

Avira **AntiVir** Exchange

Support
June 2010

www.avira.com

Errors in design and contents cannot be excluded
© Avira GmbH

Table of content

1. Installation AntiVir for Exchange	3
2. Licensing	5
3. Creation of new Email Filters.....	7
4. Configuration of the Email Filter	9
5. Activation of the Information Store Job	13
6. Quarantine.....	14
7. Summary Reports (Quarantine).....	15
8. Update Settings	18
8.1 Update via Proxy Server	19
9. Job recommendations	22
9.1 Remove Addition in subject.....	22
9.2 Block unwanted attachments	23
9.3 Advanced Spamfiltering mit separaten Quarantänen.....	24
9.4 Add receiver automatically to the whitelist	26
9.5 Password protected Archives.....	28

All necessary packages for the installation and all manuals as pdf-files can be found on our website:

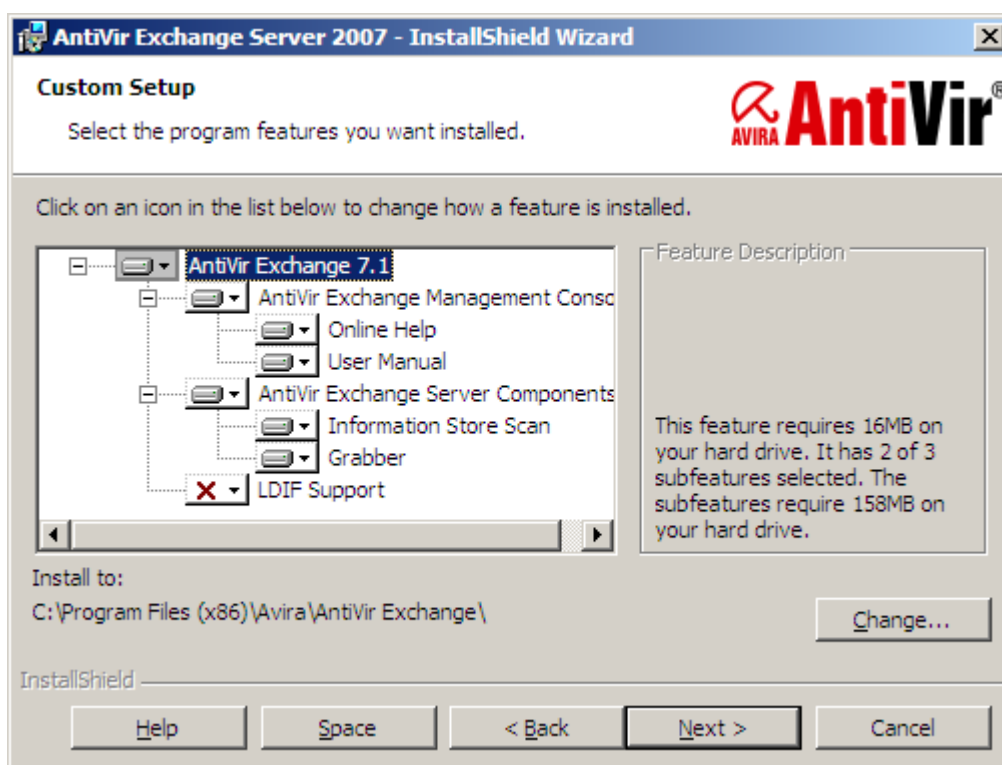
<http://www.avira.com> (<http://www.avira.com/en/download/index.html>)

Hint: There are different installation packages for the different MS Exchange systems! Please, make sure to use the right installation package (Exchange 2000/2003 or 2007).

1. Installation AntiVir for Exchange

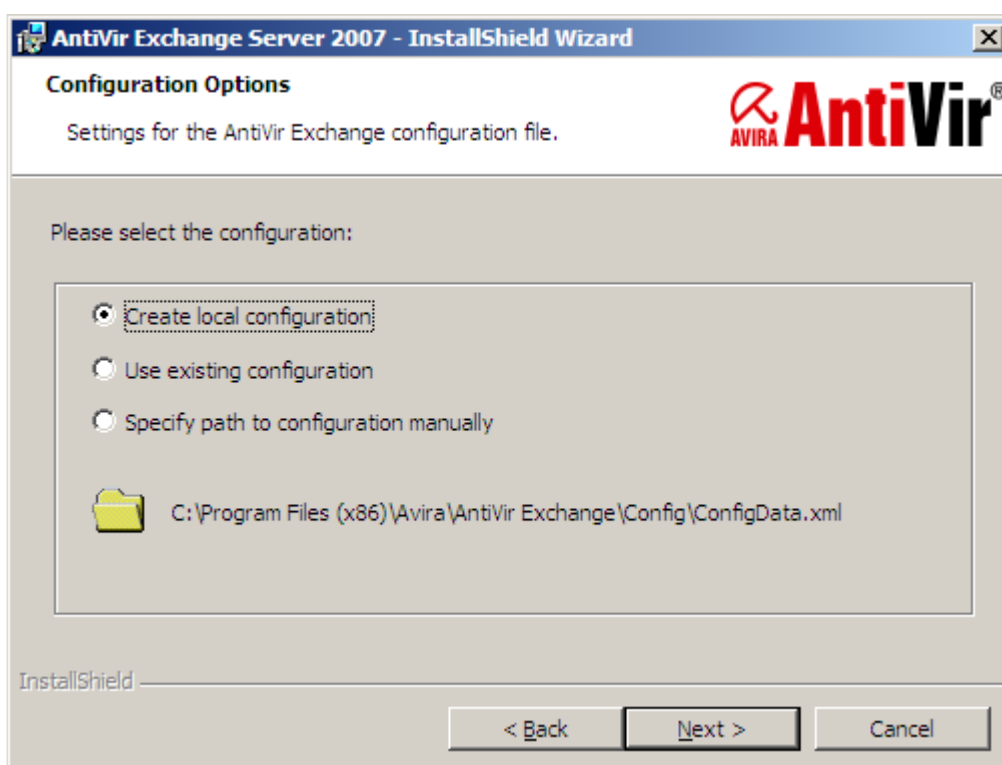
After downloading the installation package for AntiVir Exchange, please, start it on your Microsoft Exchange Mailserver.

During the installation a window appears which allows you to choose the components you want to install. Please, make sure that the management console as well as the server components are chosen here.



After choosing the components for installation the program will ask you if there is already an existing configuration. This window is important if you have already used an older installation of AntiVir Exchange which should be replaced now. You can choose one of three different possibilities:

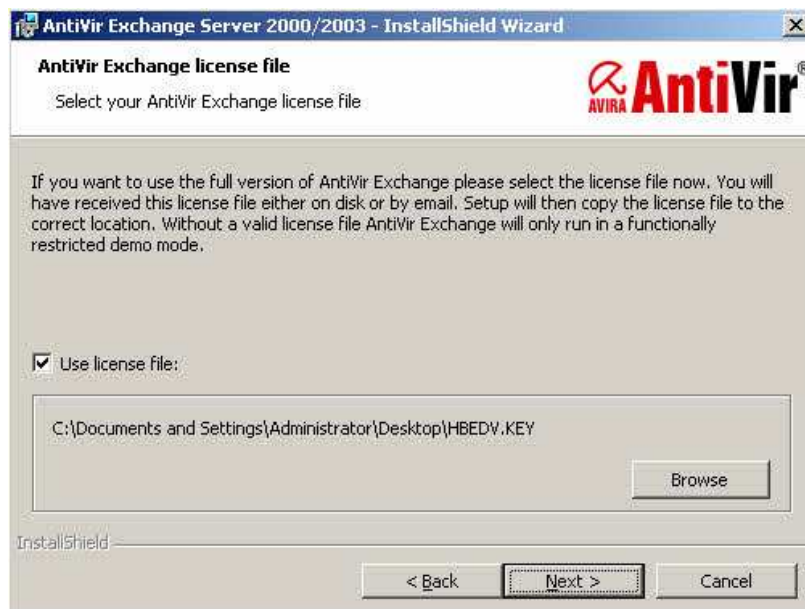
- **Create local configuration**
Choose this one for a first installation or if there is no existing configuration.
- **Use existing configuration**
The existing configuration will be kept for the new installation. The file configdata.xml has to be saved into the installation directory of AntiVir Exchange.
- **Specify path to configuration manually**
In case the configuration should be in a different directory you can enter the path here.
Important: The entered path cannot be changed afterwards!



During the following steps you have to enter some administrative pre-adjustments. These include the administrator's email address and a possibly existing proxy server for the internet update. These settings are saved to the configuration file "savapi.ini" during the installation, where they can be changed afterwards.

2. Licensing

During installation, the license file is requested and inserted correctly.

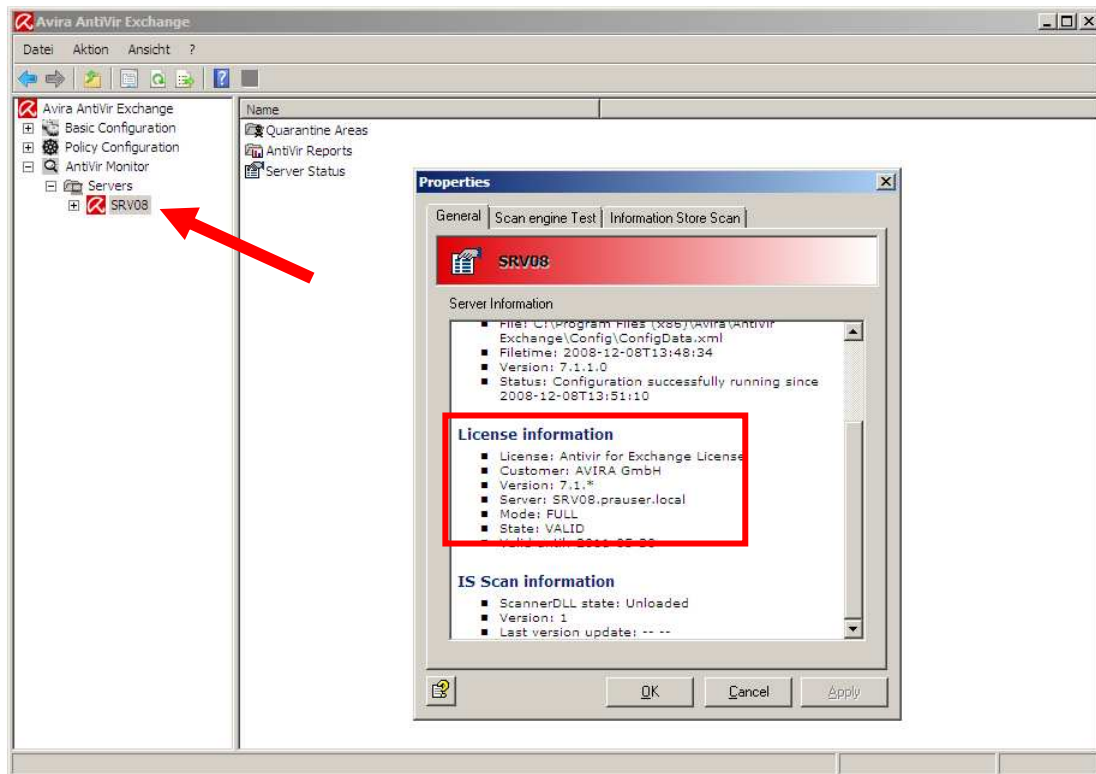


If you want to change the license later, please proceed as follows:

- Copy the file **HBEDV.key** which you have received via email into the installation directory of AntiVir Exchange. There is already a directory named "license" into which the file has to be saved. The directory "license" contains already a file named "oem.lic", which has to remain there.
- After copying the license file into the corresponding directory a restart of the service "AntiVir for Exchange Control" is necessary. During the restart you receive a hint that the service "AntiVir for Exchange" has to be rebooted too. Please, confirm with "yes".



In order to check if the licence file has been entered properly, start the AntiVir Exchange Management Console and open the menu AntiVir Monitor. Open the properties of the server in the following window in order to check the license information:

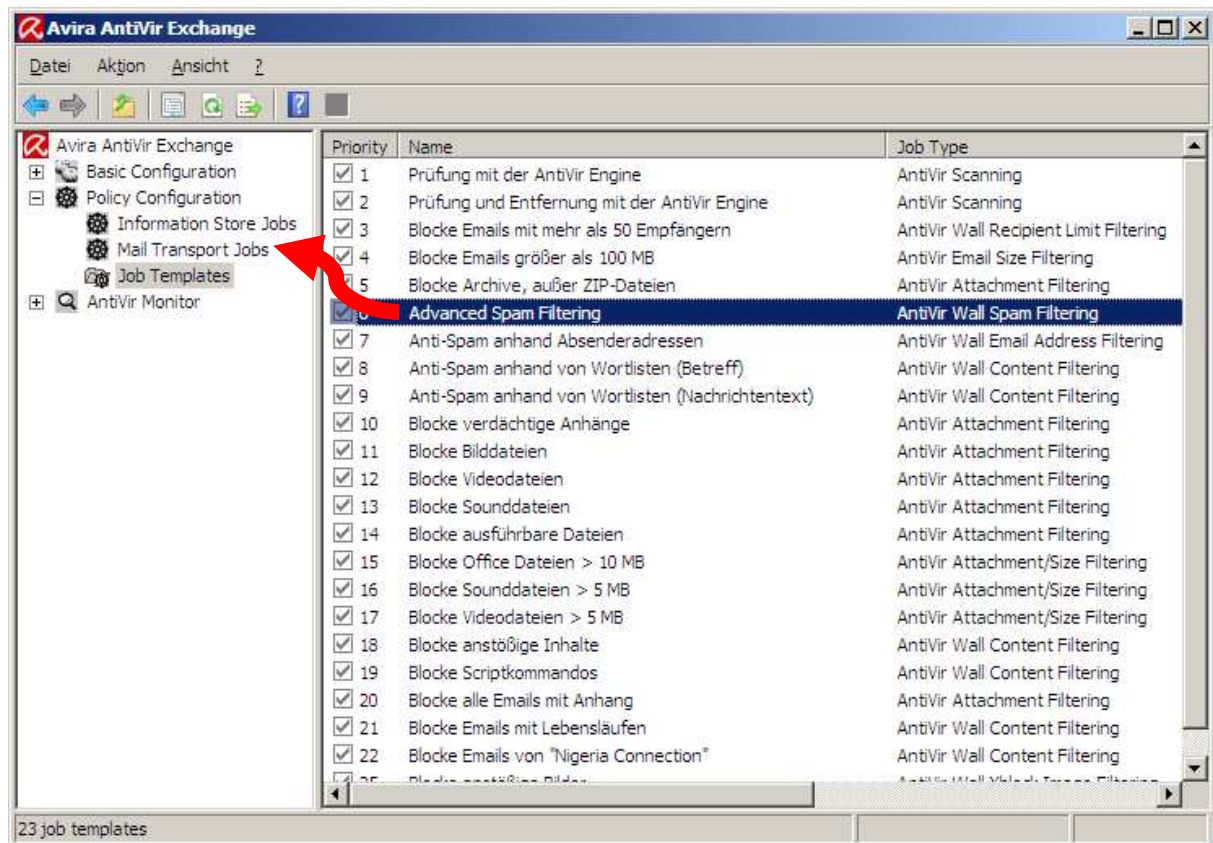


The license information is shown here. The values **Mode: FULL** and **State: VALID** show that the license has been installed properly and that it is valid. If it is not, please, check if you have used the right license file via the text file "lic_info.txt". Please, if necessary contact the Avira Support (support@avira.com) and send us the license file so we can check it.

3. Creation of new Email Filters

Directly after the installation the product is already preconfigured. Incoming emails will already be checked for viruses and moved into quarantine in case of a virus detection. In order to extend the email filtering and to set new jobs you can use the existing job templates.

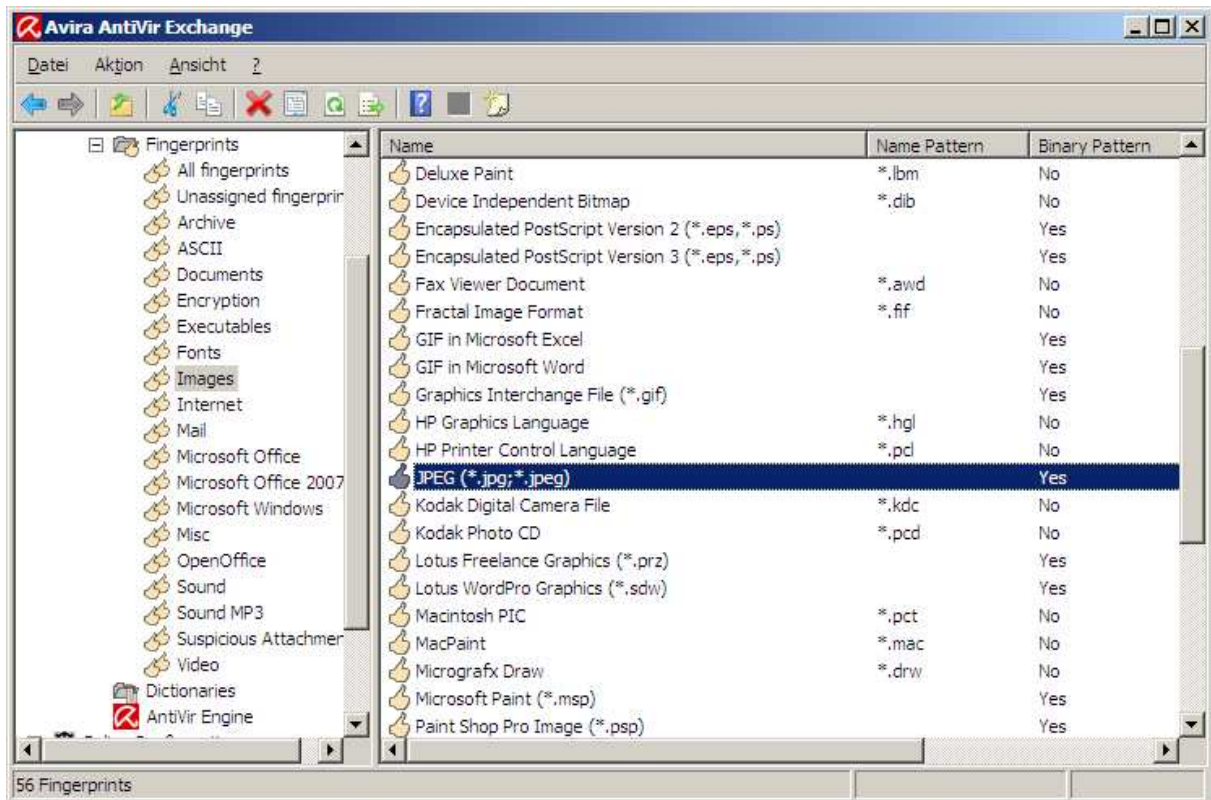
You will find preconfigured jobs which extend the already activated virus scanner with spam filtering or a content / attachment filter.



In order to activate a filter job you put it via drag & drop into the **“Mail-Transport-Jobs”**. There it can be activated and configured.

Hint: If you are not sure which filter to choose we recommend the “Advanced Spam Filtering” which contains several filtering methods and has a good detection rate.

Other jobs check the content of emails on the basis of fingerprints. A so called Fingerprint is the pattern of the specific file. These patterns are classified by the file extension or its binary code.



“Basic Configuration” → “Utility Settings” → “Fingerprints”

Single fingerprints are summarized in groups. The “Images”-group for example contains a multiplicity of known file extensions and patterns.

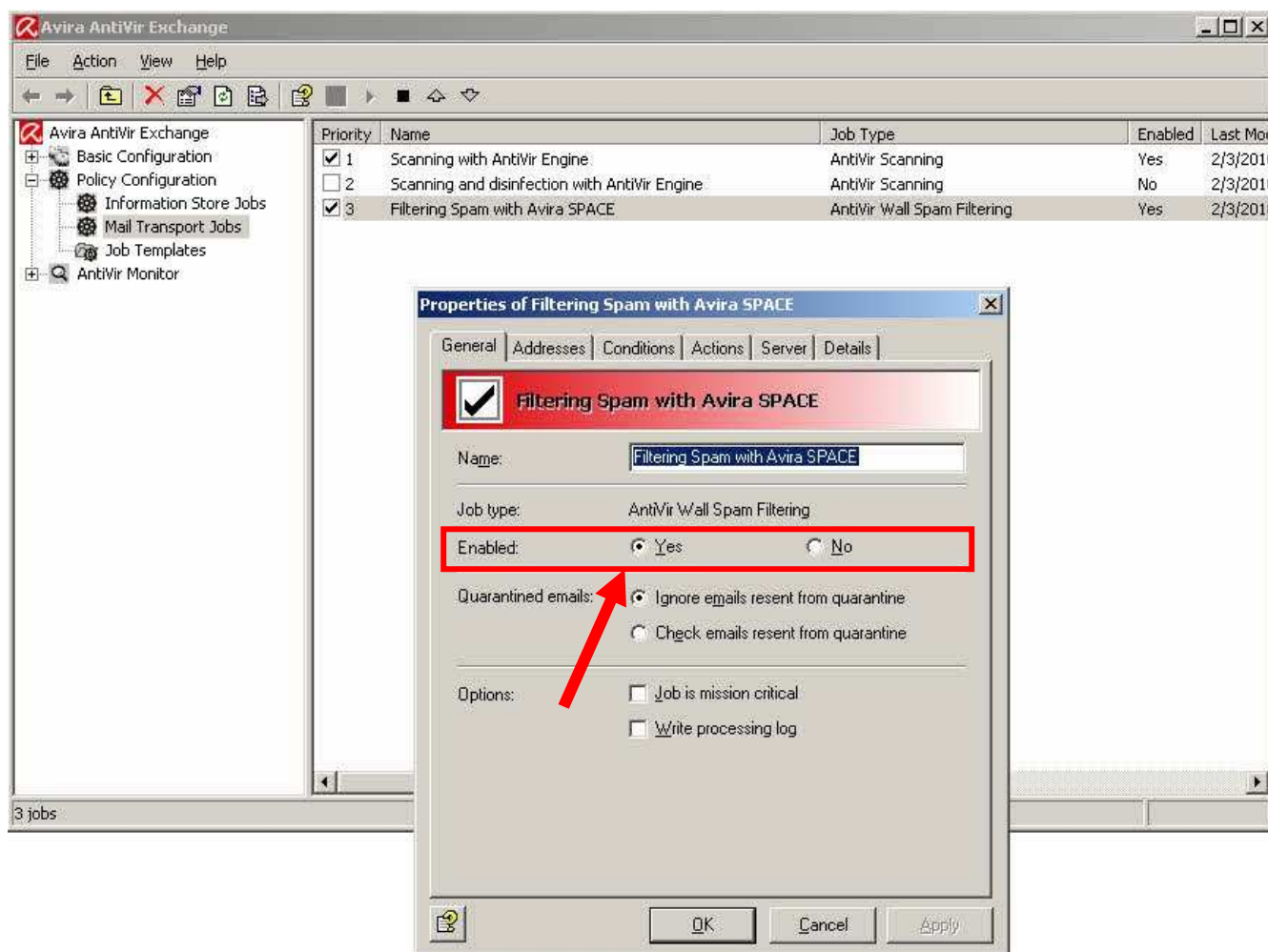
Such a fingerprint group (e.g. Images) is now being assigned to a job. This job filters emails and checks if it contains such a fingerprint.

job example:	function:
Block image files	This job accesses the fingerprint group “Images“, where it gets the information what an image file is and how to recognize it.
Block video files	It is the same principle as before. The difference is the group and so the patterns. Accessed group: “Video“
Block archive, except ZIP-files	This job accesses the fingerprint group ” Archive “. But the fingerprint “ ZIP Archive “ is set as an exception in the properties of this job.

4. Configuration of the Email Filter

As most of the filters are already preconfigured an adjustment is not necessary. If you should not use these default settings the filters can be adjusted individually. In order to open the properties for the configuration you double click on the chosen job and a window with the properties opens automatically.

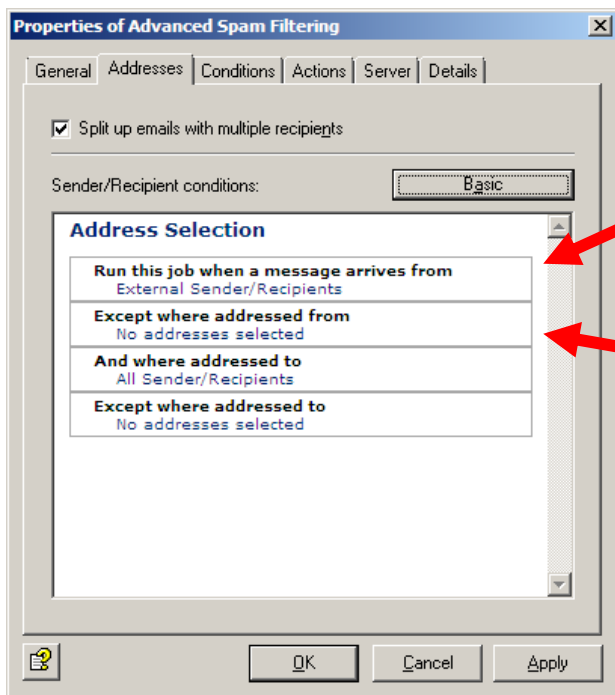
Hint: The addition [AntiVir checked] which appears in the subject of an email is added by the job “Check with AntiVir search engine”. If you don’t want this addition you can remove it via the properties of the job.



Every new job is deactivated by default. In order to activate it, please, change the settings in the tab “**General**” to enabled: “**yes**”.

Every job is valid for all incoming and outgoing emails. In order to change this and to use black- / whitelists, please, go to the tab “**Addresses**”.

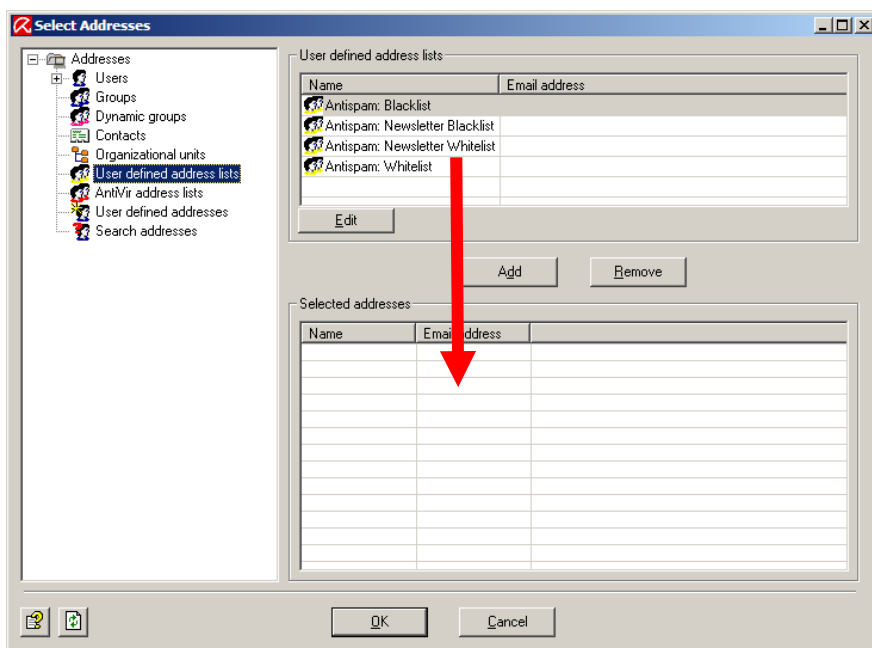
Via the menu point **Advanced** the window changes and you have the possibility to enter addresses/address lists as exceptions.



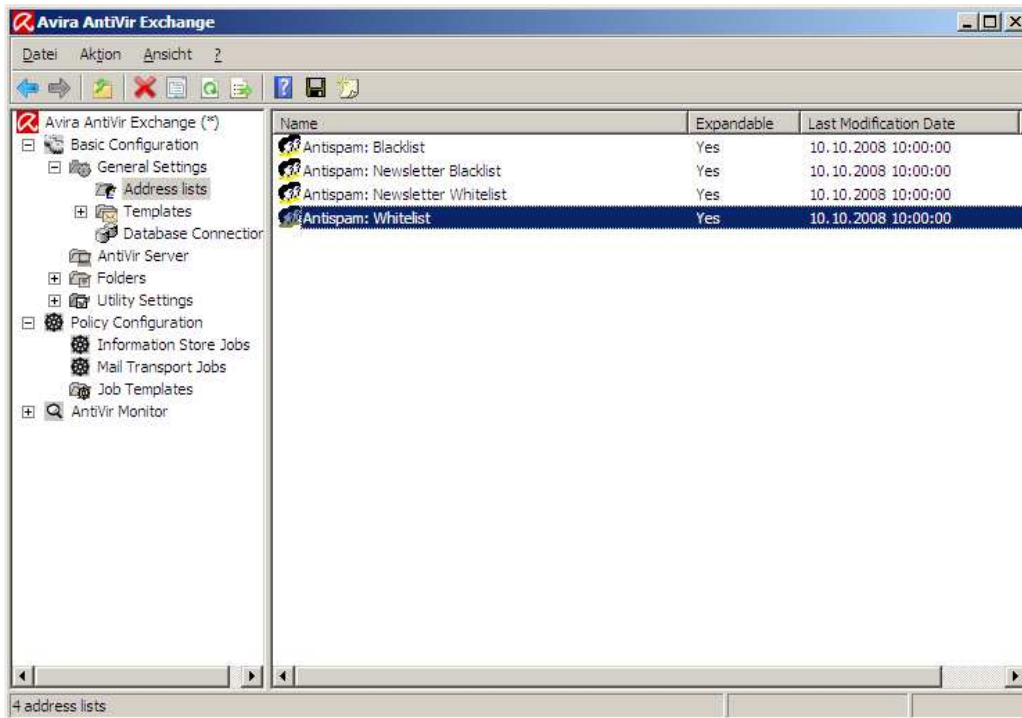
Every email from external or to external will be checked by this job.

You can add own addresses or address lists which are excepted from the job. (e. g. whitelists)

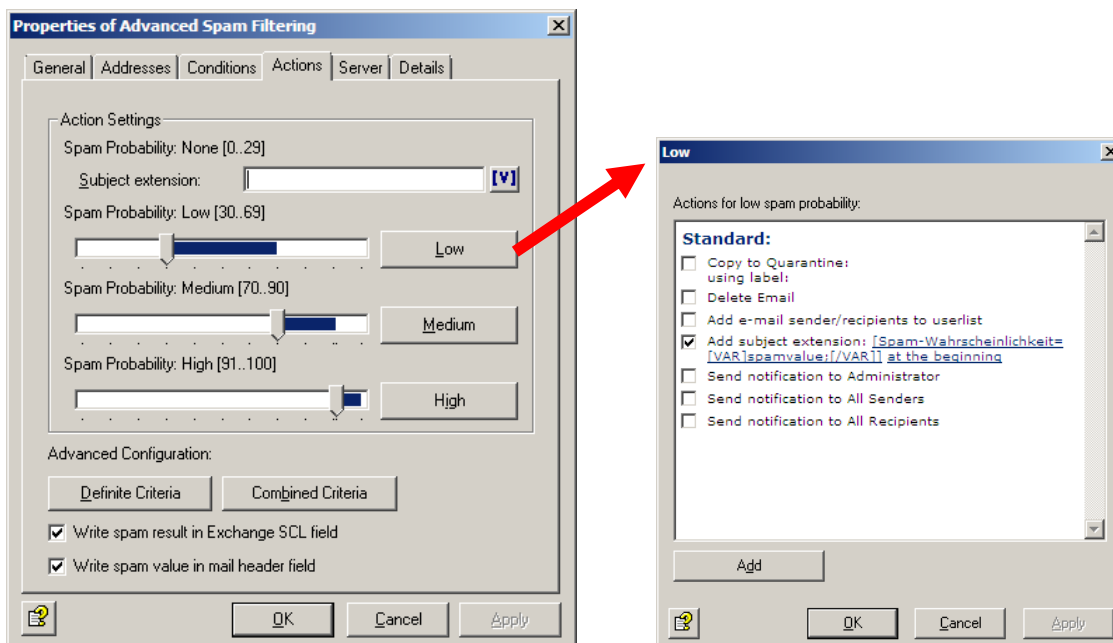
As you can see in the screenshot the addresses can be adjusted. Via a simple mouse click on “No addresses selected” in the menu “Except where addressed from” you can add an address list. All senders that are entered in this address list will be excepted from this job. That means the emails will be sent to the recipient in any case.




If you decide to use one of the entered lists an adjustment might be necessary. This adjustment can be done afterwards via the program menu “**Basic Configuration**” → “**General Settings**” → “**Address lists**”.



In order to decide what should happen in case of a classification as spam / virus you can adjust the settings in the tab “Actions”. You have different possibilities due to the different spam probabilities.



The tab “Actions” has to be configured separately for every job. Changes are only valid for this particular job.

After finishing the configuration, please, confirm it with a click on “OK” and save the changes in AntiVir Exchange via a click on the diskette symbol .

Hint: Without saving the changes, they are not applied and cannot work. This concerns all changes in the program.

Definite Criteria:

This means criteria that classify an email definitely as “SPAM” or “no SPAM”.

There are values like e.g.

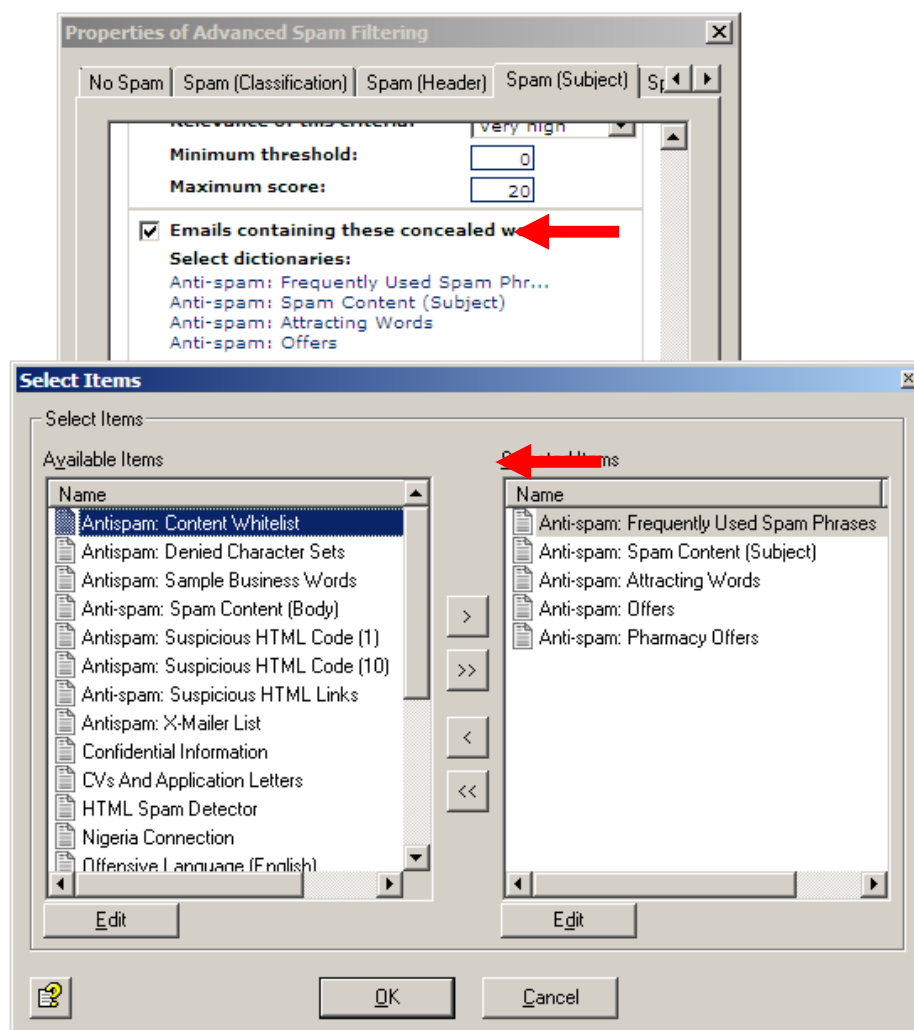
“Emails from Active Directory users = no SPAM”

“E-mails from User Blacklist entries = SPAM”.

Combined Criteria:

Via the “Combined Criteria” several filters are used. Here the Avira Space Module is working among others which provides an automatic spam detection. The detection patterns of the spam mails are updated in regular intervals.

In addition a word list detection for the subject line and content text is used. The word lists are fixed and are not updated automatically. But you can change the word lists manually.



5. Activation of the Information Store Job

Beside the virus scan on the transport level AntiVir Exchange is also able to check data in the public or private information store of the MS Exchange.

This filter is deactivated by default but can be activated if desired. Three main sectors are covered with the information store scan:

On-Demand Scan

In case a client tries to open a message a comparison is proceeded in order to make sure that the text and the attachment has been checked by the latest virus signature file. If the content has not been checked by the latest virus signature file the corresponding message component is sent to the virus scanner before it is forwarded to the client. The on-demand scan is the most common sector for which the information store scan is chosen.

Proactive Scan

The proactive scan checks new incoming messages before the client accesses to it via the on-demand scan. The proactive scan is an addition to the on-demand scan which can provide a faster client access.

Background Scan

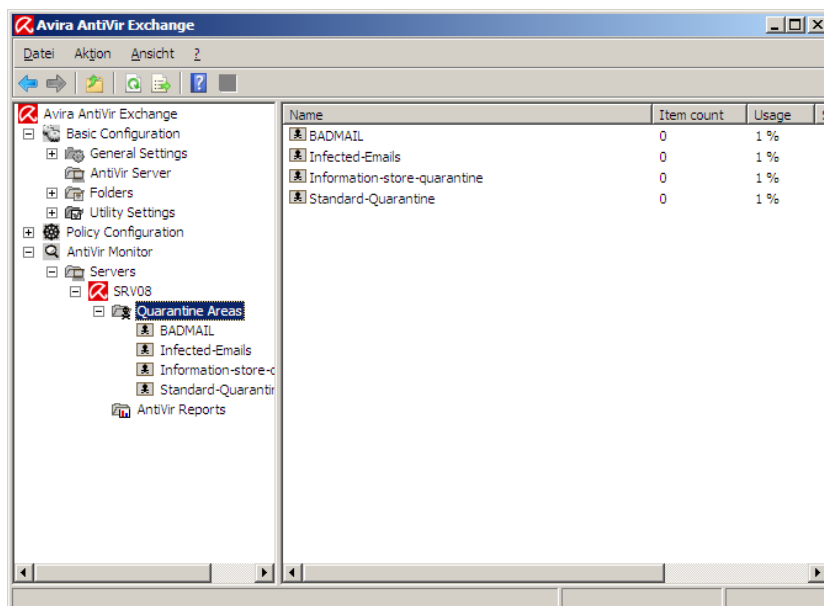
With the background scan a complete scan of all elements of the information store can be proceeded. This scan can be activated separately for the public and the private information store. All elements are scanned which have not yet been checked with the latest virus signature file.

In addition you have the possibility to proceed a time controlled scan. So you can scan the information store f. ex. on the weekend.

Just like for the "Mail-Transport-Jobs" you can define the actions to be proceeded in case of a virus detection here.

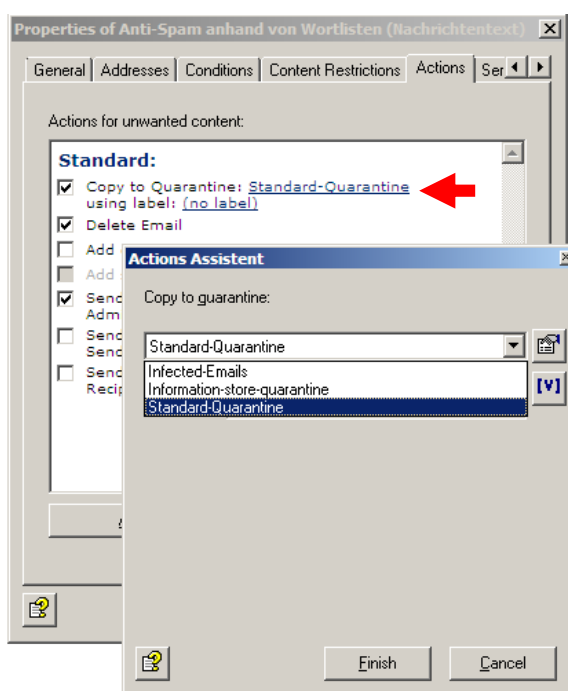
6. Quarantine

AntiVir Exchange possesses of a central quarantine which can be displayed via the menu point “**AntiVir Monitor**” → “**Server**” → “<Your server>” → “**Quarantine Areas**”.



In case another quarantine is needed, you can create it in the sector “**Basic Configuration**” → “**Folders**” → “**Quarantines**”.

Please, take into consideration that the predefined quarantines were already assigned to the particular jobs and that further adjustments might be necessary. In order to use your new quarantine it has to be saved into the chosen job in the tab “**Action**”.

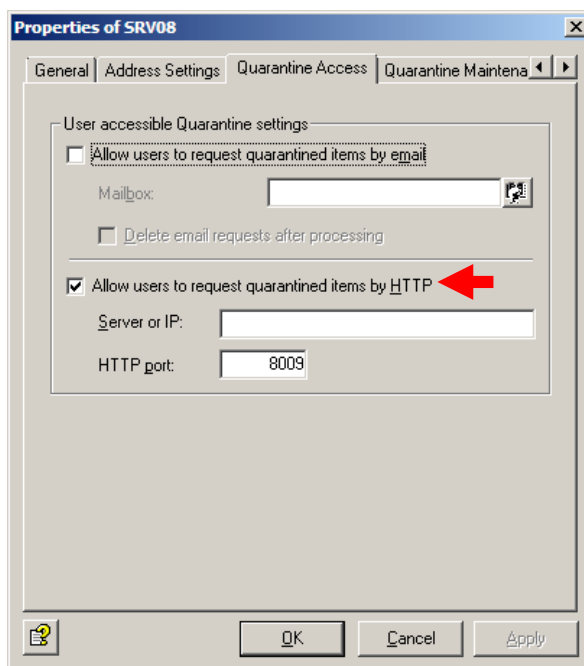


7. Summary Reports (Quarantine)

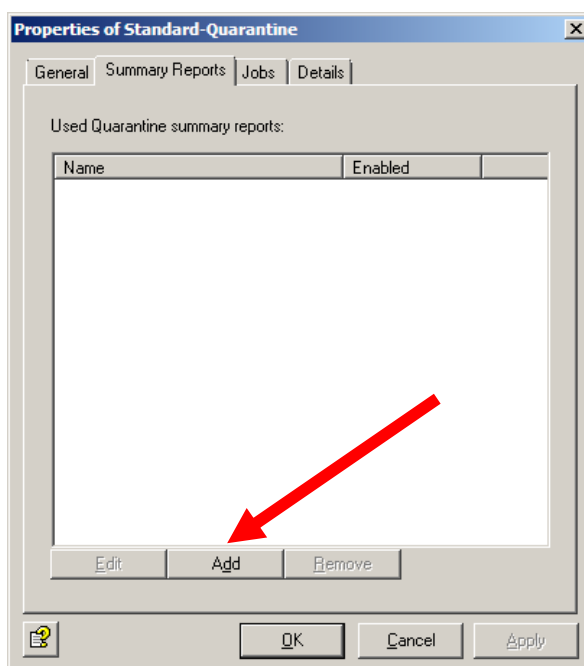
In order to use the summary report function, please, proceed as follows:

First enable the quarantine access:

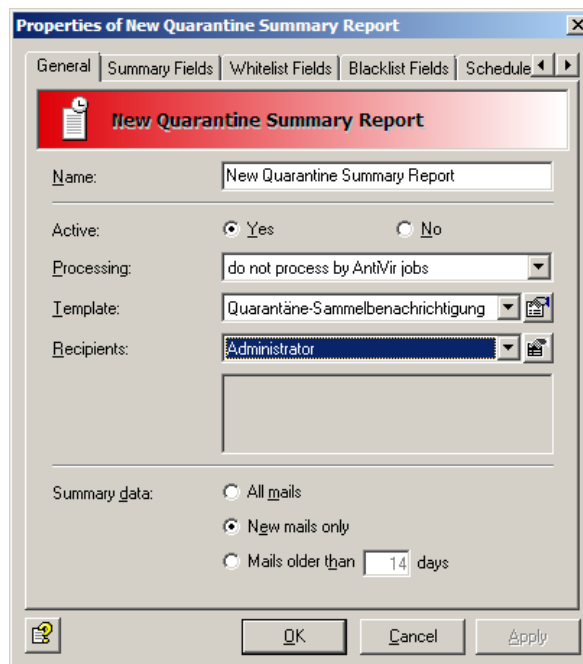
“Basic Configuration” → **“AntiVir Server”** → Double click on **“<server name>”** → **“Quarantine Access”** → **“Allow users to request quarantined items by HTTP”**



After that, please, go to: **“Basic Configuration”** → **“Folders”** → **“Quarantines”**
There you open the properties of the chosen job by double clicking on it. Then click on **“Add”** in the tab **“Summary Reports”**.

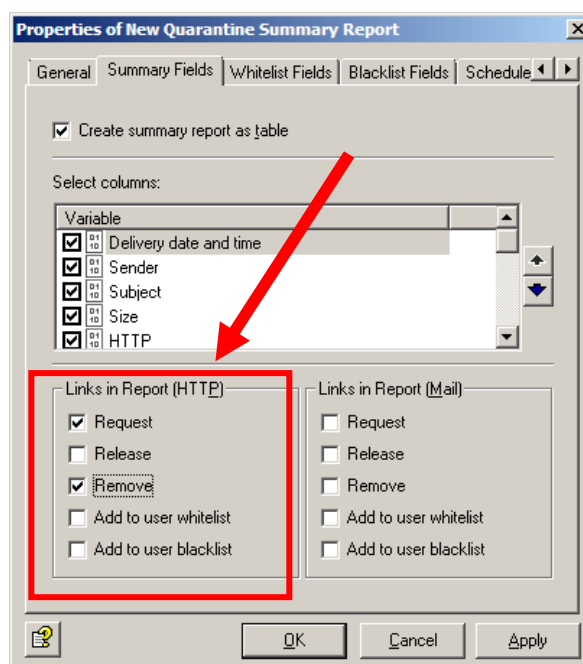


In the properties of the summary report you can define who should receive this message. In addition you define a name and the contents here.



In the tab “**Summary Fields**” you define which possibilities the recipient has.

Hint: As the quarantine access was set on HTTP, only a HTTP access is possible here. In case the email access should be used, this has to be activated also in the quarantine access.





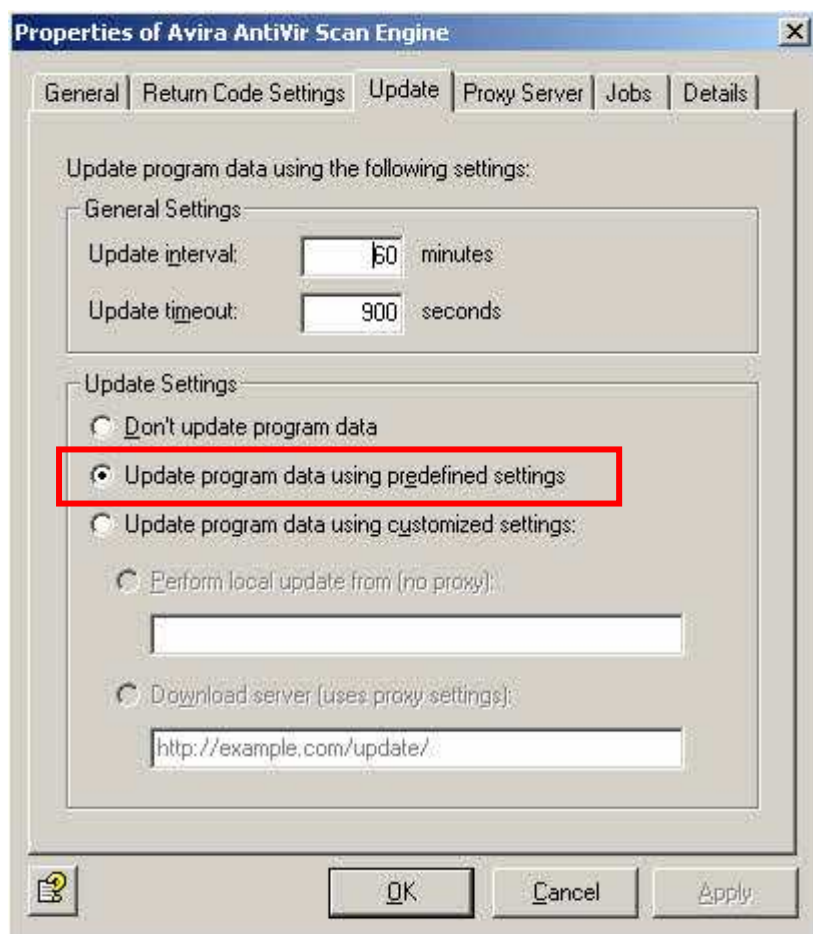
After having defined the possible actions you only have to configure the schedule which defines when the summary reports should be sent.

The point **“Add to user white- / blacklist”** in the register **“Summary Fields”** refers to separate address lists and not to the lists in the sector **“Basic configuration”**→ **“General settings”**→ **“Address lists”**.

8. Update Settings

Since version 8 the update settings can be configured within the AntiVir Exchange Management Console.

Navigate to “**Basic Configuration**” → “**Utility Settings**”. Open the properties of **AntiVir Engine** (virus signatures) and accordingly **AntiSpam Engine** (AntiSpam signatures). In the Tab “**Update**” the option “**Update program data using predefined settings**” is preselected. These are the standard Avira update servers in the Internet.



It is also possible to choose your own update server or to disable the update completely (which is not recommended).

All relevant logfiles can be found in the following directories:

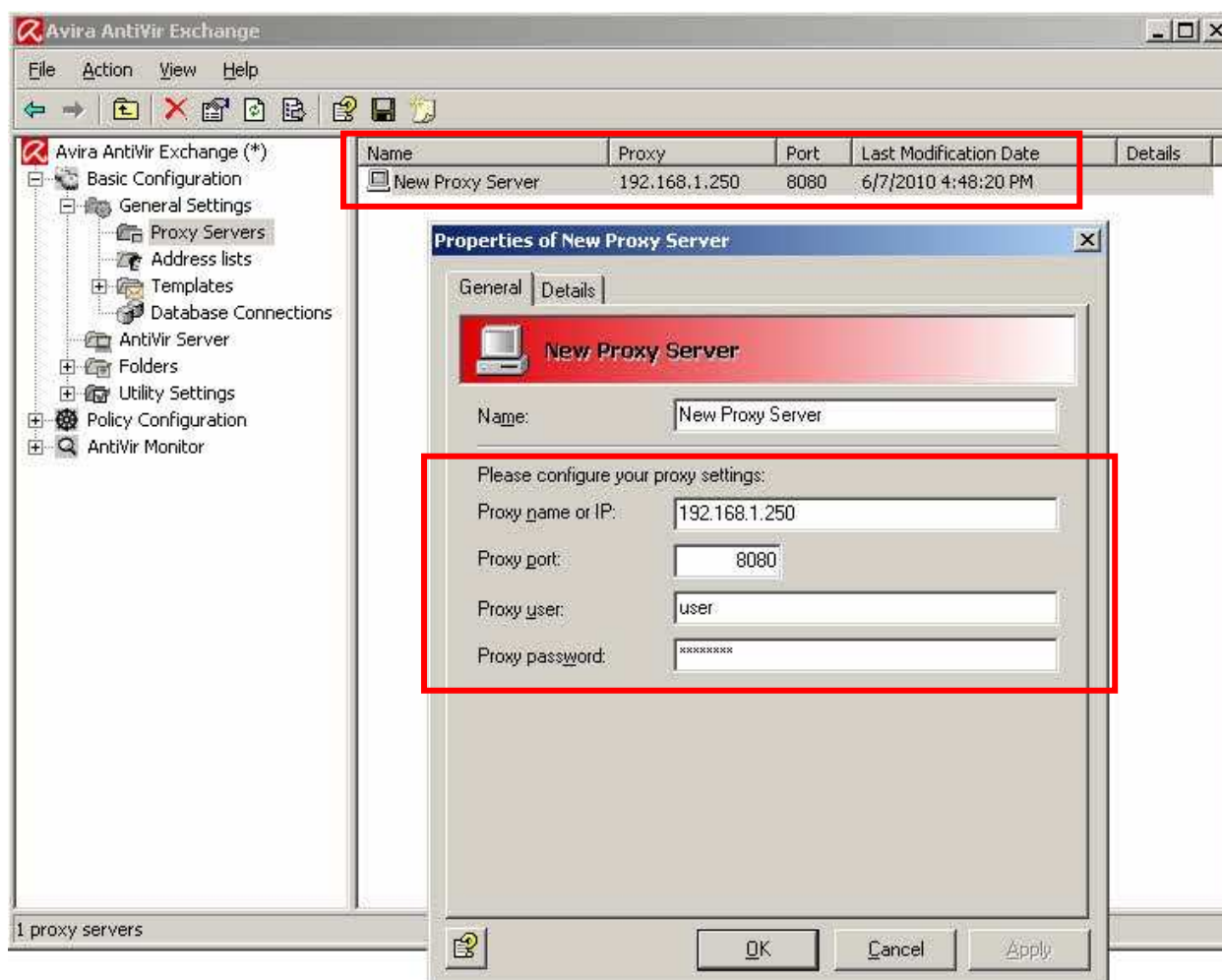
- **AntiSpam Engine:**
C:\Program Files (x86)\Avira\AntiVir Exchange\Bin\SPACE\Update\avupdate.log
- **AntiVir Engine:**
C:\Program Files (x86)\Avira\AntiVir Exchange\Bin\Savapi\Update\avupdate.log

8.1 Update via Proxy Server

The ability to configure your proxy in the AntiVir Exchange Management Console is also a new feature in version 8.

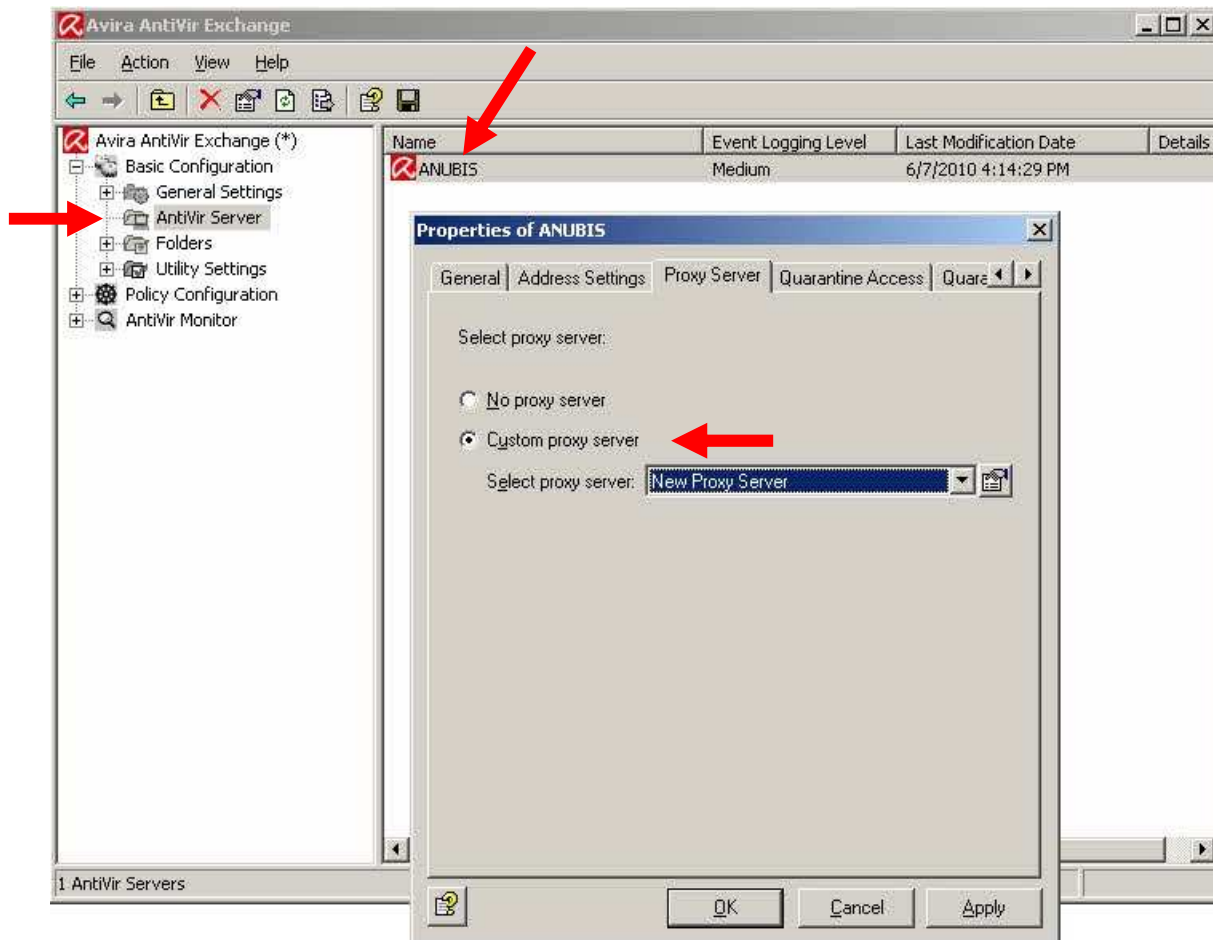
The necessary configuration must be done in different places.

First, you have to specify one or more proxy servers. Navigate to the "**Basic Configuration**" → "**General Settings**" → "**Proxy Server**" and create a new entry.



Fill in the properties the according DNS-Name or IP-address, the correct port and username and password if necessary.

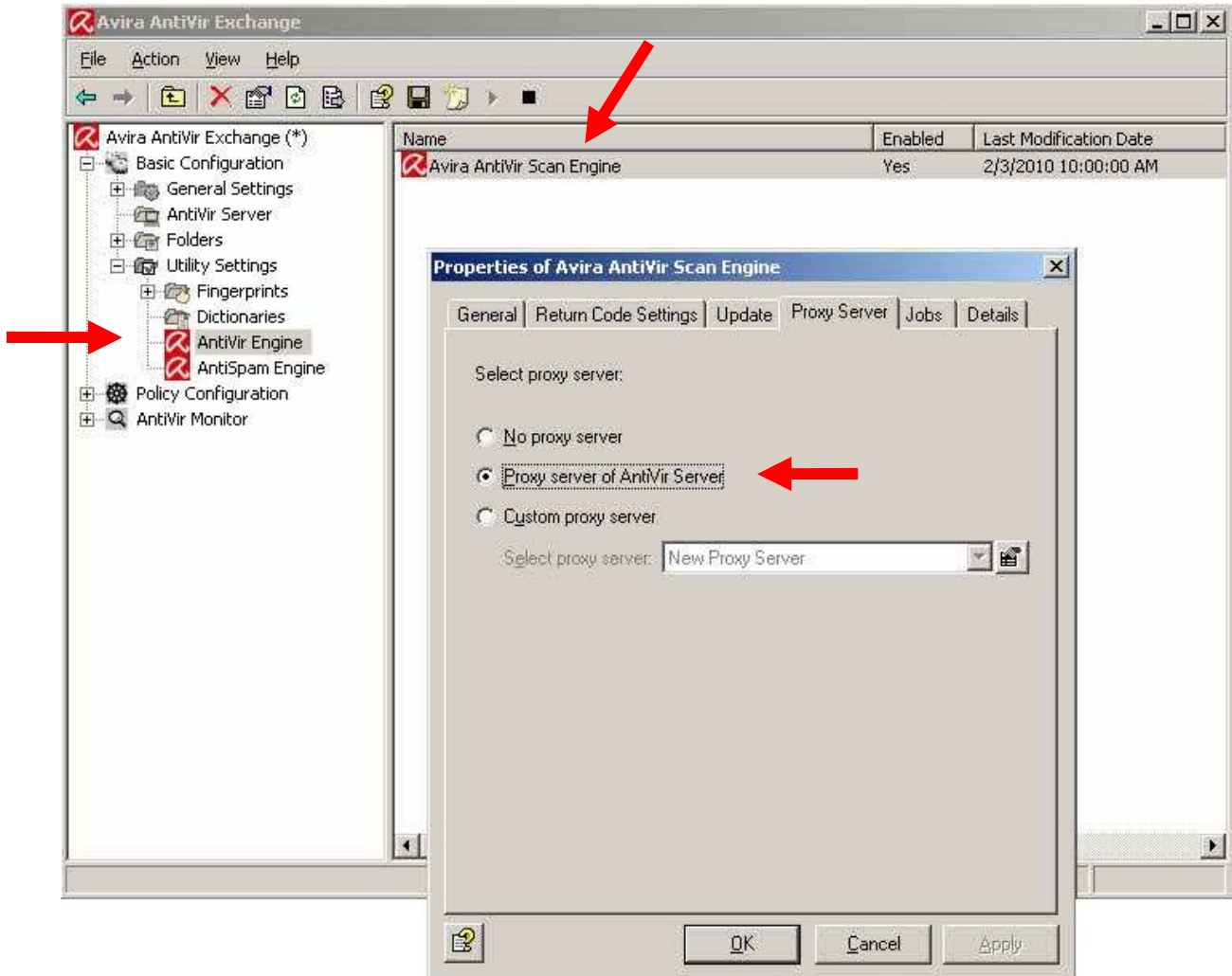
This server must be selected in the properties of your Server under "**Basic Configuration**" → "**AntiVir Server**" → Tab "**Proxy Server**"



After you have defined a global server, this proxy server is used in the following modules:

- *AntiVir Engine*
- *AntiSpam Engine*

These modules can be found under “**Basic Configuration**” → “**Utility Settings**”. Open the properties of the according module and make sure, that the option “**Proxy server of AntiVir Server**” is selected in the proxy tab.

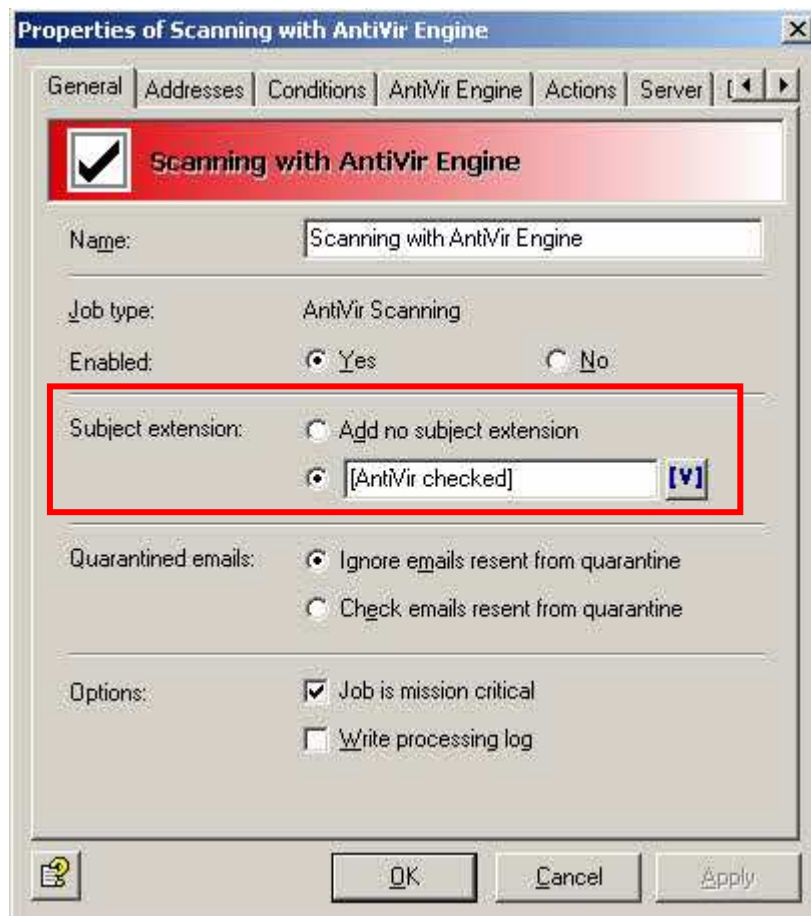
**Hint:**

It is possible to configure multiple proxy servers and to assign a different server to each module. In this case, select the option “**Custom proxy sever**” and choose the concerning server from the list.

9. Job recommendations

9.1 Remove Addition in subject

In the default configuration AntiVir Exchange adds in each email the subject [AntiVir checked]. To turn the Subject extension on or off, each job has to be configured separately. Open the properties of each job and verify in the tab "**General**" if the addition is set.



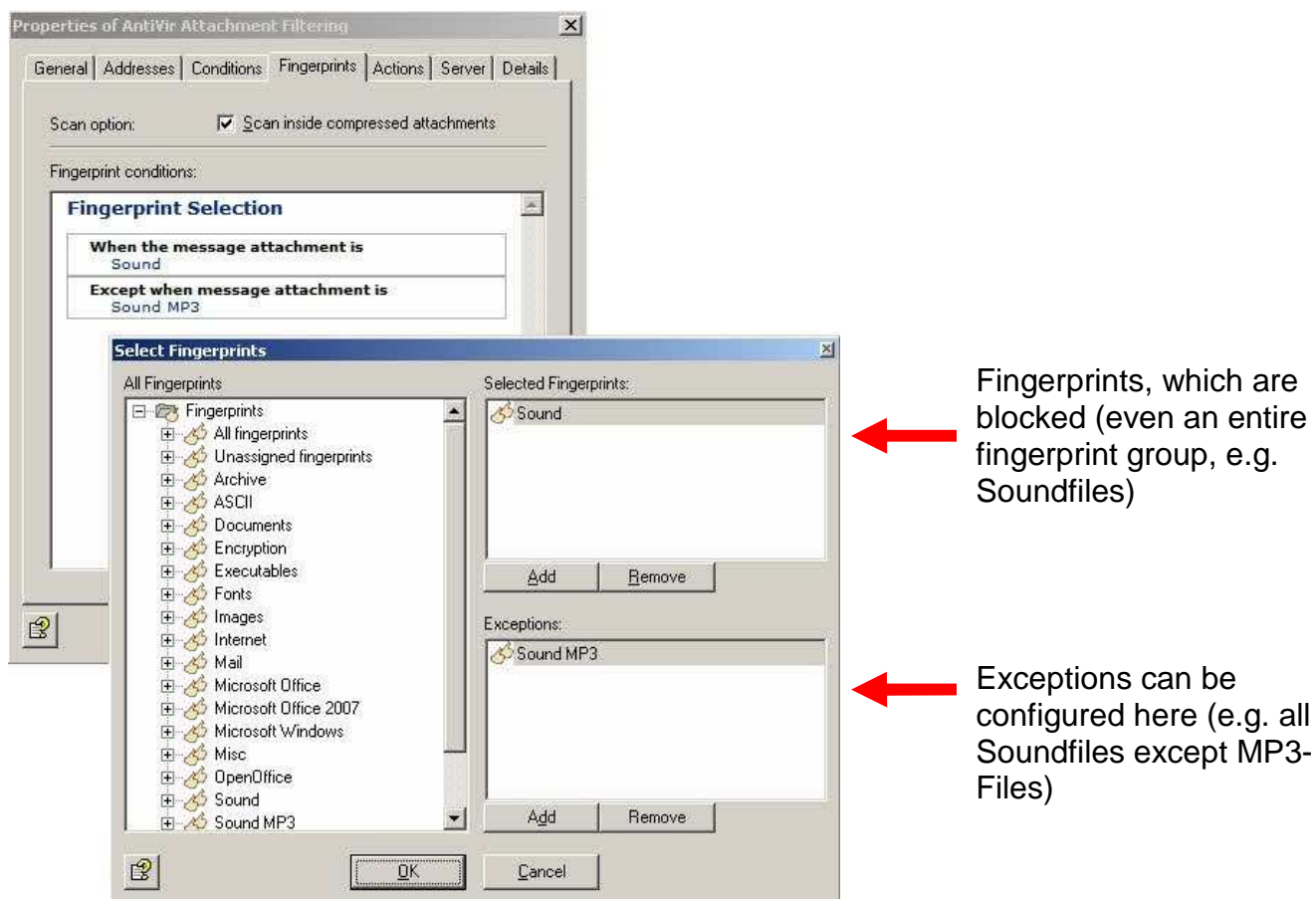
9.2 Block unwanted attachments

In order to block certain unwanted file attachments, AntiVir Exchange offers under "**Job Templates**" some pre-configured jobs. These are referred in the column "**Job Type**" as "**AntiVir Attachment Filtering**".

You can use these predefined jobs or create a new job.
The detection based on fingerprints is the best way to block unwanted attachments.

Navigate to the "**Policy Configuration**" → "**Mail-Transport-Jobs**" and create a new job, in this case "**AntiVir Attachment Filtering**".

Open the properties of this job and configure conditions and/or exceptions in the tab "**Fingerprints**".



Fingerprints, which are blocked (even an entire fingerprint group, e.g. Soundfiles)

Exceptions can be configured here (e.g. all Soundfiles except MP3-Files)

If you want to notify the sender about blocked Attachments, activate the option "**Send Sender: forbidden attachment found to All Senders**". It is recommendable that the administrator doesn't receive an email each time an attachment is blocked. Disable the option according to your requirements.

9.3 Advanced Spam Filtering with separate Quarantines

Hint: Please note, that the following job proposal is included and activated by default since version 8: "Filtering Spam with Avira SPACE"

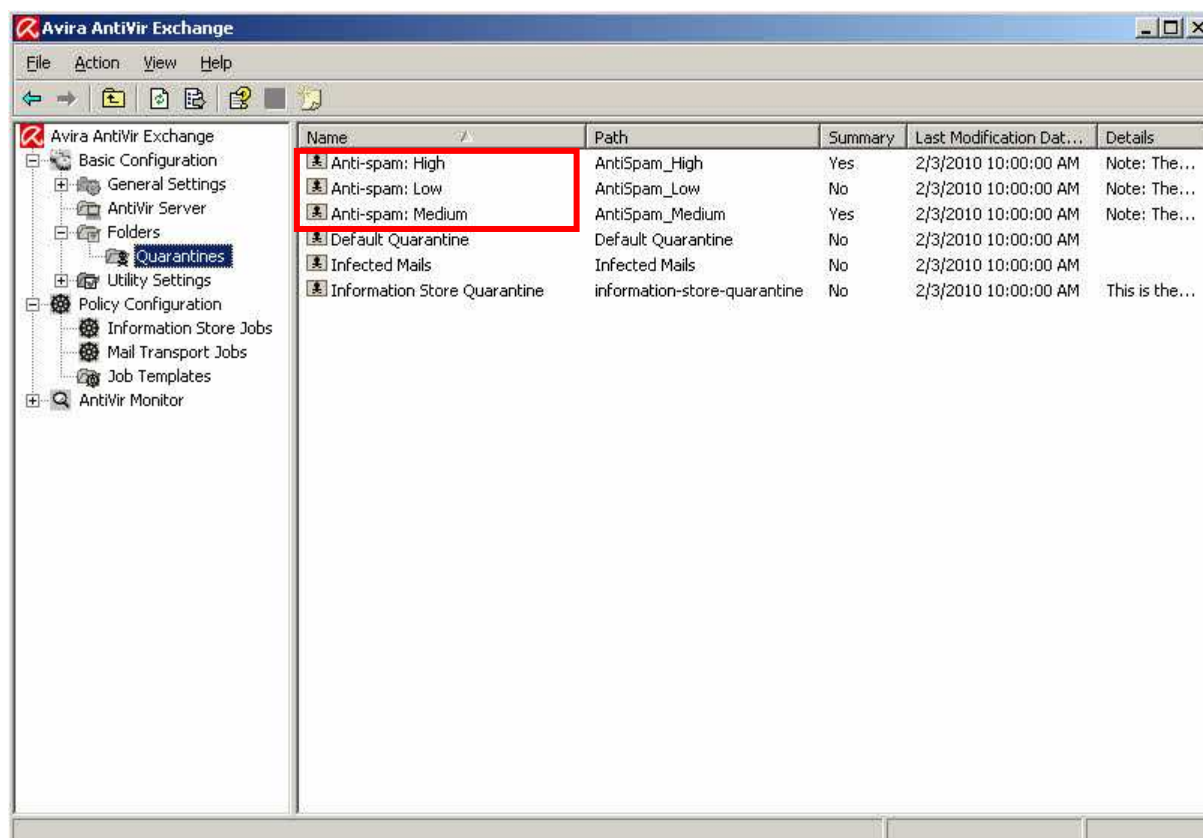
Spam can be divided into three categories with the job "Advanced spam filtering":

- Spam probability: Low
- Spam probability: Medium
- Spam probability: High

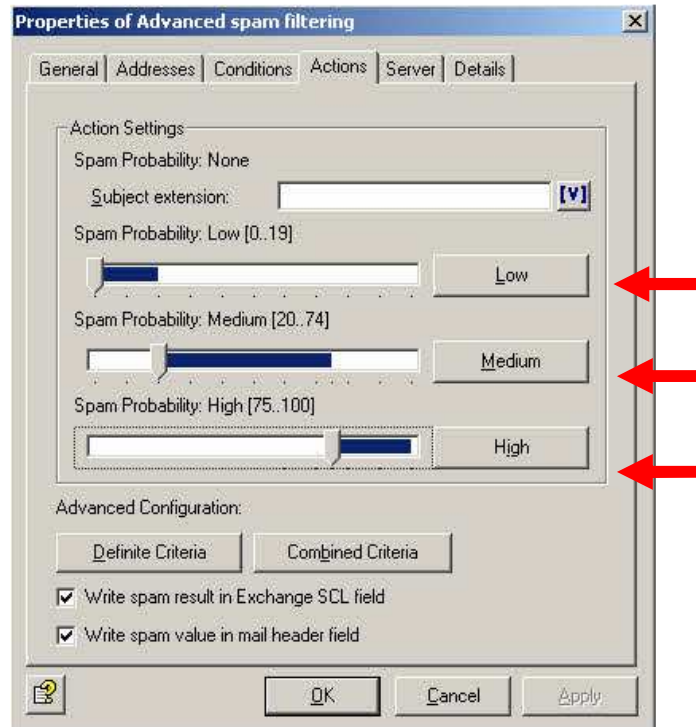
For each category, you can choose a separate quarantine folder for incoming mail and can thus be stored in different quarantine folders.

You must first create an appropriate quarantine folder. Navigate to the AntiVir Exchange console for the "**Basic Configuration**" → "**Folders**" → "**Quarantines**". Click the right mouse button to add a new quarantine folder and create the following folders (maximum 30 characters):

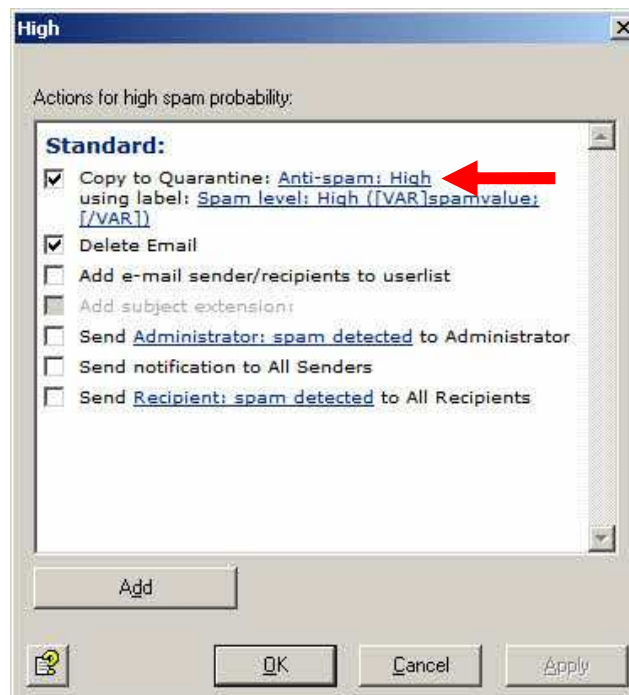
- Anti-spam: Low
- Anti-spam: Medium
- Anti-spam: High



After that, the job "**Advanced spam filtering**" under "**Mail Transport Jobs**" must be configured accordingly. The previously created quarantines must be defined in the properties of this job under the tab "**Actions**".



Now, configure each category (in the example "**High**") and select the appropriate quarantine folder:

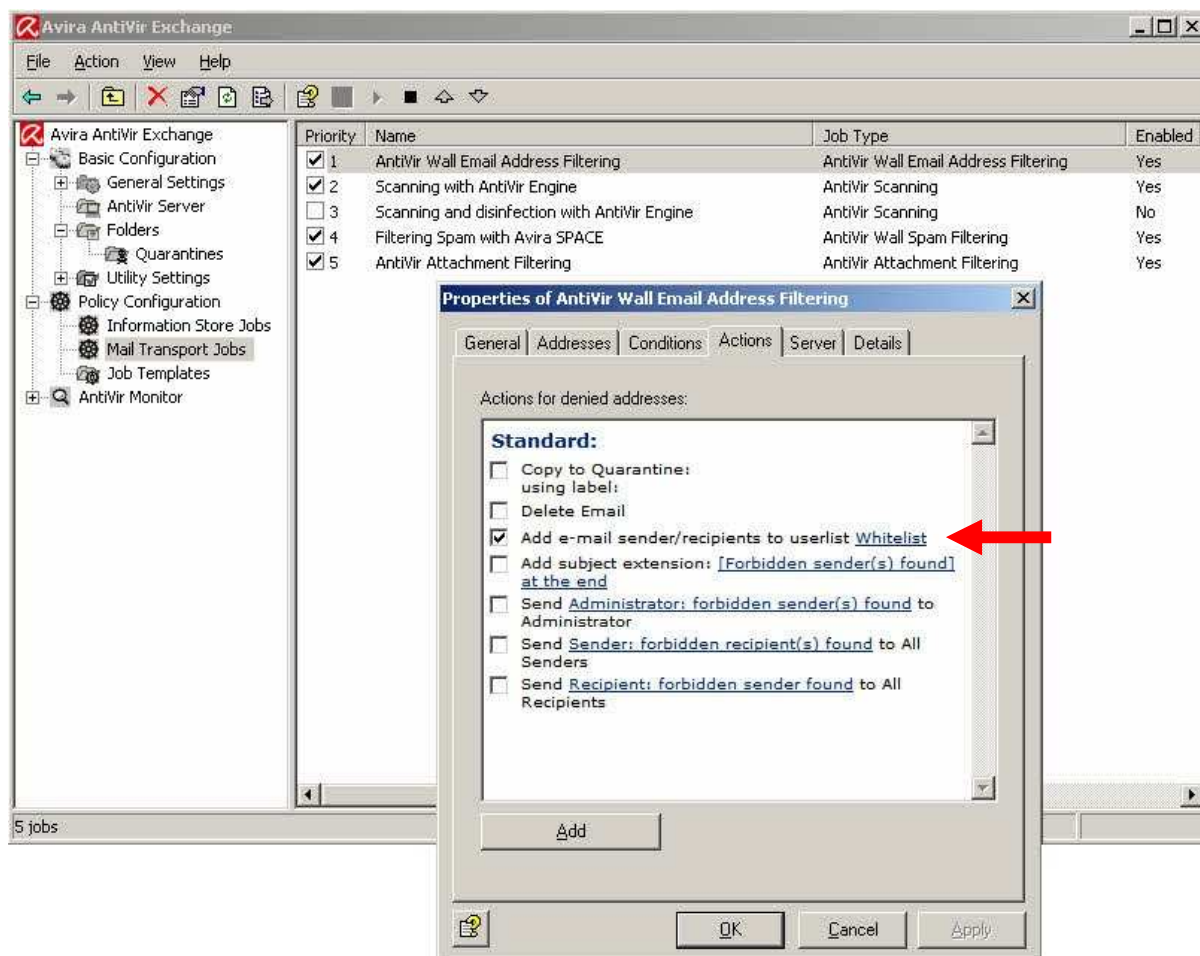


Repeat this process for the category "**Medium**" and "**Low**".

9.4 Add recipient automatically to the whitelist

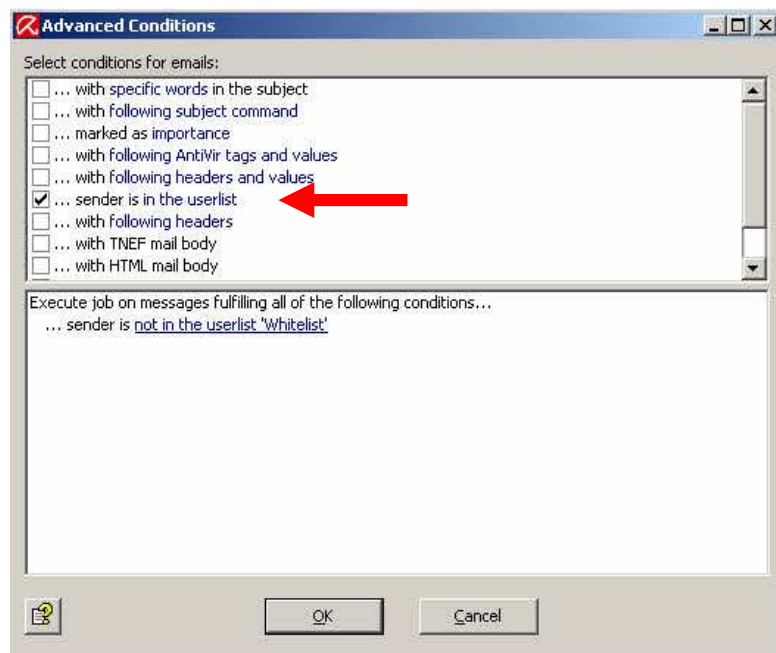
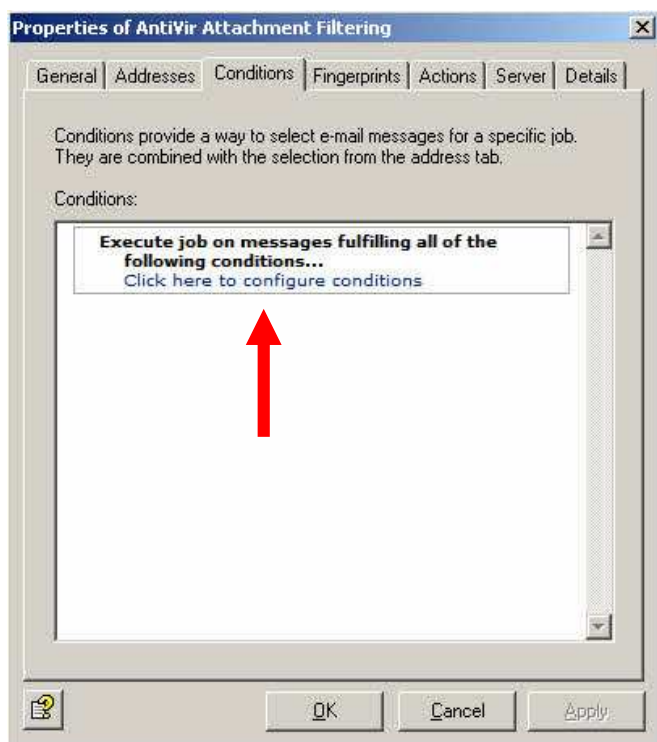
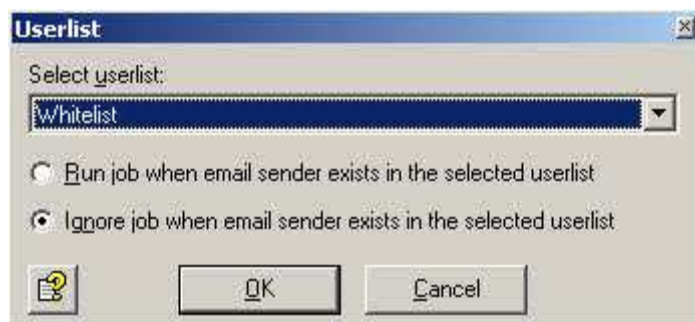
You can add recipient automatically to the whitelist the following way:

- Create a new job under “**Mail Transport Jobs**”:
“**AntiVir Wall Email Address Filtering**”
- Navigate to the tab “**Actions**” and set the hook *only* on “**Add e-mail sender/recipients to userlist Whitelist**” (like shown in the screenshot below)
- Slide the job in “**Mail Transport Jobs**” in the first place



Now, every following Anti-spam job must be configured like this, so that the job will be ignored if the sender is listed in the Whitelist.

- Open the properties of the corresponding job and navigate to the tab **“Conditions”**
- Add a new condition: **“...sender is *not* in the user list ‘Whitelist’”**

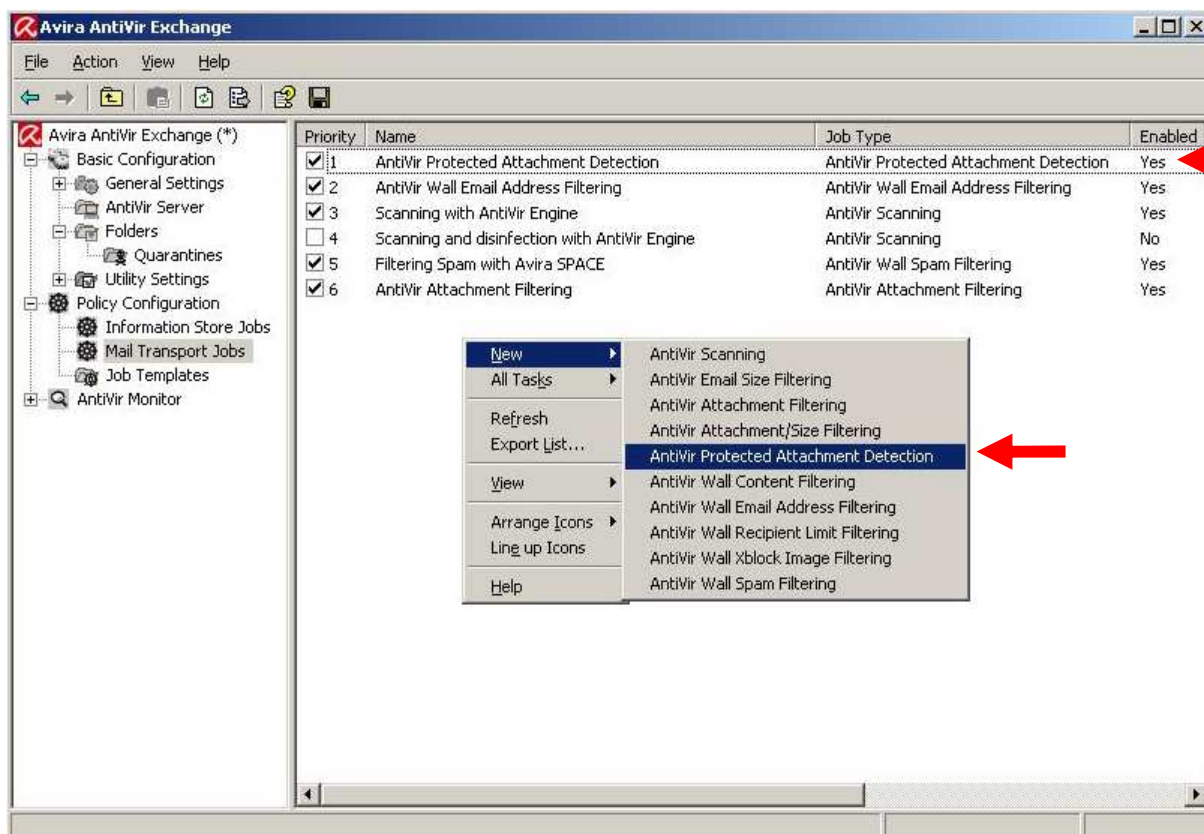


After you have saved the configuration, all recipients will be added automatically to the Whitelist and ignored by the following Anti-spam Jobs.

9.5 Password protected Archives

All password protected Archives will be blocked by default. However, since version 8 a new job exists: "**Antivir Protected Attachment Detection**". As this job is not activated by default, you have to enable it first.

Configure the mentioned job under "**Mail Transport Jobs**" and slide it to the first place.



Now you can configure the job and define how an email is processed after a password protected files has been detected. Open the properties of the job and navigate to the tab "**Actions**".

Please, don't forget to save the configuration to activate the changes you made.