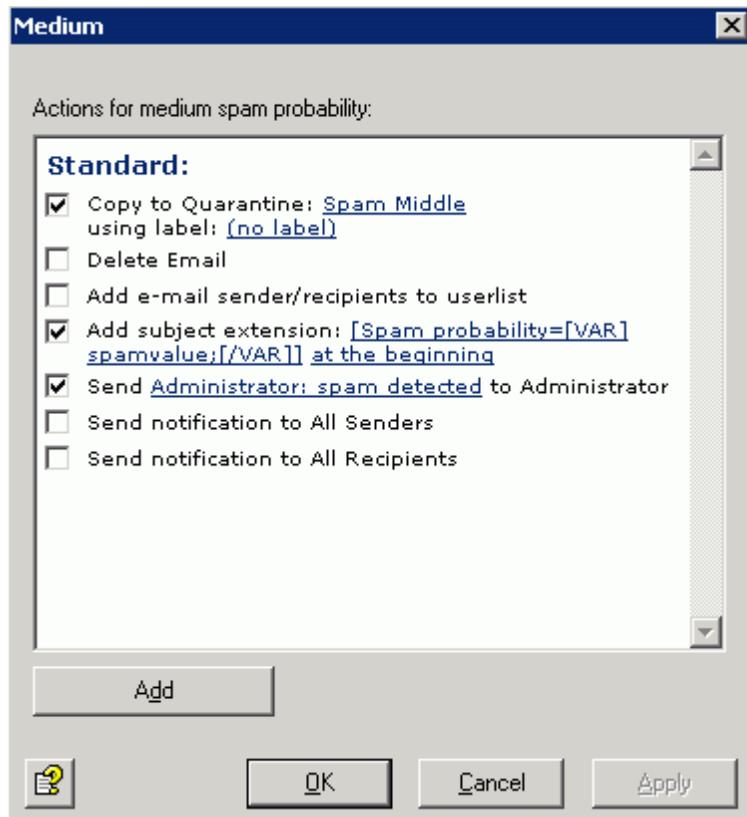
- Normally, no action is carried out in the range **Spam Probability: None** (value = 0-29). The only possible action in this probability range is a **Subject extension** which can be configured directly within this tab. It would be possible to add a subject extension such as Anti-spam checked, etc.
- Set the actions on a separate tab for the range **Spam Probability: Low** (in this case set between 30 and 69). Click the **Low** button.

You will see the following dialog:



The only action is to add the spam probability to the subject line.

To configure the actions in the range **Spam Probability: Medium** (in this case set to 70 - 90) click the **Medium** button. You will see the following dialog:



As an action, a copy of the email will be placed in quarantine and the administrator will be notified. The original mail is delivered to the recipient. Another action is the **Subject extension**, which notifies the recipient of the probability of spam in this email (e.g. Spam Probability = 75). The higher this value, the more certain the recipient can be that this email is not very important. Medium spam probability is intended for emails that may or may not be spam. Lower values in this setting mean that a medium probability can be assumed for spam if only a few criteria have detected massive spam indicators or numerous criteria have detected a small number of spam indicators. It is recommended that these emails should be gathered in a separate quarantine area (**Anti-spam: Medium**) area and that it should be left up to the users to decide what to do with these emails.

Note: Users can be notified of the spam mails in a quarantine area by means of quarantine summary reports. You can also arrange for the Exchange Store to redirect the emails directly to the user's junk folder using the Microsoft SCL value (see also the next section). The configured **Subject extension** indicating the spam probability value enables every user to decide how this email will be handled, possibly even with a filter in Outlook.

Writing the spam result in the Exchange SCL field

Microsoft supplies its own spam filter, starting from Service Pack 1 for Exchange 2003 and Outlook 2003. This Intelligent Message Filter (IMF) determines the probability that an email is spam. The result of this calculation is the so-called Spam Confidence Level (SCL). It can have integer values between -1 and 9. The higher the SCL, the greater the probability of spam. An SCL of 0 means that the email is unlikely to be spam, while the value -1 is assigned for emails to which the filter was not applied at all, for example internal emails from senders in the same Exchange organization. The Exchange-SCL value can automatically trigger certain actions, such as the forwarding of emails to users' junk mail folders in Outlook 2003, without users having to do anything. The "Exchange System Manager" allows you to make central definitions for what is to happen to emails at a particular SCL threshold. The action no longer needs to be defined on the system that performs the evaluation. Because the IMF writes the SCL value into the email, the required action can only be taken by the destination system. This requires that the email gateway must also be run with Exchange 2003.

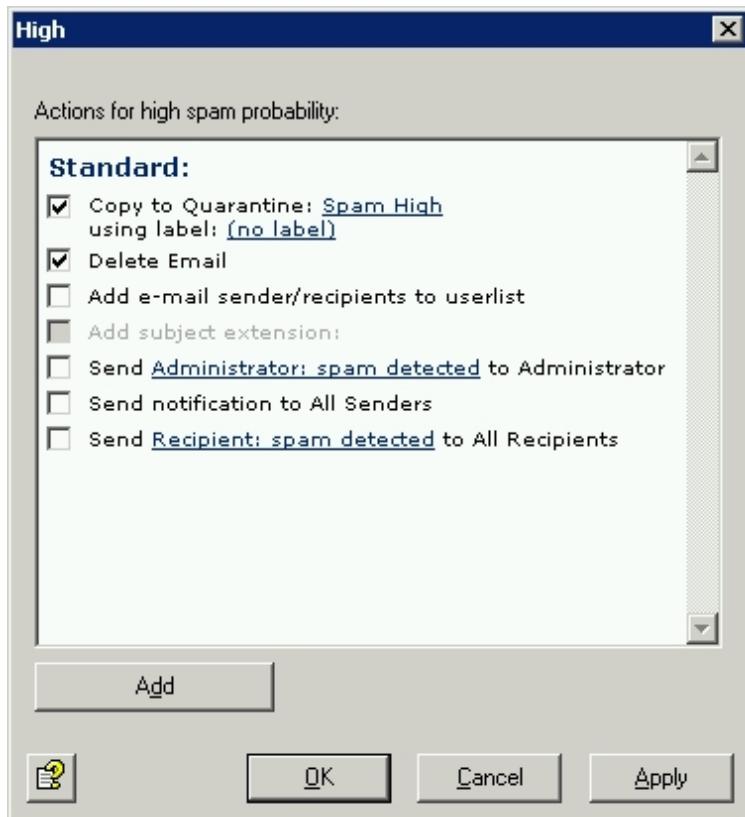
Even if you cannot use the IMF, or do not wish to do so, you can use this option to define the spam probability value for the spam filtering job as an SCL result, so that you can use the Exchange Store functionality for the possible actions or for further processing purposes. The spam probability value is converted internally to the SCL values, so that Outlook can recognize them.

Note: If you use quarantine summary reports, users will be informed about all relevant spam mails. In this case you can dispense with the Exchange Store redirection of emails to the junk mail folder. For more information about the Exchange SCL field, see
<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx>

Writing the spam result in the mail header

The spam probability value is added to the email header for all three spam probabilities (low, medium and high). This involves converting the result value into a series of stars (1 star indicates a value up to 10, 2 stars a value up to 20, 3 stars up to 30, etc.) so that an Outlook rule can be applied. You can also define the result separately for each spam probability by selecting **Add - Add X header field** under the **Actions** tab. In this case the result is not converted into a series of stars but is output directly as a value.

To configure the actions in the range **Spam Probability: High** (in this case set to 91 - 100) click the **High** button. You will see the following dialog:



High Spam probability is intended for emails that really are spam and hence should not be delivered. The original mail is immediately deleted and is not delivered to the recipient. A copy of the email is sent to quarantine. Because of the current volume of spam, no notifications are sent to the administrator.

Note: When email volumes are high, quarantines can quickly become very inflated, impacting negatively on email throughput. If you no longer need the emails, you should deactivate the low and high quarantine copy.

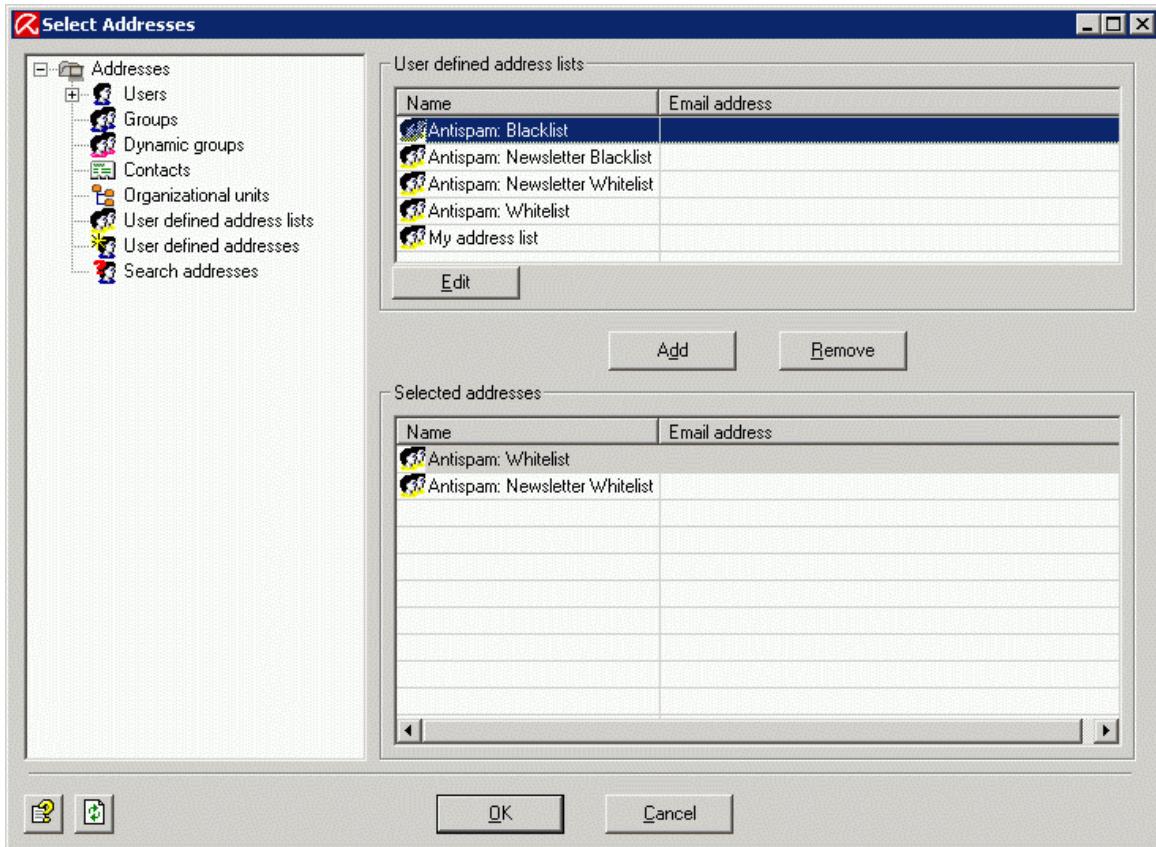
Note: Depending on your productive environment, it may be reasonable for you to set the probabilities for the **Medium** and **High** ranges differently. It is probably best for you to spend some time in advance examining whether the job achieves good results with this email in your productive environment.

The aim should be

- as many spam mails as possible in the **Anti-Spam: High** quarantine,
- as many ham mails as possible in the **Anti-Spam: Low** quarantine
- and therefore as few emails as possible in **Anti-Spam: Medium**

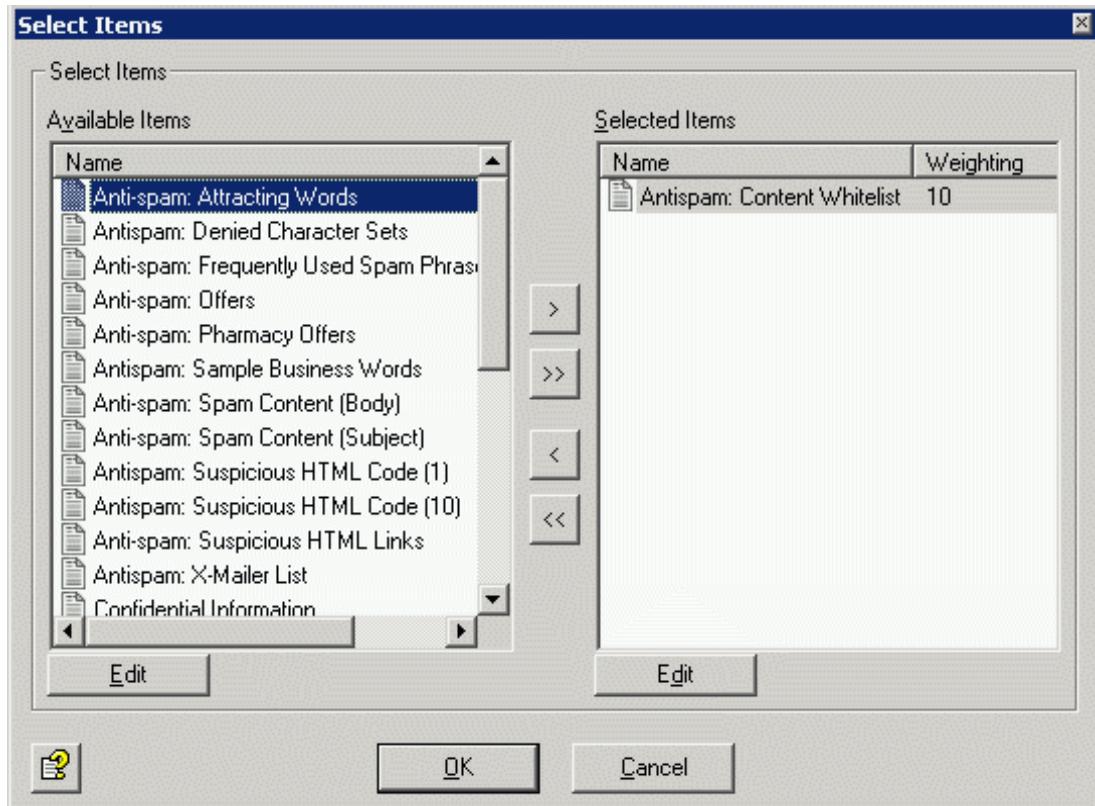
You can adjust the spam criteria in the **Actions** tab. Click **Definite Criteria**. You will see the following dialog:

If you wish always to permit emails from particular senders, in the **Emails from these trusted senders (whitelist)** criterion, click on the **Anti-Spam: Whitelist** and **Anti-Spam: Newsletter Whitelist** lists. You will then see the address drop-down list:



Select the addresses here or specify your own email addresses which are always to be permitted as senders. The * (asterisk) and ? (question mark) symbols can be used as wildcards. This means that you can specify domains in the form *.domain.com. Once you have entered your addresses, click **OK**.

You can now adapt the next criterion **Email subject containing these words** in the Definite "No Spam" Criteria dialog. Click **Anti-Spam: Content Whitelist**. You will then see the dialog for selecting the dictionaries:

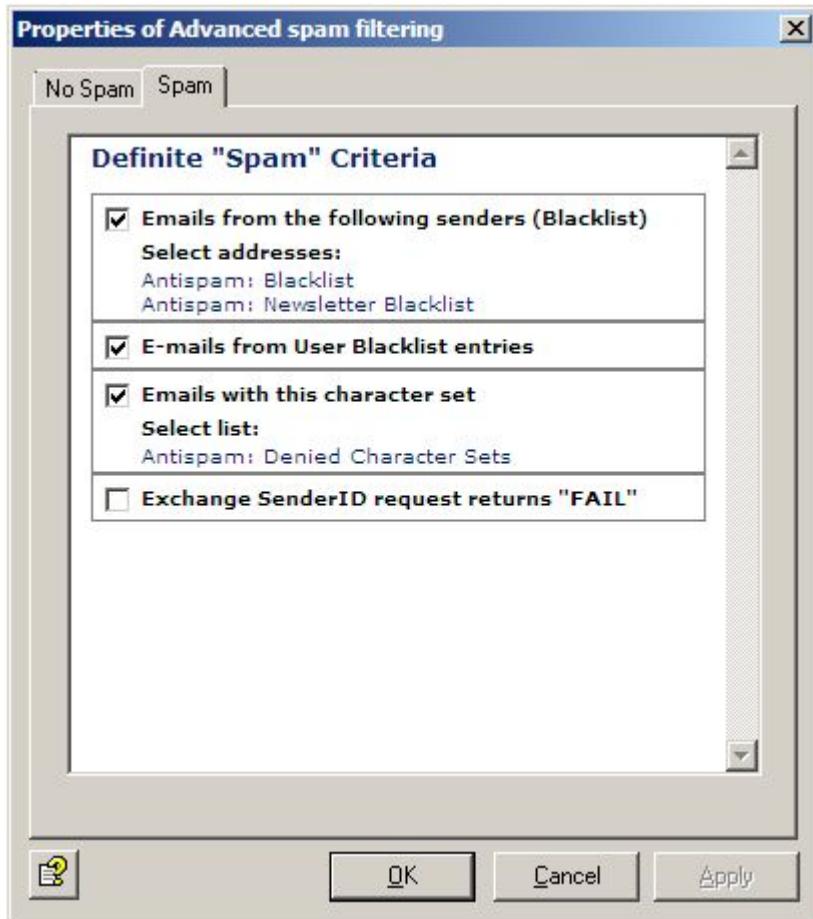


The arrow keys **<** and **>** can be used to add and remove dictionaries in the list. The double arrows add or remove all marked dictionaries. Click **Edit**. You will see the following dialog:



You will see more information about creating dictionaries in [dictionaries](#). There is a further description of the other criteria under [Definite No Spam Criteria](#).

Once you have completed the word list and confirmed it twice with OK, click the **Spam** tab:



In the **Emails from the following senders (Blacklist)** field click on the list with **Anti-Spam: Blacklist** and **Anti-Spam: Newsletter Blacklist**. You will once again see an address dropdown list and can add your own email addresses or domain names.

Note: Both the whitelist and the blacklist should be kept correct and up-to-date!

In addition, by selecting a specific character set you can declare emails from particular regions as definite spam. Enable the checkbox next to **Emails with this character set** and click **Anti-Spam: Denied Character Sets** then open the relevant list for editing. Each line contains the code for one character set. The **Details** tab shows the correspondence between the various countries and a character set. If you have communication partners in the countries whose character sets appear in this list, you should modify the list as follows:

1. Copy the **Anti-Spam: Denied Character Sets** list under **Basic Configuration - Utility Settings - Word Lists**.
2. Give your list a new name.
3. Delete the character sets corresponding to the countries of your communications partners from the list.
4. Save the list.
5. Delete the **Anti-Spam: Denied Character Sets** list in the **Advanced Spam Filtering** job and set your own list under **Definite Spam Criteria - Emails with this character set**.

Note: This function solely checks the “charset” header field in the email. For this option you should make sure that you only select the relevant character set list(s) and no other word list.

Selecting servers

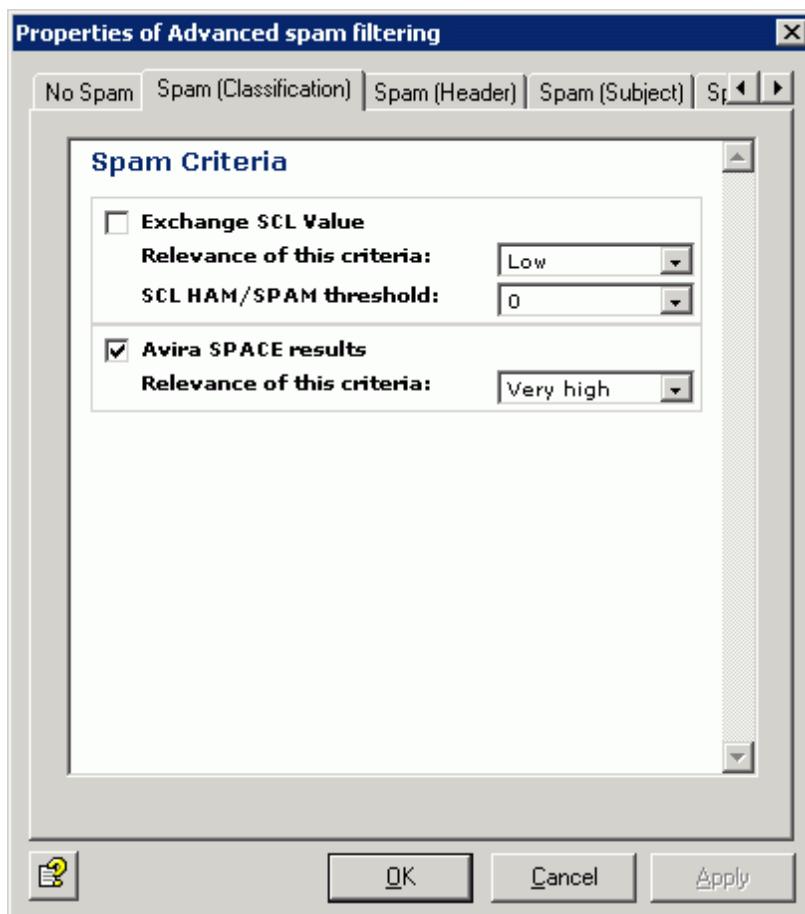
Servers are selected as described in [Selecting servers](#).

Saving the configuration

Save the configuration of the Avira AntiVir Exchange Console every time you make changes. To do so, click the  button. The configuration is saved in the *ConfigData.xml* file, which is stored in the *Avira\AntiVir Exchange\Config* directory. Open changes are indicated by (*) at the uppermost node.

7.3.4 Configuring advanced spam filtering jobs

1. Under **Mail Transport Jobs** open the **Advanced Spam Filtering Job**. Enable the job and retain the default settings.
2. In the **Actions** tab click **Combined criteria - Spam (Classification)** and enable the **Avira AntiSpam results** criterion. You are advised also to retain these settings.



Relevance of criteria: Define the relevance (weighting) for the entire criterion (ranges from low to very high). The values for relevance and the coefficient are multiplied and together yield the result for this criterion

3. When this job is enabled, the configured AntiSpam Engine is also enabled automatically.

7.3.5 Manual AntiSpam configuration

If you do not want to use the Wall Spam Filtering job described above, it is recommended that you set up the following sequence in the job process to ensure an effective anti-spam configuration.

1. Address check for known spam addresses
2. Subject line check for text and for conspicuous features in the formatting, e.g. periods or spaces. See **Spam Content (Subject)** under **Dictionaries** in the basic configuration.
3. Message text check for spam links (e.g. also for redirections and click trackers). See the **Spam Links (Body)** dictionary under **Dictionaries** in the basic configuration.
4. Message text check for spam text and known typical conspicuous features such as HTML comments in a HTML mail text. See also the **HTML Spam Detector** dictionary under **Dictionaries** in the basic configuration.

Ensure that the jobs are executed in the correct processing order so that the checks are carried out as effectively as possible and the performance is optimized.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH. Errors and technical subject to change.

Issued Q2-2011

AntiVir® is a registered trademark of the Avira GmbH.
All other brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.



live free.™

© 2011 Avira GmbH. All rights reserved.
Errors and technical subject to change.

Avira GmbH
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com