



Avira

Exchange Security

User Manual

Avira Exchange Security

Table of contents

1 Quickstart.....	5
1.1 Installing on an Exchange server.....	5
1.2 Starting the Avira Exchange Security Management Console.....	5
1.3 Configuration in the Avira Exchange Security Management Console.....	6
1.3.1 Required settings in Basic Configuration.....	6
1.3.2 Required settings in Policy Configuration.....	7
1.3.3 Recommended settings in the Basic Configuration.....	7
1.3.4 Virus scan of the Exchange databases.....	7
1.4 Observing data in Avira Monitor.....	8
2 Installation.....	9
2.1 System requirements.....	9
2.2 Installing Avira Exchange Security on an Exchange server.....	10
2.3 Uninstalling Avira Exchange Security.....	14
3 Product modules.....	16
3.1 Avira Exchange Security Management Console.....	16
3.1.1 Access methods.....	16
3.1.2 Administration modes.....	16
3.2 Avira Exchange Security Server.....	17
3.2.1 The transport agent.....	17
3.2.2 Avira Exchange Security Service Service = Enterprise Message Handler (EMH).....	17
3.2.3 Quarantine.....	18
3.2.4 The Active Directory/ LDIF.....	19
3.2.5 Compressed files or archives - Avira Exchange Security Unpacker.....	19
3.3 The configuration file of Avira Exchange Security.....	20
3.3.1 Using a custom configuration file.....	20
4 Avira Monitor.....	22
4.1 Setting the access to Avira Monitor.....	22
4.2 Using the Avira Monitor.....	22
4.3 Using quarantines.....	23
4.4 Sending emails from quarantines.....	24
4.5 Adding a sender to an address list.....	26
4.6 Adding a domain to an address list.....	26
4.7 BADMAIL.....	26
4.8 Details of a quarantined email.....	27
4.8.1 Message details.....	27
4.8.2 Quarantine processing log.....	28
4.8.3 Quarantine details.....	29
4.9 Details in the IS quarantine.....	29
4.9.1 Message details in IS quarantine.....	29
4.9.2 IS Quarantine processing log.....	30
4.10 Quarantine buttons.....	31
4.11 Statistics in Avira Exchange Security.....	32
4.12 Generating statistics.....	32
5 Avira Scan Engine.....	33
5.1 Avira Scanning jobs.....	33

5.1.1 Configuring and enabling Avira Scan Engine.....	34
5.1.2 Activating a virus scanning job.....	37
5.2 Information Store Scan jobs.....	43
5.2.1 Checking the status of the Information Store.....	44
5.2.2 Restarting the Information Store Scan.....	45
5.2.3 Activating the Information Store Scan job.....	46
5.3 Avira Protected Attachment Detection.....	51
5.3.1 Setting a Avira Protected Attachment Detection job.....	52
5.4 Avira Attachment Filtering jobs.....	53
5.4.1 Fingerprints.....	54
5.4.2 Blocking video files.....	55
5.5 Avira Email Size Filtering jobs.....	58
5.5.1 Restricting email size.....	59
5.6 Avira Attachment/ Size Filtering jobs.....	62
5.6.1 Blocking Office files.....	63
6 Avira Email Filter.....	67
6.1 Address filtering.....	67
6.1.1 Blocking senders or recipients.....	68
6.2 Content filtering with dictionaries.....	71
6.2.1 Setting up dictionaries.....	71
6.2.2 Searching for text in dictionaries.....	73
6.2.3 Blocking offensive content.....	74
6.2.4 Calculation of content filtering threshold.....	77
6.3 Limiting the number of recipients.....	78
6.4 Advanced Email Filter settings.....	81
6.4.1 Definite criteria.....	82
6.4.2 Combined criteria.....	84
6.4.3 Advanced Email Filtering.....	89
6.4.4 Configuring Email Filter manually.....	99
7 Detailed configuration.....	101
7.1 Basic Configuration.....	101
7.1.1 Generating configuration reports.....	101
7.1.2 Importing a configuration.....	102
7.1.3 Making default settings for all servers.....	103
7.1.4 Creating an Avira Server.....	106
7.1.5 Making settings for an individual Avira Server.....	106
7.2 Database connections.....	113
7.2.1 Prerequisites for database connection.....	113
7.2.2 Configuring the database connection.....	113
7.2.3 Example of ADO string configuration.....	115
7.2.4 Configuring central whitelists.....	116
7.2.5 Configuring a quarantine database.....	116
7.2.6 Handling problems with SQL servers.....	117
7.3 Address lists.....	117
7.3.1 Creating address lists.....	118
7.3.2 Deleting an address list.....	119
7.3.3 Using address lists in jobs.....	119
7.3.4 Address settings when scanning for viruses.....	121
7.3.5 Address settings when blocking attachments.....	122

7.4 Templates.....	123
7.4.1 Creating notification templates.....	124
7.4.2 List of notification variables.....	124
7.5 Quarantine configuration.....	131
7.5.1 Creating a new quarantine.....	132
7.5.2 Configuring a quarantine.....	132
7.5.3 Example of mission critical quarantine.....	134
7.5.4 Quarantine Summaries.....	134
7.5.5 Setting a summary report.....	135
7.6 Utility Settings.....	140
7.7 Policy Configuration.....	141
7.7.1 Example of a policy.....	141
7.7.2 Job types.....	141
7.7.3 Job conditions.....	142
7.7.4 Job actions.....	143
8 Toolbar buttons.....	145
9 Icons reference.....	146
10 Support information.....	149

1 Quickstart

The quickguide to Avira Exchange Security.

1.1 Installing on an Exchange server

1. To install Avira Exchange Security, double-click the installation file:

- *avira_exchange_security_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 Exchange Security is installed in the following default directory:

for the 64-bit version:

- *C:\Program Files(x86)\Avira\Avira Exchange Security (English)*
- *C:\Programme(x86)\Avira\Avira Exchange Security (German)*

3. Disable the real-time or on-access scan functions of any virus scanners you use, for the directory ... \Avira\Avira Exchange Security\AppData
4. Start the Avira Exchange Security Management Console.
5. Carry out the recommended settings for the **Basic Configuration** and **Policy Configuration**.

Related topics:

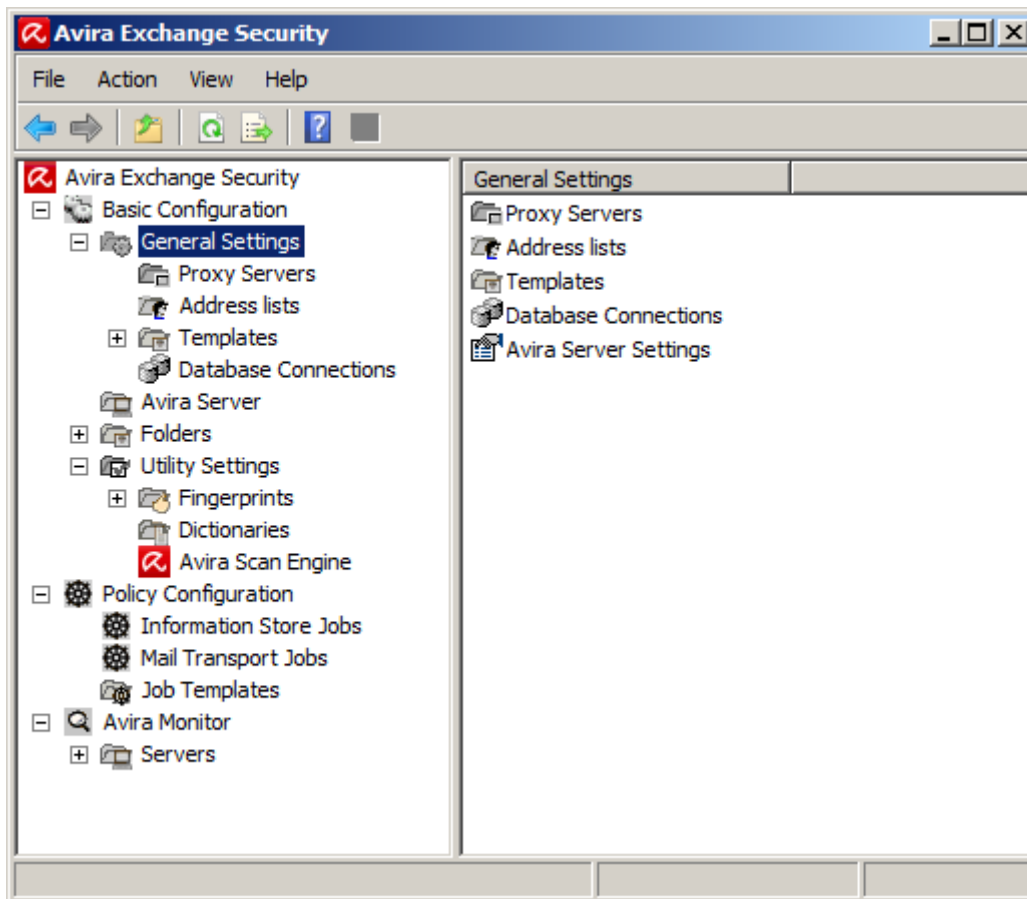
[Required settings in Basic Configuration](#) - page 6


[Required settings in Policy Configuration](#) - page 7

1.2 Starting the Avira Exchange Security Management Console

Avira Exchange Security is a server product that is configured using the Avira Exchange Security Management Console. To run Avira Exchange Security, the service Avira Exchange Security Service must be started.

1. To start the console, click **Start > Programs > Avira > Avira Exchange Security > Avira Exchange Security Management Console**.



2. To save changes you made to the configuration in the console, click the **Save Configuration**  button.

Unsaved changes are indicated by (*) at the uppermost node.

The configuration is saved in the *ConfigData.xml* file, which is stored in the directory ...\\Avira\\Avira Exchange Security\\Config.

Related topics:

[Avira Exchange Security Service = Enterprise Message Handler \(EMH\)](#) - page 17

[Toolbar buttons](#) - page 145

[Icons reference](#) - page 146

1.3 Configuration in the Avira Exchange Security Management Console

After installing Avira Exchange Security, set the configuration in the console.

1.3.1 Required settings in Basic Configuration

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

Select **Basic Configuration** > **General Settings** > **Avira Server Settings** on the **Email addresses** tab to check the entries for the **Administrators** and the **Internal domains**.

Related topics:

[Making default settings for all servers](#) - page 103

1.3.2 Required settings in 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 rule-based measures or actions that apply to the email traffic.

It is important to distinguish between two categories of jobs.

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

To create a new job, carry out the following steps:

1. Find the required template in **Job Templates**.
2. Select the template and drag it to the **Mail Transport Jobs** folder.
3. Set the name and the properties of the job and enable the job (*Active: Yes*).

Note

The order determines the sequence in which the jobs are processed.

4. Click **Save Configuration** to save the settings.

1.3.3 Recommended settings in the Basic Configuration

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

1. Configure the **Address lists** (for the selection in the job rules) under **General Settings**.
2. If necessary, 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 Avira 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, the information store job is also deleted.

Related topics:

[Information Store Scan jobs](#) - page 43

1.4 Observing data in Avira Monitor

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

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

Related topics:

[Avira Monitor](#) - page 22

2 Installation

2.1 System requirements

Minimum system requirements for installing Avira Exchange Security

Note

For information about the installation of clusters, contact the Avira Sales team.

Warning

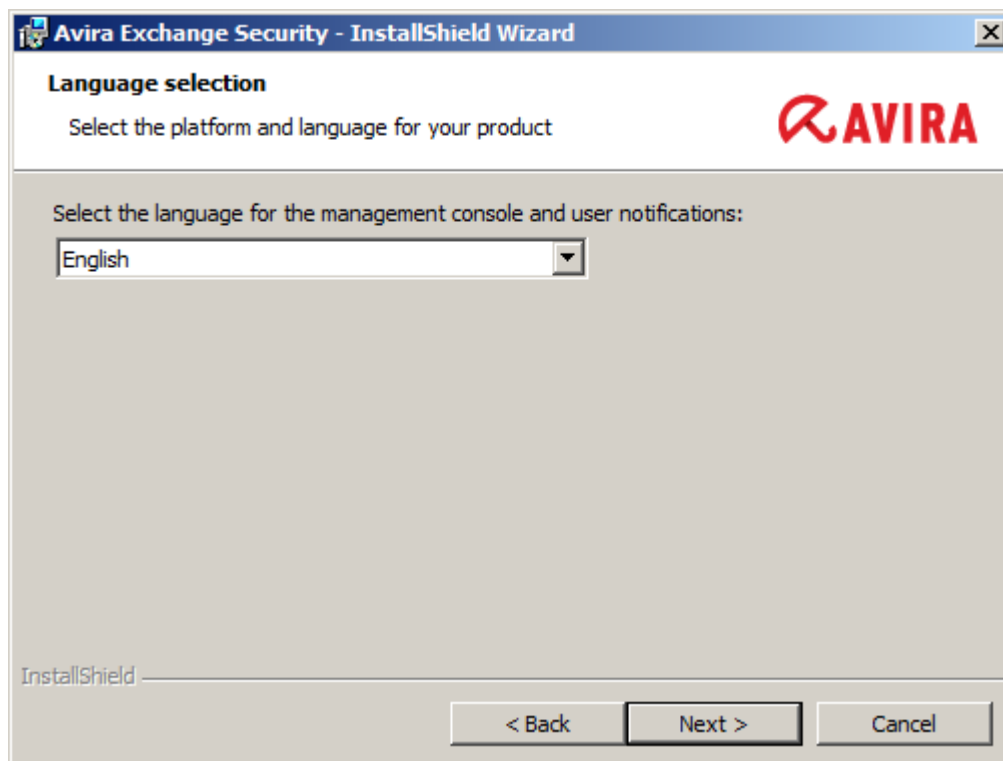
Disable the real-time or on-access scan functions of any virus scanners you use, for the directory ...\\Avira\\Avira Exchange Security\\AppData.

- Operating systems (64-bit):
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
- Exchange server:
 - MS Exchange Server 2007 SP1 Update Rollup 4 (64 Bit) (or higher, i.e. SP2/ SP3 including all Rollups up to date)
 - MS Exchange Server 2010 (64 Bit) (or higher, i.e. SP1/ SP2 including all Rollups up to date)
 - MS Exchange Server 2013 (64 Bit)
- RAM: Exchange-recommended + additional 64 MB
- Hard drive: At least 400 MB for the installation
- CD-ROM drive or network access
- Microsoft .NET Framework 3.5
- 100 MB for event logging recommended
- Internet access for engine updates (Scan Engine and Email Filter Engine)
- User privileges: Active Directory user with full reading access to the Active Directory.
- Operating systems for Avira Exchange Security Management Console:
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows XP Professional
 - Windows Vista
 - Windows 7
 - Windows 8

2.2 Installing Avira Exchange Security on an Exchange server

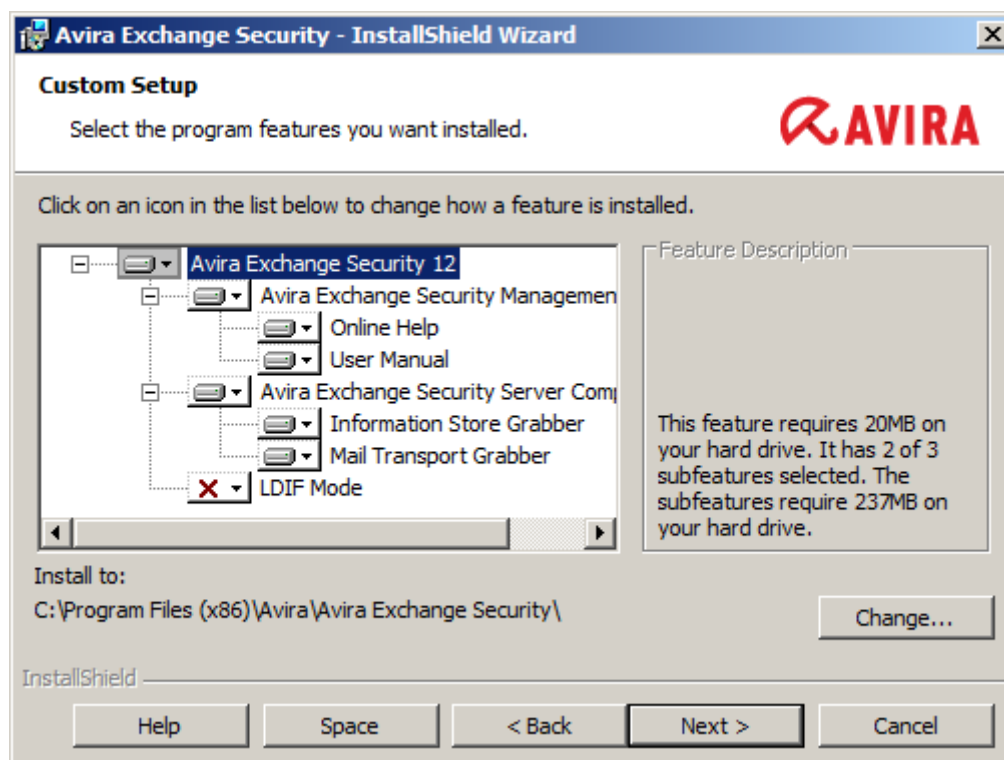
1. To install Avira Exchange Security, double-click the installation file. For example:
avira_exchange_security_64bit.exe
2. Select the setup language and click **Next**.
3. Select the platform and the language for the product.

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



4. In the next dialog box, accept the *license agreement* to be able to continue, and click **Next**.
5. Select the features that you want to install.

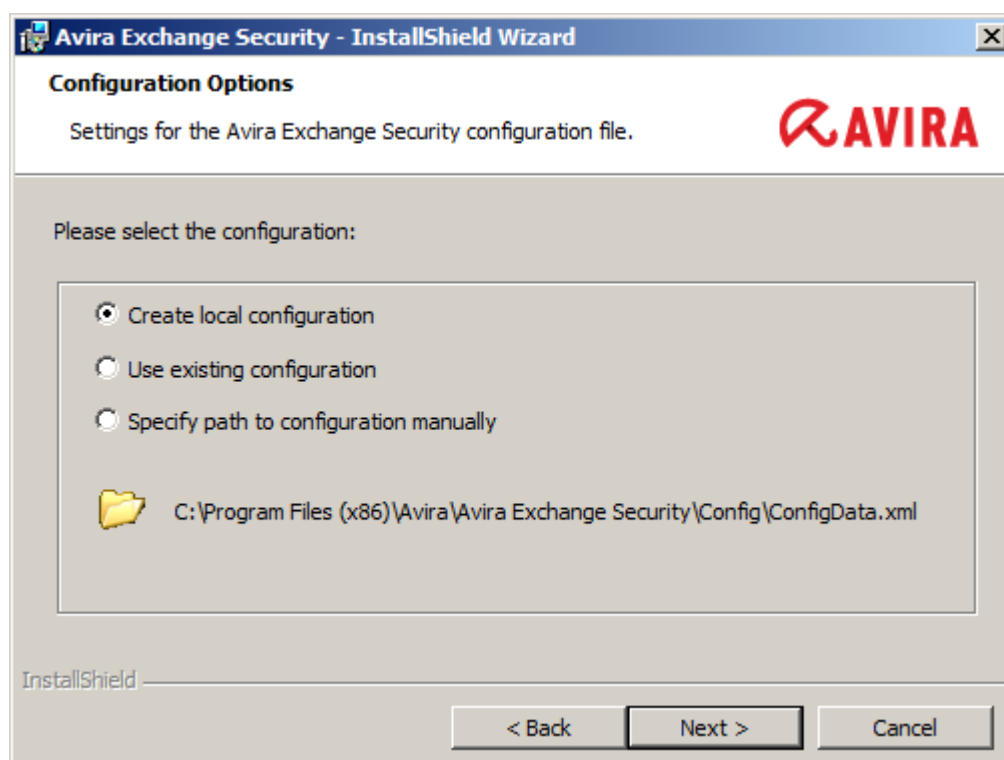
All selected server components and the Avira Exchange Security Management Console are installed.



If another active information store scan application apart from Avira Exchange Security 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.

6. Click **Next**.

You are asked for the storage location of the configuration file.



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

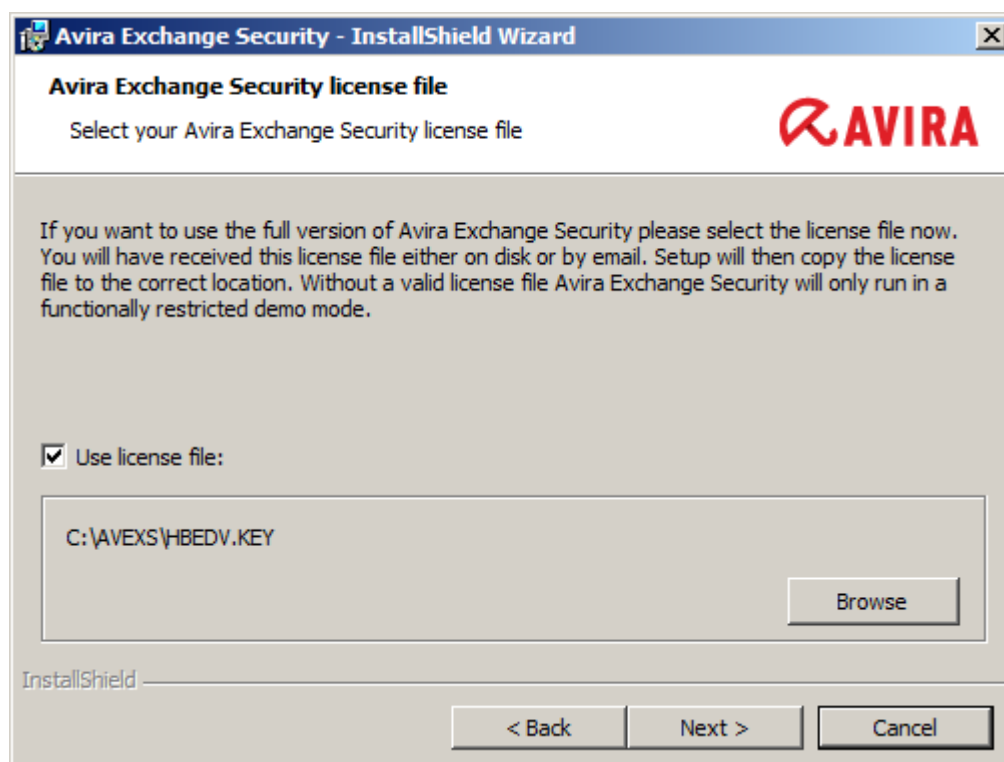


8. Define the email address of the administrator and click **Next**.
9. If you are using a proxy server for the Avira update, check the box and enter the proxy settings for IP address, port, user and password. The password is stored in plain text.



10. Click Next.

You are asked for the license file.



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

12. Click Next.

You receive a summary of your settings.



13. Disable the real-time or on-access scan functions of any virus scanners you use, for the directory ... \Avira\Avira Exchange Security\AppData, if you have not already done so.
14. Check your configuration settings. These settings are accepted as the default settings in the configuration of Avira Exchange Security Server.
15. Follow the rest of the instructions and click **Install**.
Avira Exchange Security is installed in the following directory (example): C:\Program Files(x86)\Avira\Avira Exchange Security
16. Click **Finish**.

Avira Exchange Security is successfully installed. The virus scanner is completely configured and can be used immediately. For this purpose, we provide a job for the virus scan with Avira, which you can easily enable.

Related topics:

[Making default settings for all servers](#) - page 103

[Configuring and enabling Avira Scan Engine](#) - page 34

2.3 Uninstalling Avira Exchange Security

1. Click **Start** > **Control Panel** > **Programs and Features**.
2. Select Avira Exchange Security.
3. Click **Change**.

The setup starts and uninstalls **Avira Exchange Security**.

3 Product modules

Avira Exchange Security consists of multiple components.

3.1 Avira Exchange Security Management Console

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

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

The Avira Exchange Security Management Console gives the administrator access to all the necessary configuration information and access to the Avira Monitor (which includes an overview of quarantines) of the Avira Exchange Security servers.

Related topics:

[Starting the Avira Exchange Security Management Console](#) - page 5

[Configuration in the Avira Exchange Security Management Console](#) - page 6

3.1.1 Access methods

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 configuration of Avira Exchange Security, for example to manage security settings. The configuration of Avira Exchange Security may be available locally.

2. SOAP and SSL

The Avira Monitor is accessed via SOAP and SSL. A defined communication port is used for communication purposes.

Related topics:

[Avira Monitor](#) - page 22

3.1.2 Administration modes

The Avira Exchange Security Management Console supports two administration modes.

1. Local administration

The Avira Exchange Security Management Console runs directly on the Exchange server, on which all the Avira Exchange Security components have been installed. This mode is suitable for smaller environments and administration takes place on the local server.

2. Remote administration

The Avira Exchange Security Management Console runs on a client, not on the Exchange server.

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

3.2 Avira Exchange Security Server

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

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

The Avira Exchange Security Server is divided into a number of different areas.

3.2.1 The transport agent

The transport agent is a process that ensures that all emails, scheduled 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, for both emails that are sent between mailboxes on the same mailbox, and for incoming and outgoing emails.

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

3.2.2 Avira Exchange Security Service Service = Enterprise Message Handler (EMH)

The Avira Exchange Security Service Service is always started as a Windows service and accepts all information from the transport agent. All further processing by Avira Exchange Security will be monitored and controlled by the Avira Exchange Security Service Service from this point forward.

Warning

If the Avira Exchange Security Service Service is stopped, the security functions of Avira Exchange Security are disabled.

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

- The configured jobs in Avira Exchange Security
- The installed license in Avira Exchange Security
- The Active Directory
- The quarantine of Avira Exchange Security

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

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

3.2.3 Quarantine

One possible option in Avira Exchange Security is to stop infected emails or other undesirable emails on the server. This prevents infected emails from reaching the relevant recipients. Infected emails are placed in the Quarantine instead.

A number of quarantines are available on each Avira Exchange Security Server after installation. Additional quarantines can be created by the administrator.

The components of the Quarantine:

- A quarantine directory on the Exchange server (...*\Avira\Avira Exchange Security\AppData\Quarantine\Default Quarantine*)
- The emails copied to quarantine.
- A quarantine database (*LocIdxDB.mdb*).

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

When a quarantine is displayed in the Quarantine, the information from the quarantine database is displayed first.

Information stored in the quarantine database

The following information is stored in the quarantine 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 Exchange Security job that placed this email in quarantine
- Name of the Exchange server
- Name of the email file
- Processing history

Communication with the quarantine

Communication with the Quarantine uses SOAP (Simple Object Access Protocol) and SSL (Secure Socket Layer). This applies both for directing "local" access to the server and for accessing from a remote Windows workstation.

Port 8008 is the default communication port. This port can be changed in the Avira Exchange Security Management Console (under the server's node). If this port is changed for the server, this change must also be adapted to all accessing consoles. All computers must use the same port.

SSL is used for encrypting the SOAP communication channel. All the necessary components are provided during installation.

3.2.4 The Active Directory/ LDIF

Avira Exchange Security does not make any changes or additions to the Active Directory (AD). However, Avira Exchange Security reads information from the Active Directory at various stages.

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

The Avira Exchange Security Management Console uses the Active Directory when selecting sender or 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).

3.2.5 Compressed files or archives - Avira Exchange Security Unpacker

Files are often compressed when sent by email. To ensure that the virus scan and all checks also work for archives, Avira Exchange Security uses an included unpacker to be able to check files within the archive.

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

By default, nested archives (recursively packed files) are unpacked to a depth of 5 levels. All archives that exceed this limit are transferred to the BADMAIL area.

The default upper limit for an email including unpacked files is 300 MB. This limit 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 > Avira Server > Properties > General**.

3.3 The configuration file of Avira Exchange Security

All the information required to run Avira Exchange Security is stored in the configuration, in the form of an XML file (*ConfigData.xml*), with separate 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 is required both by the Avira Exchange Security Server and by the Avira Exchange Security Management Console. Among other things, the Avira Exchange Security Server uses this information for the Avira Exchange Security job.

To be able to make changes to the configuration with the Avira Exchange Security Management Console, the console requires access to the *ConfigData.xml* file.

The configuration information for Avira Exchange Security can be stored both in a local directory and on a network share. An entry in the registry defines which Avira Exchange Security configuration is used by the Avira Exchange Security Management Console or by the Avira Exchange Security Server.

The path to the Avira Exchange Security configuration can be specified in "C:\..." format or as UNC path `\\Servername\Share\ConfigData.xml`.

If the specified Avira Exchange Security configuration is not available, Avira Exchange Security uses the so-called "Last-Known-Good" configuration, which 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 Exchange Security configuration. It is possible to access the "Last-Known-Good" configuration from the Avira Exchange Security configuration.

3.3.1 Using a custom configuration file

A parameter is available to use a custom configuration file.

To open a custom configuration file in the console, start the *Avira.msc* file with parameter *config* and the required configuration file.

```
"C:\Program Files(x86)\Avira\Avira Exchange Security  
\Avira.msc" config "C:\OtherFolder\Directory\ConfigData.xml"
```

You can also specify a UNC path here.

4 Avira Monitor

You can use Avira Monitor to observe all the quarantine and bad mail areas on every available server. You can also access the statistical evaluations.

Avira Monitor lists all the servers configured under **Basic Configuration > Avira Server**.

Avira Monitor uses SOAP/SSL encryption to access the server via the network.

Related topics:

[Access methods](#) - page 16

4.1 Setting the access to Avira Monitor

1. To access a server, first add it under **Basic Configuration > Avira Server** and refresh Avira Monitor in this view.

Note

The access to details in Avira Monitor also depends on each quarantine's configuration.


2. To display detailed information about the version of Avira Exchange Security and about the configuration for every server, right-click on the required server in **Avira Monitor** and select **Properties**.
3. If you are not logged locally on the server, a login dialog appears for you to enter your user name and the password for the relevant domain. The authorization for accessing Avira Monitor is entered in the properties of the file *access.acl* in the folder ... \Avira\Avira Exchange Security\AppData.
4. Click the **Security** tab and assign the relevant user at least read-only rights.


Related topics:

[Making settings for an individual Avira Server](#) - page 106

[Quarantine configuration](#) - page 131

4.2 Using the Avira Monitor

1. Click the required server.
2. Authenticate yourself with a user name and password that has authorizations for the Avira data on the server's file system.
3. Click on the area you want to view, for example on **Default quarantine** or **BADMAIL**. All existing emails are displayed (limit: 10,000 emails).
4. Available actions:
 - Filter the required emails with the **Filter Options** icon .

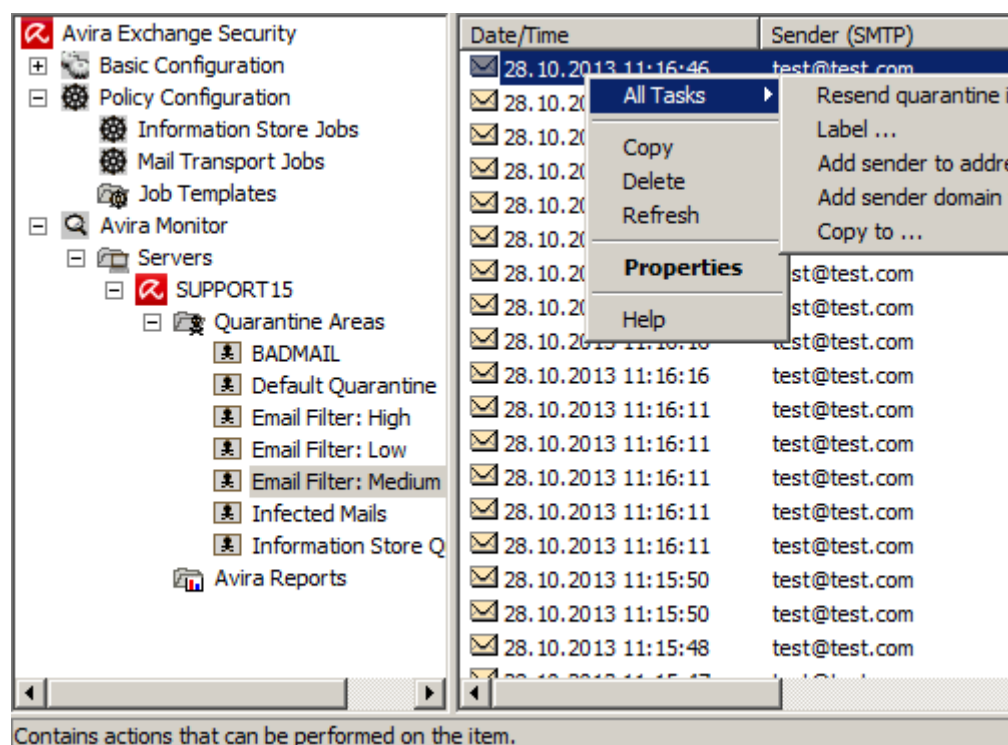
- Open an email with a double-click.
- Send the email by clicking the **Resend** button  a second time if necessary.


4.3 Using quarantines

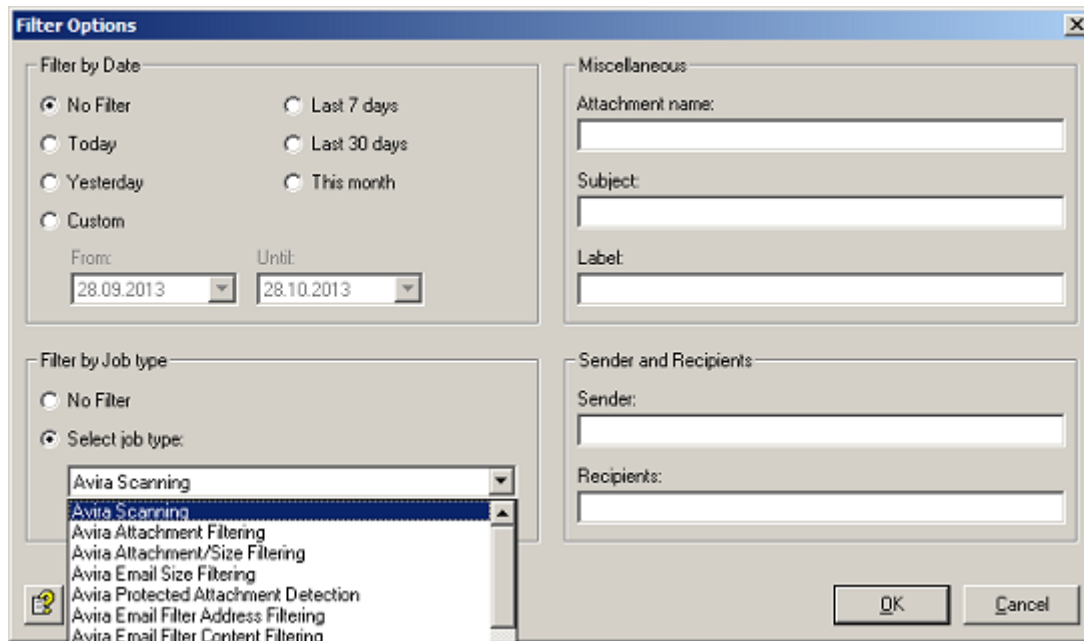
If you enabled the **Copy to quarantine** action in the job, then all affected emails are in a quarantine and all available information on the individual emails can be found in the Avira Monitor

Within a quarantine, it is possible to filter emails according to numerous criteria.

1. Click the quarantine.
A maximum of 10,000 emails (the most recent) are displayed in the Avira Monitor.
2. Available actions:
 - To obtain older emails that are no longer listed, restrict the view using a corresponding filter option.
 - If you want to move an email to a different quarantine, you can use your mouse to drag it.
 - Right-click the email in the list and select an action.




3. To filter the emails:
 - Right-click **View > Filter Options**.
 - Click the **Filter Options** icon .



The **Filter Options** dialog box is used to configure email filtering rules. It contains the following sections:


- Filter by Date:** Includes radio buttons for **No Filter**, **Today**, **Yesterday**, **Custom**, **Last 7 days**, **Last 30 days**, and **This month**. Below these are **From:** and **Until:** date pickers, currently showing 28.09.2013 and 28.10.2013 respectively.
- Filter by Job type:** Includes radio buttons for **No Filter** and **Select job type:**. Below is a list box showing various job types, with **Avira Scanning** selected. The list includes:
 - Avira Scanning
 - Avira Attachment Filtering
 - Avira Attachment/Size Filtering
 - Avira Email Size Filtering
 - Avira Protected Attachment Detection
 - Avira Email Filter Address Filtering
 - Avira Email Filter Content Filtering
- Miscellaneous:** Contains text input fields for **Attachment name:**, **Subject:**, and **Label:**.
- Sender and Recipients:** Contains text input fields for **Sender:** and **Recipients:**.

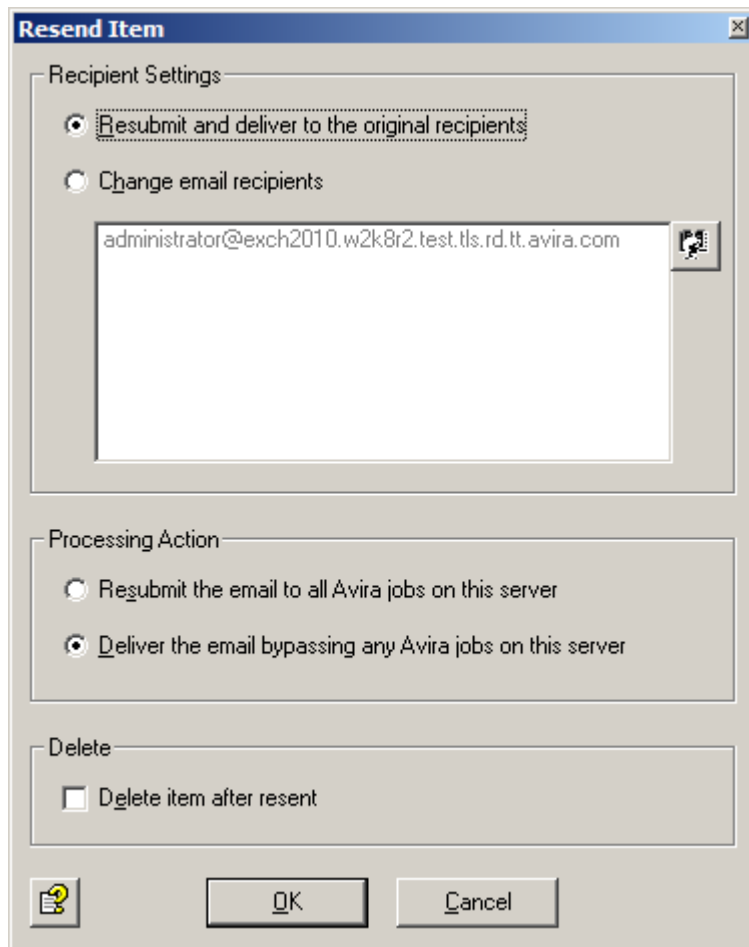
At the bottom right are **OK** and **Cancel** buttons.

4. To reset the filters:
 - Enable the **No Filter** option in **Filter Options**.
 - Right-click **View** > **Show all objects**.
 - Use the **Deactivate filter** button  in the toolbar.


4.4 Sending emails from quarantines

If you want to deliver an email from quarantine to its original or another recipient, you can send it directly from the quarantine, without having it checked again by a job in Avira Exchange Security.

1. Open the list of emails of a quarantine in the **Avira Monitor**.
2.
 - Right-click the required email and then select **All Tasks** > **Send from Quarantine**.
 - Click the **Resend** button  in the **Properties** window.



The recipient sees the original sender in the **From** field of the email (not as forwarded email).

3. Optional: You can change the recipient by enabling the **Change email recipients** option, then clicking the **Select address** button .

Note

When selecting addresses for the resending of emails from quarantine, no address lists are available.

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

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

Note

This is the default setting. If you enabled jobs that also scan resent emails from quarantine, then set this option to **Resubmit the email to all Avira 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 option **Resubmit the email to all Avira jobs on this server** applies for the jobs for which the option **Quarantined emails: Check before sending** was enabled. Even if you want to have the quarantine emails processed again, all jobs for which the option **Ignore emails resent from quarantine** is enabled are excluded.

Related topics:[Address lists](#) - page 117

4.5 Adding a sender to an address list

The option **Allow adding addresses from quarantine** must be enabled within the address list. Otherwise, the required sender address cannot be added to the list.

If a sender's email was placed in quarantine but you want to allow this sender's emails in the future, you can place the sender on one of your address lists, e.g. *Email Filter: Whitelist*.

1. In the **Avira Monitor**, open the quarantine containing the required email.
2. Right-click 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.

Related topics:[Address lists](#) - page 117

4.6 Adding a domain to an address list

The option **Allow adding addresses from quarantine** must be enabled within the address list. Otherwise, the required sender domain cannot be added to the list.

If emails from a certain domain are placed in quarantine, but you want to allow emails from all users of this domain in the future, you can place it on one of your address lists.

You do not have to enter all sender addresses individually in the address list. The address is added to the list in the form of `*@samplecompany.com`.

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

4.7 BADMAIL

BADMAIL contains all emails that could not be processed by the Avira jobs, such as emails with formats that cannot be processed.

Very little information exists about bad mail, because Avira cannot inspect these emails. Bad emails may also contain an undetected virus.

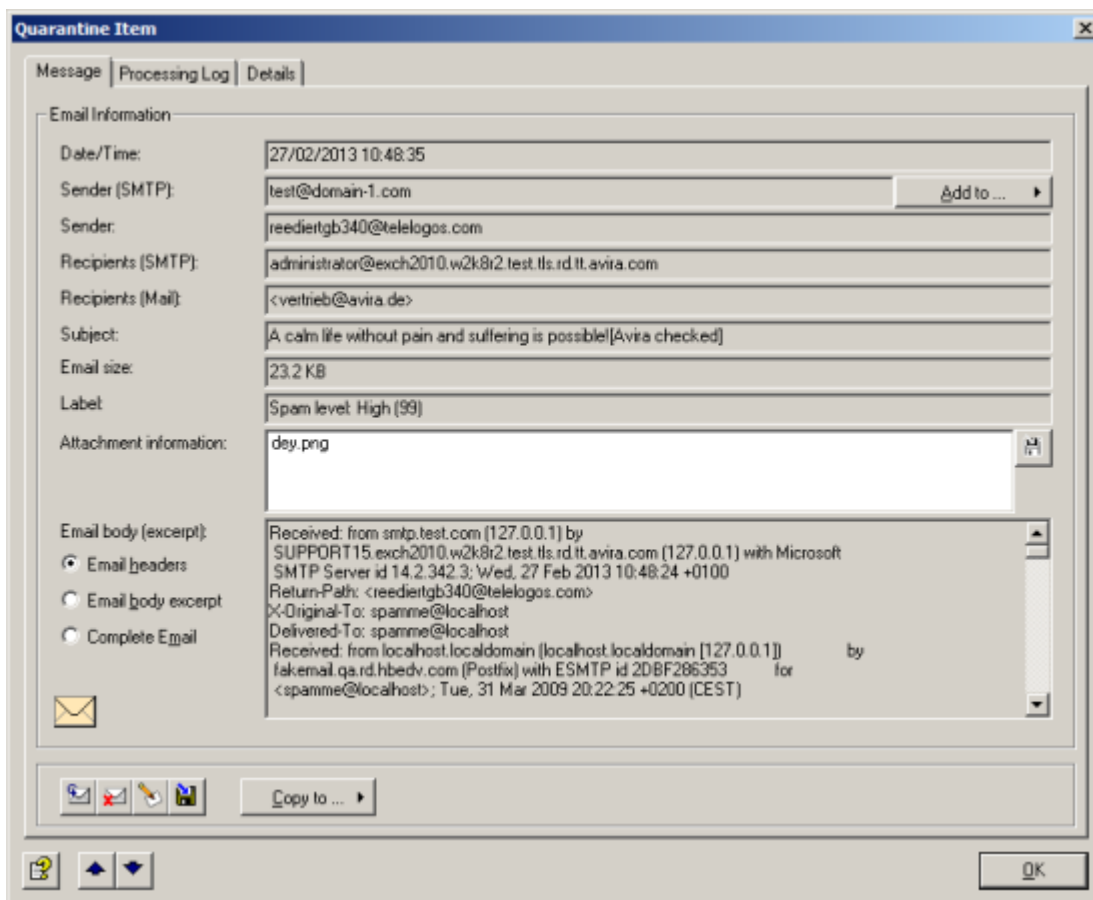
There is only one folder for bad mail on each server. The same functions and options apply for bad mail as for quarantine emails, except that no additional folders can be created.

4.8 Details of a quarantined email

You can see the details of a quarantined email, if you double-click or right-click the properties of the email in the quarantine list.

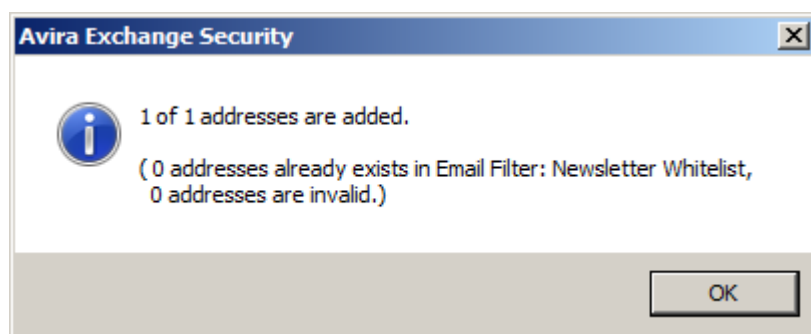
4.8.1 Message details

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



The **Add to** button allows you to add the SMTP sender of the email to the unwanted email defense of a specific address list. You define for each individual address list which address lists are displayed under this button.

Once the sender address has been added to the address list, you receive a message.

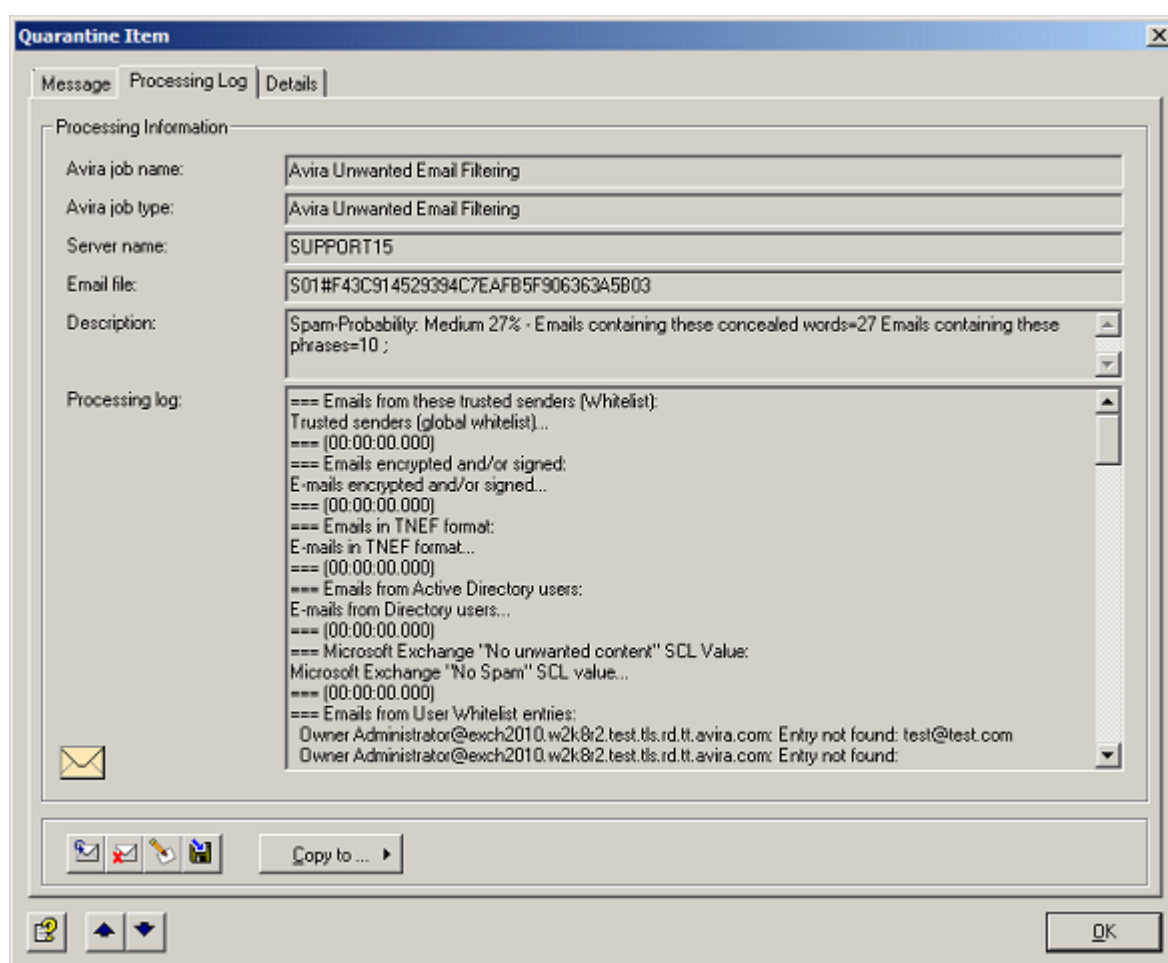


Related topics:

[Address lists](#) - page 117

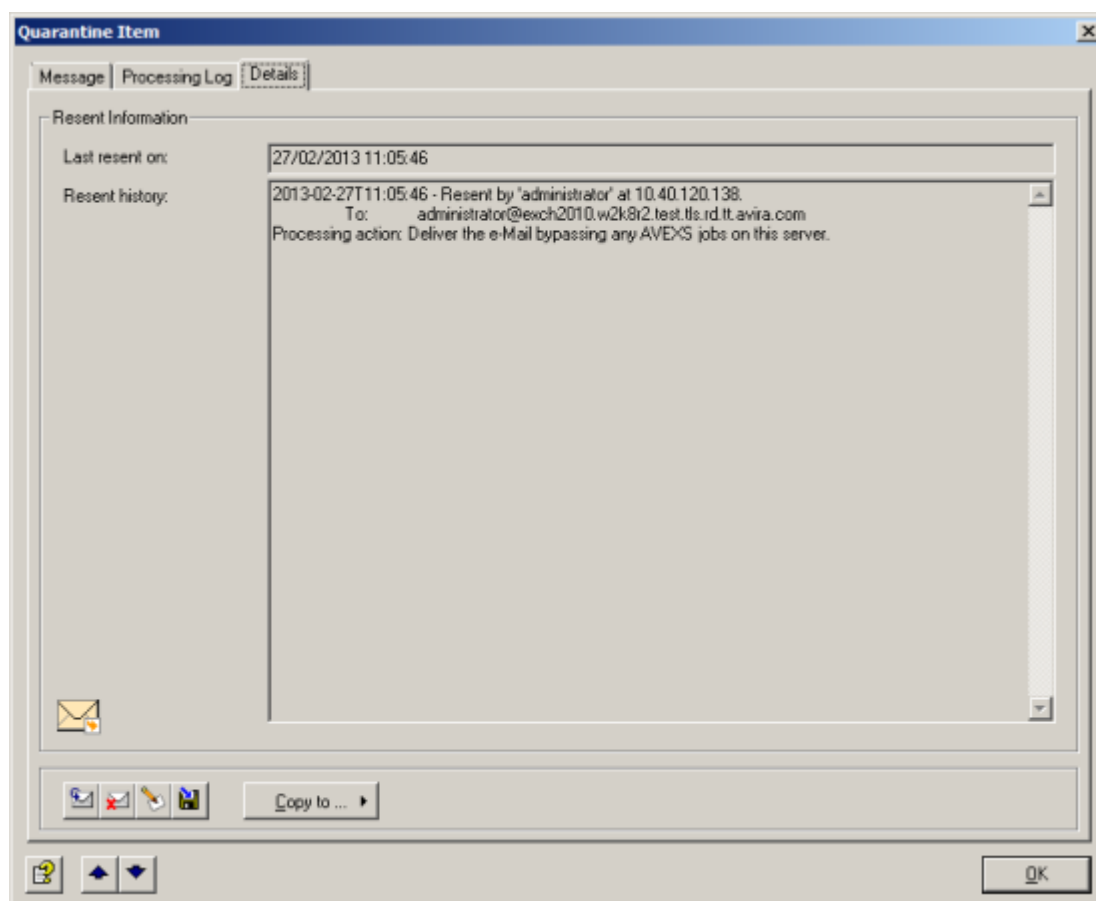
4.8.2 Quarantine processing log

The name of the job that placed the email in quarantine, the job type, the server, the reason for blocking and sending the message to quarantine, and further processing details are available under **Processing Log**.



4.8.3 Quarantine details

Information about the re-sending of the email from quarantine is available under **Details**.

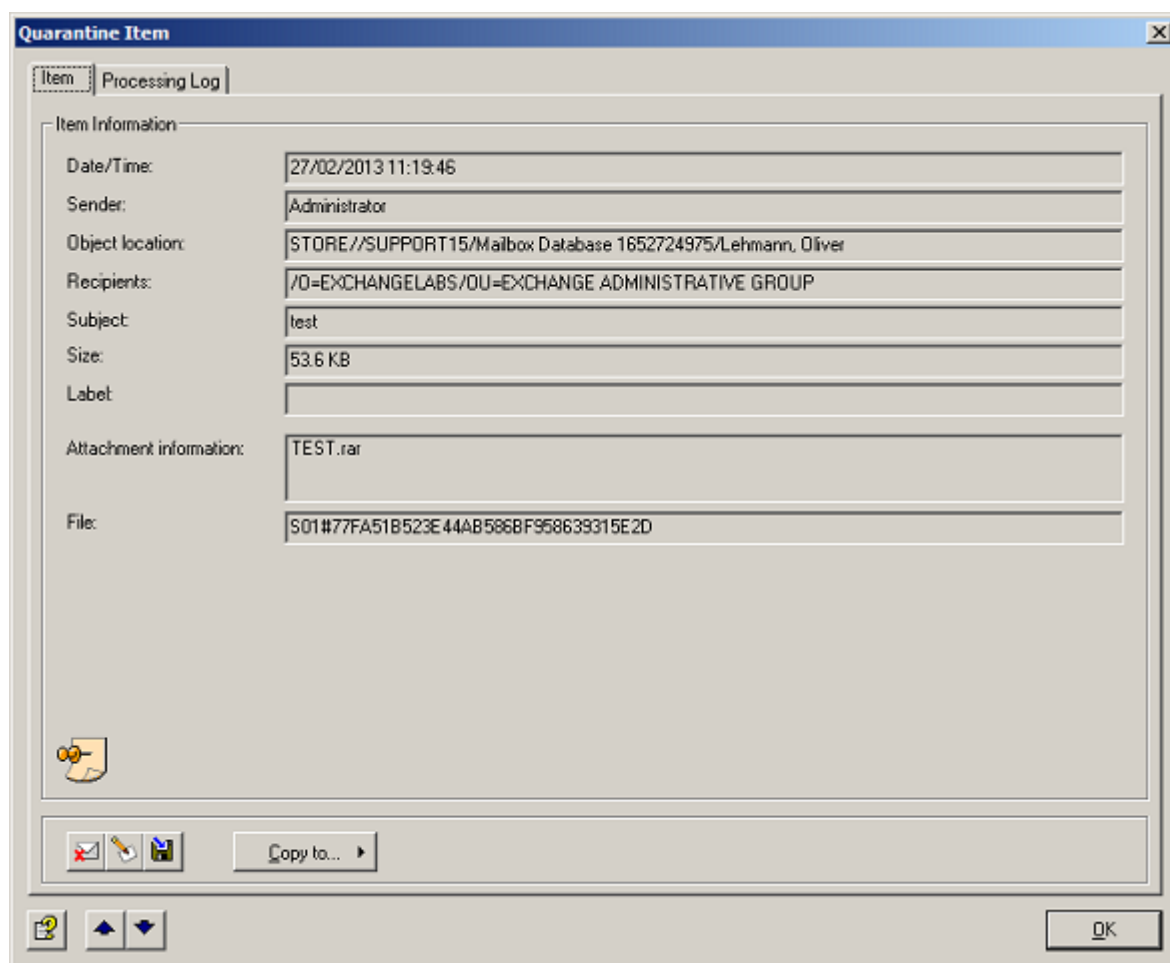


4.9 Details in the IS quarantine

You can see the details of a quarantined email, if you double-click or right-click the properties of the email in the quarantine list.

4.9.1 Message details in IS quarantine

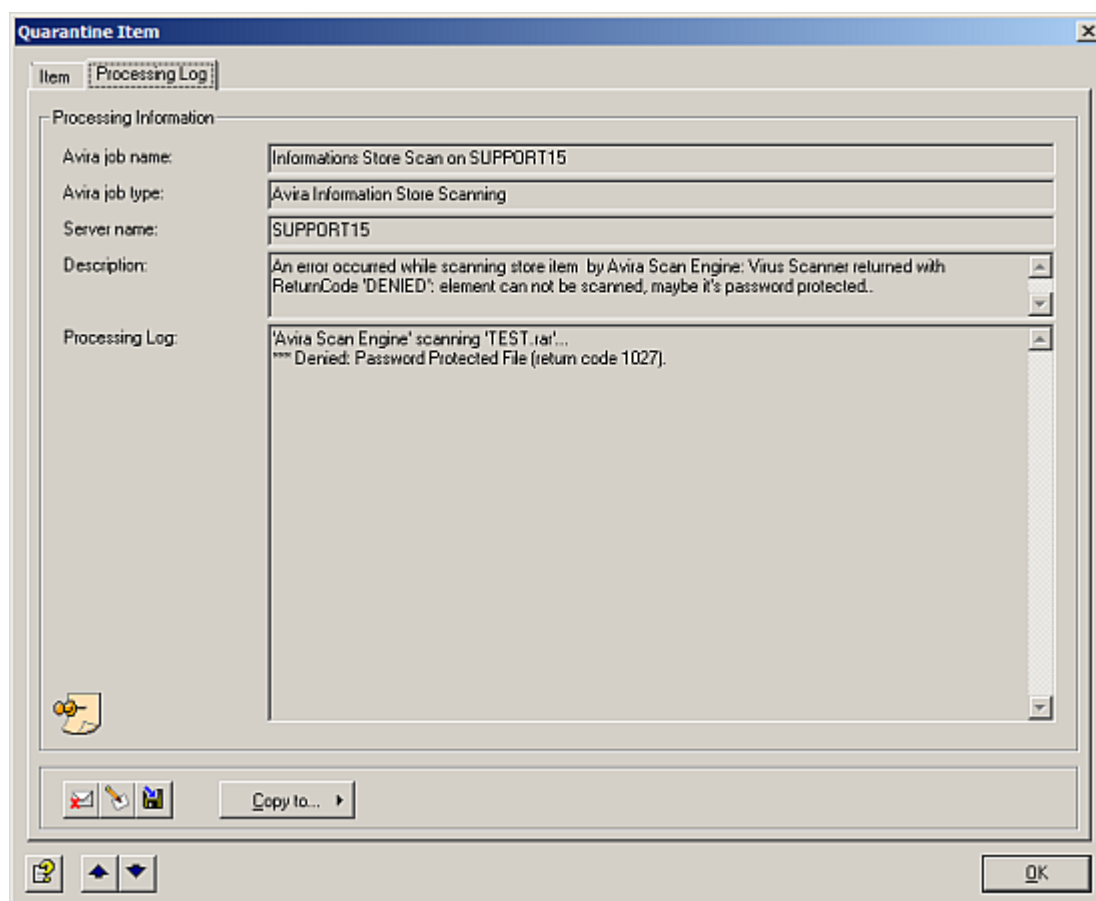
The most important information about emails in Information Store quarantine can be found at a glance on the **Item** tab.



The **Copy to** button allows you to copy the email to another quarantine on the same server.







4.9.2 IS Quarantine processing log


The name of the job that placed the email in quarantine, the job type, the server, the reason for blocking and sending the message to quarantine, and further processing details are available under **Processing Log**.



4.10 Quarantine buttons

List of the buttons available in the quarantines.

Button	Action
	Send email from quarantine (not in IS 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

Button	Action
	Previous email in the quarantine/ bad mail

4.11 Statistics in Avira Exchange Security

You can generate detailed information about email processing, using the statistics in Avira Exchange Security under **Avira Monitor**.


There are several predefined statistical reports available, as well as one advanced report that you can customize. They contain graphics and tables with information about detected policy violations (viruses, unwanted file attachments, etc.). A separate report exists that answers the most frequent questions. Data relating to Avira quarantines is also reported.

You can choose the period for which to generate the data.

The print and export buttons allow you to reuse the data easily.

Generally, processed emails do not appear immediately in the statistics. The data is cached during processing and is recorded in the evaluation database twice per hour.

4.12 Generating statistics

1. Click **Avira Reports**.
2. On the statistics list, double-click the name of the statistic you want to generate.
3. Specify the required period for the data.
4. To export the data, click the **Export** button .
You can choose between different formats.

5 Avira Scan Engine

Avira Scan Engine is used for scanning emails for viruses, for type and size of attachments and for the total email size.

Note

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

Job types

Job type	Description
Avira Scanning	Virus scan of incoming and outgoing emails
Information Store Scan	Virus scanning in MS Exchange databases (on access, proactive/ background)
Avira Protected Attachment Detection	Blocking password-protected archives
Avira Attachment Filtering	Blocking of specific file types in the attachment
Avira Email Size Filtering	Restriction of the email size
Avira Attachment/ Size Filtering	Restriction of type and/ or size of attachments

5.1 Avira Scanning jobs

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

The Avira Scanning 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.

Some possible scenarios:

- If a virus is found, the original email should be cleaned and then delivered to the recipient.
- If the original email cannot be cleaned, the affected email is copied to the folder selected by you (quarantine), the original is deleted and not delivered.
- Messages are sent to the administrator, sender and recipient, containing the relevant information regarding the virus scanner and the Avira Scanning 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

5.1.1 Configuring and enabling Avira Scan Engine

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

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

The preconfigured return codes can be processed in the **Return Code Settings** tab. If you make changes to this tab, we recommend documenting your changes on the **Details** tab.

Testing the DLL interface

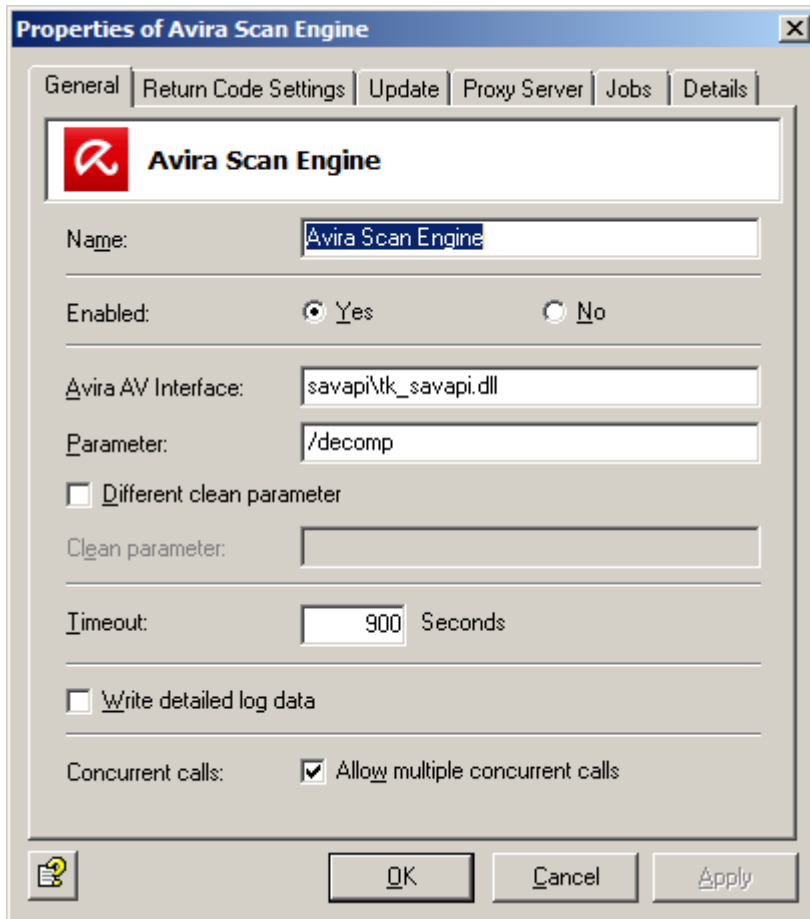
Avira Exchange Security accesses the virus scanner by means of a DLL file, the so-called Avira AV Interface.

Warning

Disable the real-time or on-access scan functions of any virus scanners you use, for the directory ...\\Avira\\Avira Exchange Security\\AppData.

1. Click the required server name under Avira Monitor and click **Server Status** in the right-hand window.
2. On the **Scan Engine Test** tab, select **Scan Engine Test**.
If the test is successful, the message contains the status *OK*, indicating that an EICAR test virus has been found.

General properties of Avira Scan Engine



- Type the name of the Avira interface DLL in the field Avira AV Interface. This DLL file is the connection between Avira Exchange Security and the virus scanner. The value is preconfigured for every virus scanner and cannot be changed!
- In the **Parameter** 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 option **Different clean parameter** and specify the associated parameter in the field **Clean parameter**.

Note

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

Note

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

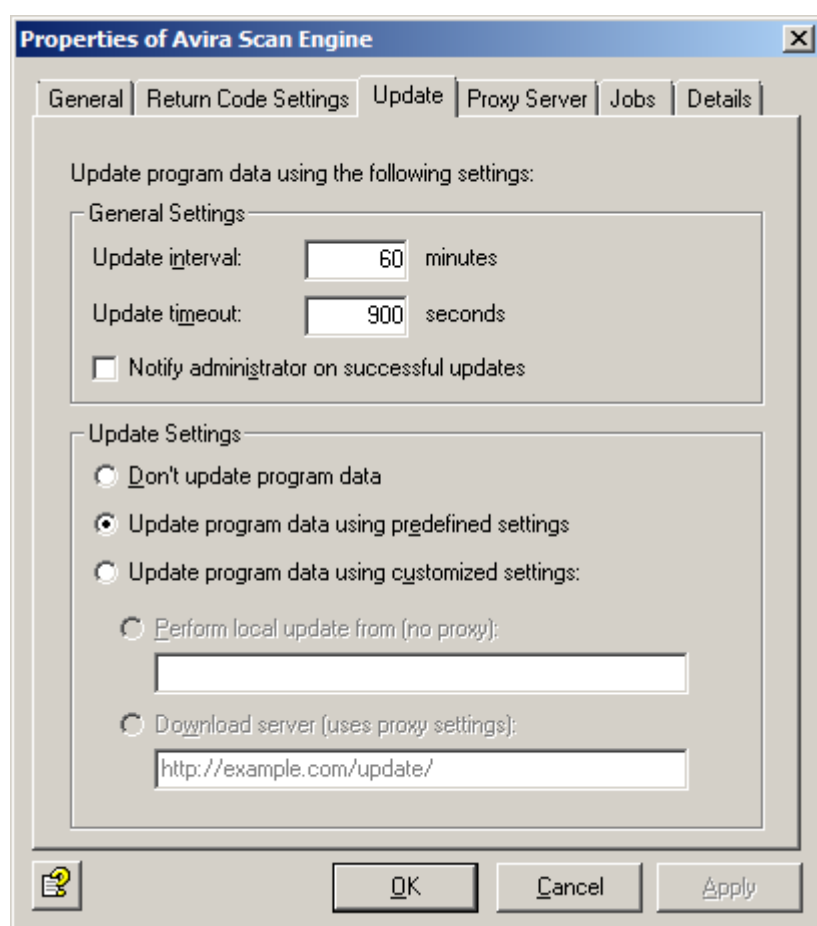
- **Timeout:** Specify the number of seconds after which an attempt to connect to the server is to be canceled (if the connection has not been established by then). When specifying a time, please consider the performance of your server. Minimum value: 60 seconds.
- **Allow multiple concurrent calls:** When active, several emails can be processed by this virus scanner at the same time. The number of calls is defined in **Avira Exchange Security Server > Properties > General > Number of threads**.

Related topics:

[Making settings for an individual Avira Server](#) - page 106

Update properties of Avira Scan Engine

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



- **Update interval:** Interval in minutes at which the pattern update scanning takes place. Minimum value: 15 minutes.
- **Update timeout:** The update procedure will be canceled after this time. Minimum value: 60 seconds.

- **Download server (uses proxy settings):** You can use a proxy server to update the virus pattern. Select the required proxy server in the **Proxy Server** tab.

Warning


To update Avira Exchange Security please do not use this tab, but rather select the **Scan Engines/Email Filter Update** option under **Avira Monitor > Server Status > Scan Engine Test** and click **Start**. After the update you will receive a detailed update report.

5.1.2 Activating a virus scanning job

1. Double-click the job **Scanning with Avira Scan Engine** under **Policy Configuration > Mail Transport Jobs**.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.
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 shows the job is enabled.
4. Set 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.
5. Set 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).

6. On the **Actions** tab, define the actions to be carried out when the job has found an infected email.
7. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
8. Write a description of the job on the **Details** tab.
9. Click the button **Save Configuration** .

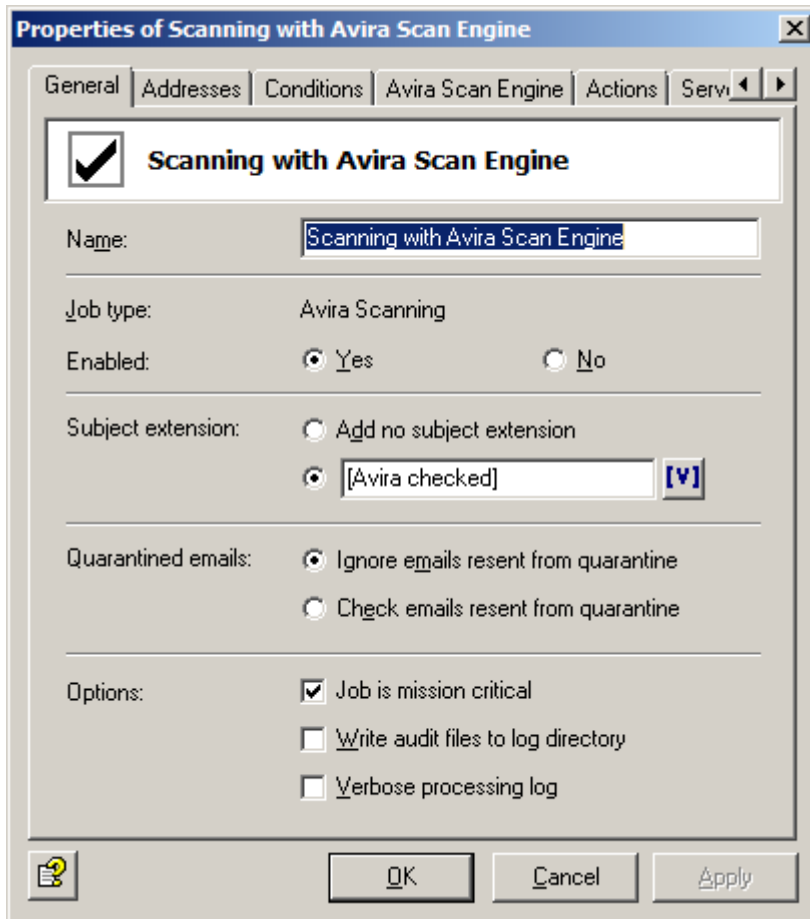
Related topics:

[Address lists](#) - page 117

[Job conditions](#) - page 142

[Making settings for an individual Avira Server](#) - page 106

General settings for virus scanning jobs



- The default for the **Subject extension** is *Avira checked*. This additional text is added to the subject line of every email checked by the job.
- The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

- **Job is mission critical**: Activate this option for mission-critical jobs such as virus scans.
- **Write audit files to log directory**: Activate this function if you have to produce verification or if you want to test a job.

Related topics:

[Sending emails from quarantines](#) - page 24

Mission critical jobs

A job is **mission critical** if the email is to be placed in the BADMAIL area in the event of a processing error, for example if the virus scanner is not found.

Warning

When this option is set, **every** email (incoming or outgoing) is kept in the BADMAIL area until the processing error is fixed.

A job is **not mission critical** if the result of the job is to be ignored for the email in question, even 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.

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.

Job processing log

You can use the processing log to observe the processing of the emails during the job. Activate this function if you have to produce verification or if you want to test a job.

When you activate this option, information as to whether and how the job processed the respective email is written to a text file for every processed email. This log text file is stored in the *Log* folder in the installation directory of Avira Exchange Security. 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*, for example *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:

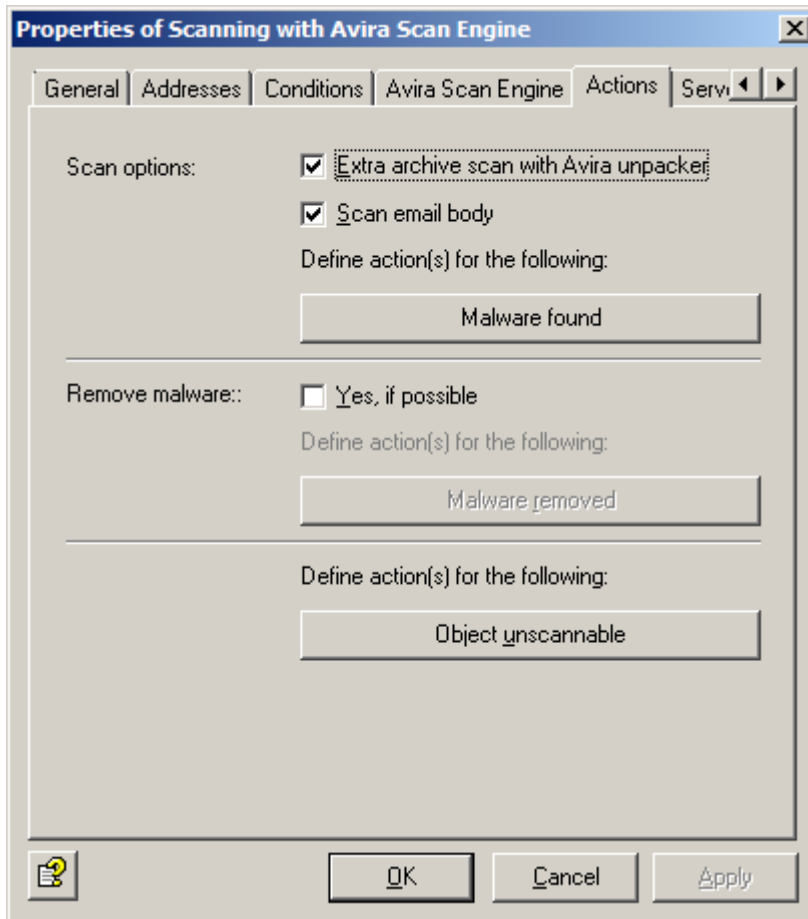
1. Date and time the email was processed.
2. Job ID
3. Job name
4. Message ID
5. SMTP sender
6. SMTP recipient
7. Result of the scan by Avira Exchange Security
 - Restricted - email matches the defined restrictions
 - Unrestricted - email does not match the defined restrictions

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

Action settings for virus scanning jobs

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

Example:



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 unwanted emails that contains viruses), it is more effective to send attachments with viruses to quarantine.

Note

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

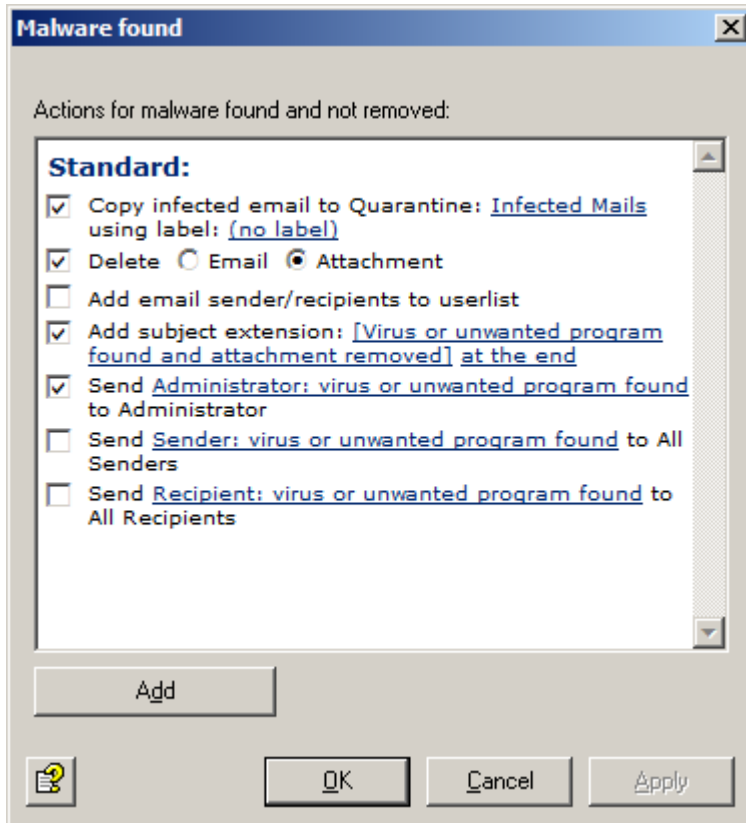
Define how to proceed with unscannable objects.

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

1. **Malware found:** For the event that a virus was found and the file could not be successfully cleaned.
2. **Malware removed:** 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.

Actions for malware found



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

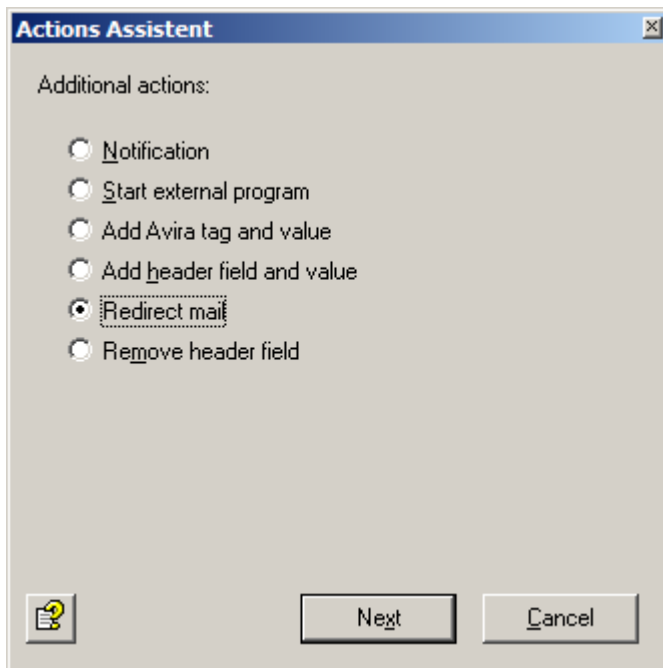
Check whether virus mails sent to your company are frequently also unwanted emails. If this is the case, it is best to immediately delete the entire email and not only the attachment. In this way, there is no need to also check the remainder of the message texts for unwanted emails.

Note

If you enabled the **Scan email body** option and if the **Delete attachment** option was set, when a virus is found in the text, the entire email, including the attachments, is deleted (an attachment is not delivered without the message text). The affected email section 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.

Further actions for malware found



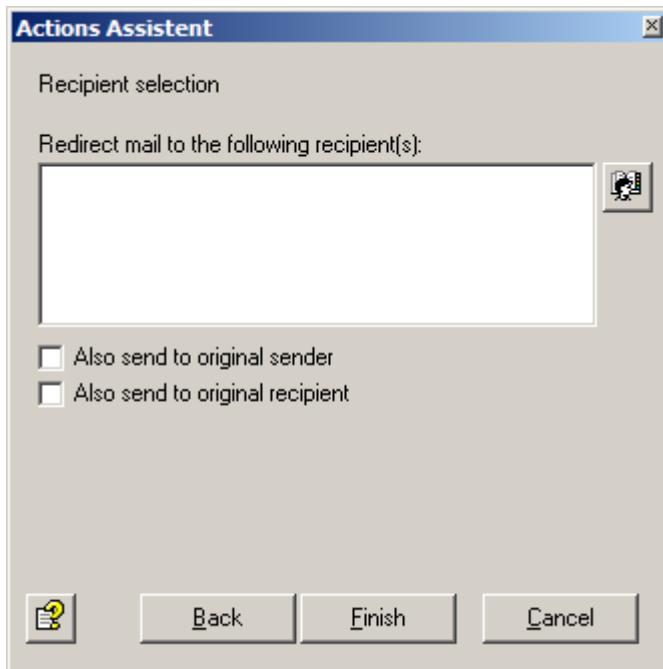
- **Notification:** Select the recipient of the notification from the address book.
- **Start external program:** A new program/application can be defined to execute the actions of this application. To start an external application, specify the path and, if applicable, the necessary parameters.
- **Add Avira tag and value:** Email header tags can be set during processing, so that special Avira Exchange Security 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 email header tags are removed.
- **Add header field and value:** Define a new X-header field and select the variable to be inserted for example, in order to output the result of an email filter analysis as a value. Unlike the email 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 suggested as an additional action.


Note

Special information with regard to **Redirect mail**: If you redirect a TNEF email 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.

- **Remove header field:** The email X-header fields are removed. You can use this action, if you want to delete the X-header fields defined previously on other servers.

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 options.

Click **Finish** to save the action settings.

5.2 Information Store Scan jobs

For Microsoft Exchange Server as of 2013 a separate EWS user with certain access rights must be created.

Create EWS user with certain access rights:

1. Open the Exchange Management Console, e.g. via `https://localhost/ecp`.
2. Create a new user (including mailbox). In this example the user is called `ews_user`.
3. Open the 'Exchange Management Shell' and provide the user with the required rights by calling the *SetEWSPermissions.ps1* script in the *Avira Exchange Security/Bin* directory. To set the access rights on the Exchange server, enter the following: `SetEWSPermissions.ps1 -User "user name" (without domain)` Example: `SetEWSPermissions.ps1 -User ews_user`

Note

Access rights can only be set for public folders that are currently available in the Information Store. When changing the database-related settings for the public folders (e.g. adding a new folder), the script must be executed again to set the required rights for the changed elements.

Specify the `ews` user including the password in the Avira Server settings:

GENERAL SETTINGS -> Avira Server settings -> OPTIONS tab. Enter the user name including the domain e.g. `ews_user@mydomain.com`.

In addition to the virus scan on transport level, Avira Exchange Security 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 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, for example drafts.

The settings for the information store scan are server-wide. There is always only one Information Store Scan job available for each server, and not any number like for Avira Scanning jobs.

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

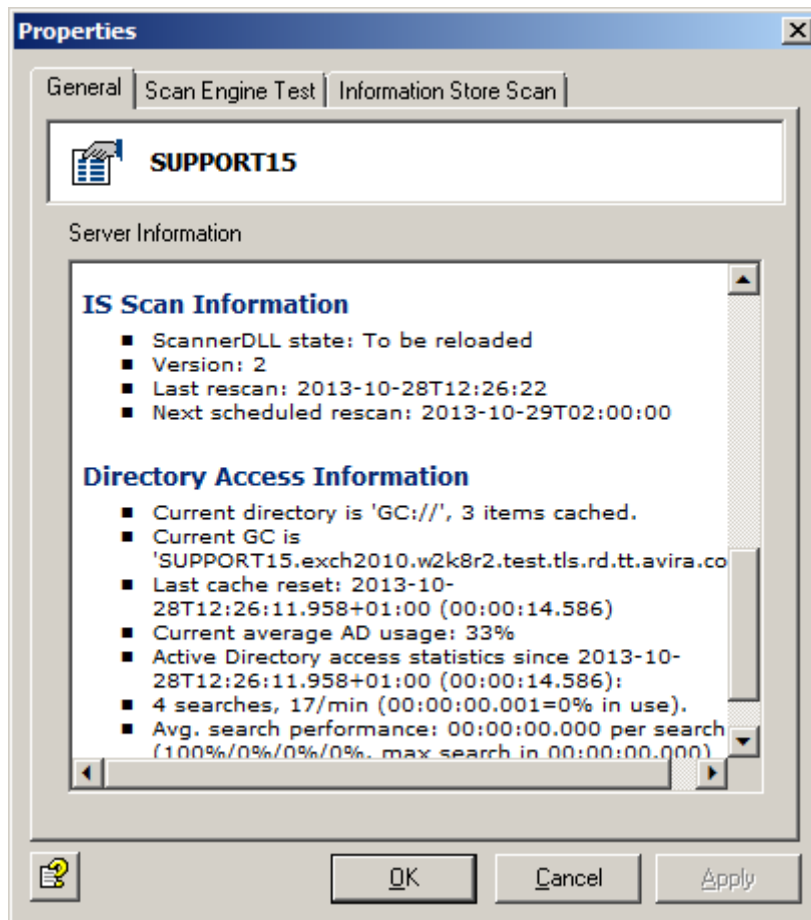
For messages that are blocked by the information store scan, there may be error messages during data back-ups of the information store.

Warning

Exiting or uninstalling Avira Exchange Security, 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.

5.2.1 Checking the status of the Information Store

1. Click **Avira Monitor** > **Server** > **Server Status**.
2. Click the **General** tab.



ScannerDLL state shows *Loaded*, when the information store scan is active.

Version shows the version of the information store scan. Each restart increases this value.

Last rescan shows when the last version update occurred and the time and date of the last restart.

Next scheduled rescan shows the time and date of the next rescan, if scheduled.

5.2.2 Restarting the Information Store Scan

Warning

When you restart the scan, all elements in the information store are scanned again. This scan may need more time and resources. It is therefore recommended that you restart at off-peak times and depending on the virus scanner update.

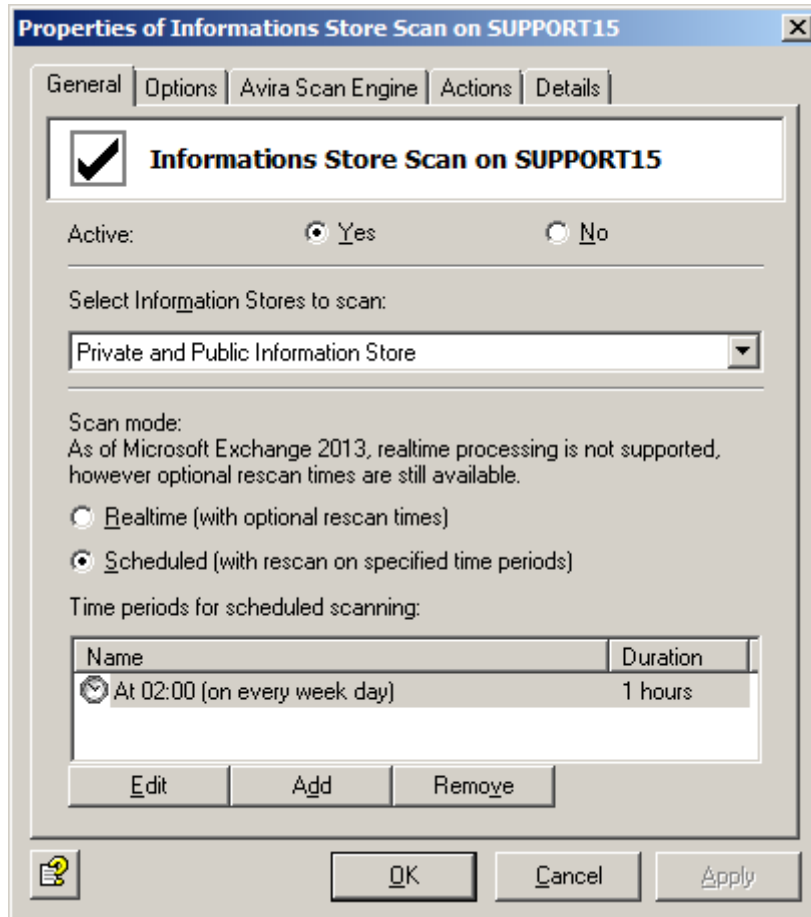
1. Click **Avira Monitor > Server > Server Status**.
2. Click the tab **Information Store Scan**.
3. Click **Rescan now**.

5.2.3 Activating the Information Store Scan job


Warning

When you enable/ disable the Information Store Scan job, it can take up to two minutes before the Exchange Store registers the change.

1. Double-click the job Information Store Scan under **Policy Configuration**.



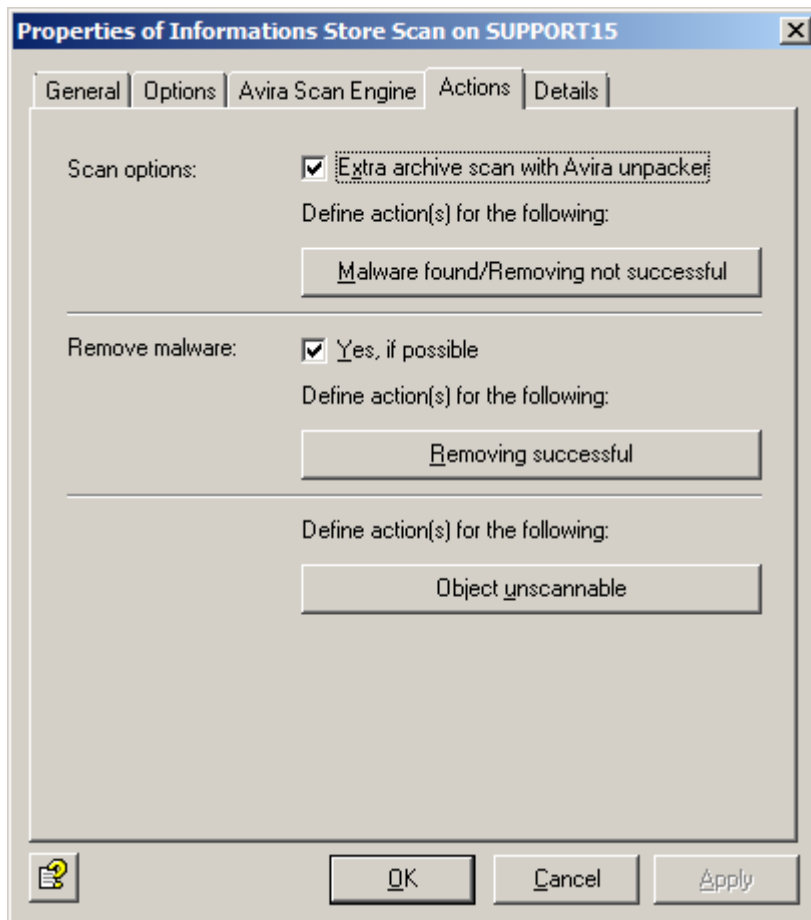
2. On the **General** tab, click **Yes** to enable the job and make further general settings. The job is enabled as soon as you save your settings with **OK** and close the job. The checkmark in the job icon immediately shows the job is enabled.
 - **Select Information Stores to scan:** Choose the stores to be scanned from the drop-down list.
 - **Scan mode:** Enable the **Realtime** or the **Scheduled** scan mode.
 - **Rescan times for realtime scanning:** Optionally, you can manage rescan times, if you use the realtime scan mode.
3. On the **Options** tab, you can enable the options **Job is mission critical** and **Use SMTP server to send notifications**.
4. On the tab **Avira Scan Engine** you can edit the list of scan engines and specify the behavior in case of errors.
 - At least one scan engine must run error free

- All scan engines must run error free
- 5. On the **Actions** tab, define the actions to be carried out when the job has found an infected email.
- 6. Write a description of the job on the **Details** tab.
- 7. Click the button **Save Configuration** .

Related topics:

[Mission critical jobs](#) - page 38

Action settings for IS jobs



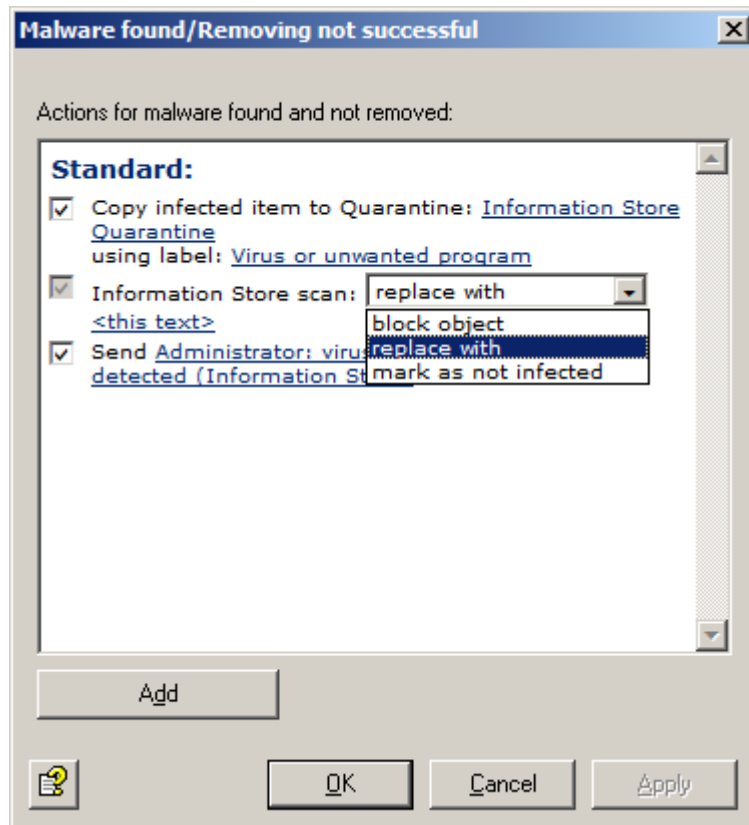
The **Actions** tab is used to define which actions are to be carried out when the job has found an infected email.

- **Extra archive scan with Avira unpacker:** When this option is enabled, an internal unpacker first extracts the packed files and then sends them individually to the virus scanner.
- **Remove malware:** If you want the IS job to attempt to remove the malware, activate the option **Yes, if possible**.
- You have to set the actions for the following situations:

- **Malware found/Removing not successful**
- **Removing successful**
- **Object unscannable**

Setting actions for malware found

Malware found/Removing not successful handles the case when a virus was found and the file could not be successfully cleaned.

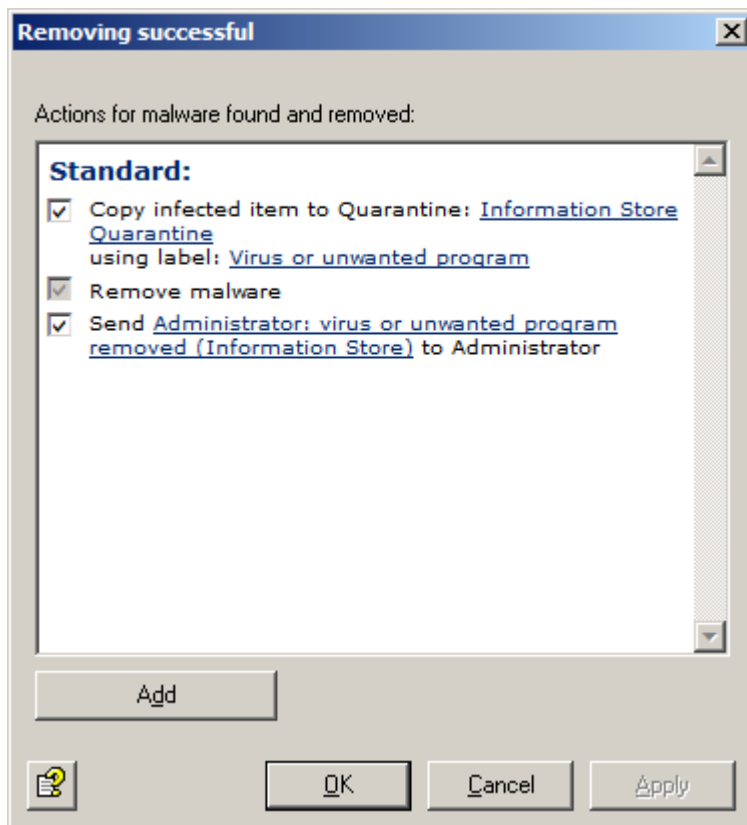


1. Select whether a copy of the object is to be placed in a quarantine and labeled.
A special default quarantine is available for the information store scan.
2. Specify how the IS should handle the object.
 - **block object:** Blocking prevents access to the entire message object. With current Microsoft email clients, a corresponding error message is displayed when an attempt is made to open such an email message. With other/ older email clients, there may be different feedback. However, the blocked messages can always be deleted via the client.
 - **replace with:** It replaces the infected element of the message (for example, the 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, because the user is not protected.

3. Select whether a notification is to be sent to the administrator(s).
4. Click the **Add** button to select further actions, such as to send notifications to any recipients or to start an external application.

Setting actions for removed malware

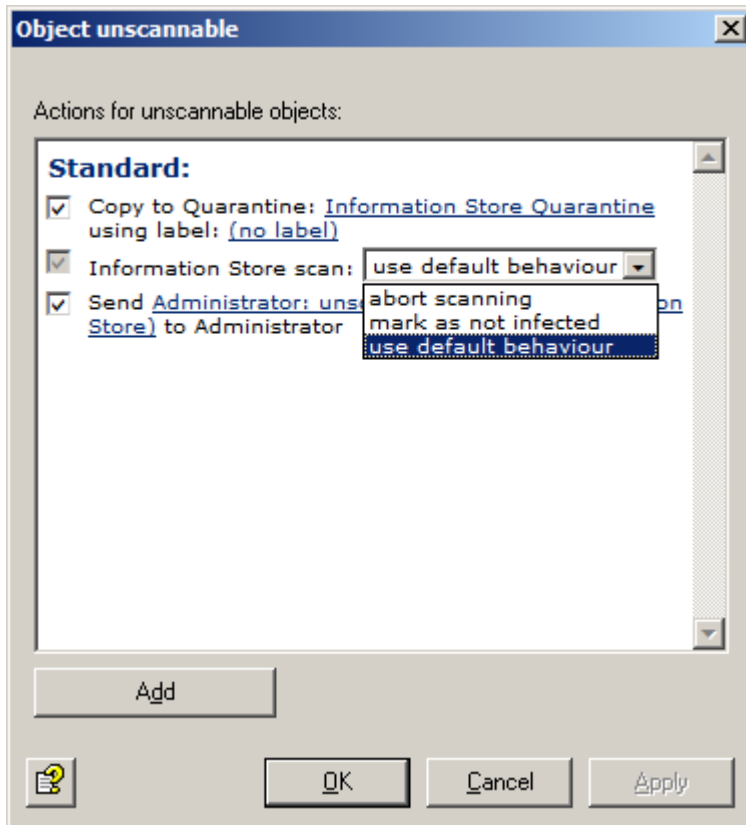
Removing successful handles the case when the file was successfully cleaned and the virus was removed.



1. 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.
2. Select whether a notification is to be sent to the administrator(s).
3. Click the **Add** button to select further actions.

Setting actions for object unscannable

Object unscannable handles the case when the files could not be scanned. This allows you to influence the behavior of Avira Exchange Security when encrypted objects are found, which due to their nature cannot be viewed and therefore cannot be scanned for viruses

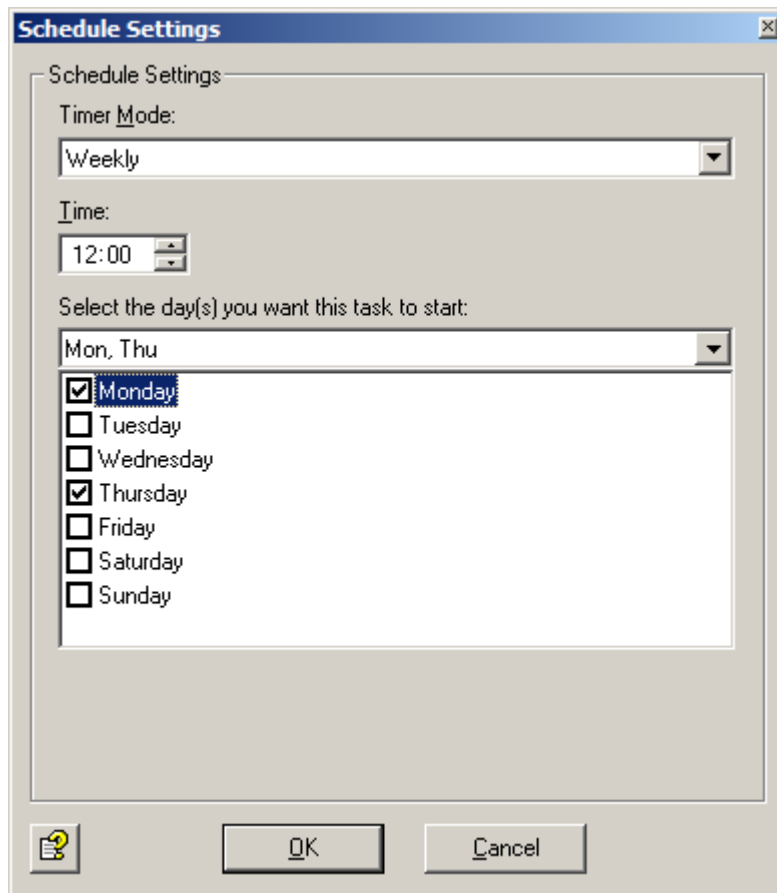


1. Select whether a copy of the object is to be placed in a quarantine and labeled.
2. Specify how the IS should handle the object.
 - **abort scanning:** The object is scanned again during the next scan process. Access to this option is blocked if previous scan processes handled the object as virus-free.
 - **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** under **Basic Configuration > Avira Server > General**.
3. Select whether a notification is to be sent to the administrator(s).
4. Click the **Add** button to select further actions.

Scheduling the Information Store Scan

You can create a schedule for restarting the Information Store Scan.

1. Double-click the job Information Store Scan under **Policy Configuration**.
2. Activate the **Scheduled** scan mode.



3. Make the schedule settings.

- Timer Mode
- Time
- Days of the week

4. Click **OK**.

5.3 Avira Protected Attachment Detection

In order for Avira 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 BADMAIL quarantine.

To prevent this action, use the job Avira Protected Attachment Detection. 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 Avira Scanning 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.

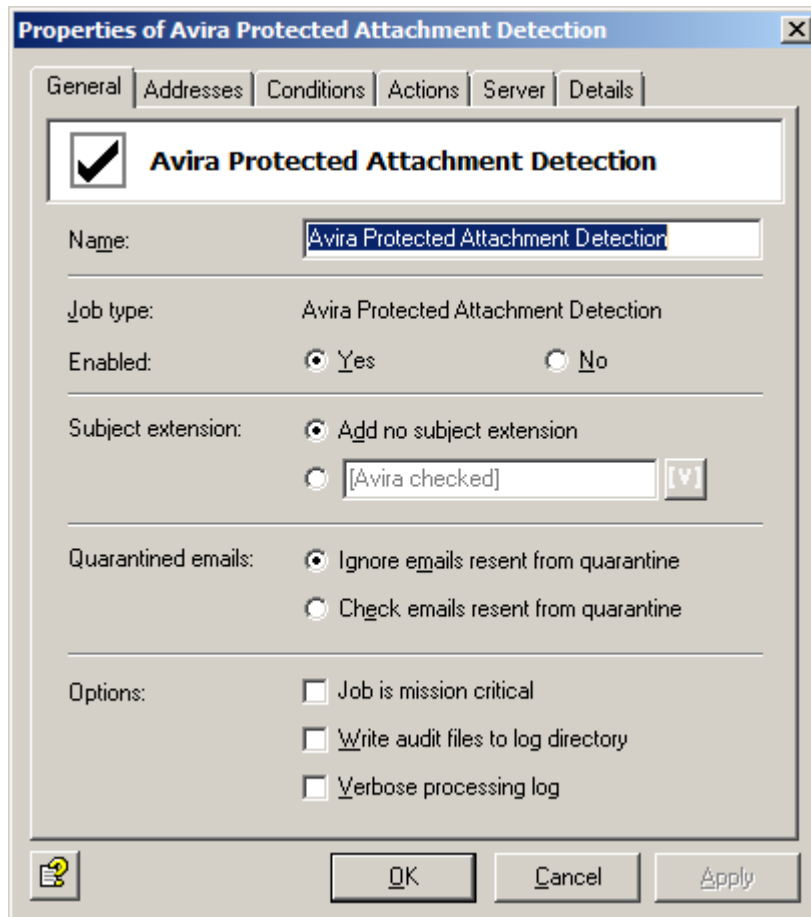
Alternatively, define an action for unscannable objects under **Mail Transport Job > Scanning with Avira Scan Engine > Actions > Define action(s) for the following: Object unscannable**

Warning

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

5.3.1 Setting a Avira Protected Attachment Detection job

1. Right-click **Mail Transport Jobs** and select **New > Avira Protected Attachment Detection**.



Properties of Avira Protected Attachment Detection

General | Addresses | Conditions | Actions | Server | Details

☒ **Avira Protected Attachment Detection**

Name:


Job type: Avira Protected Attachment Detection

Enabled: ☒ Yes ☐ No

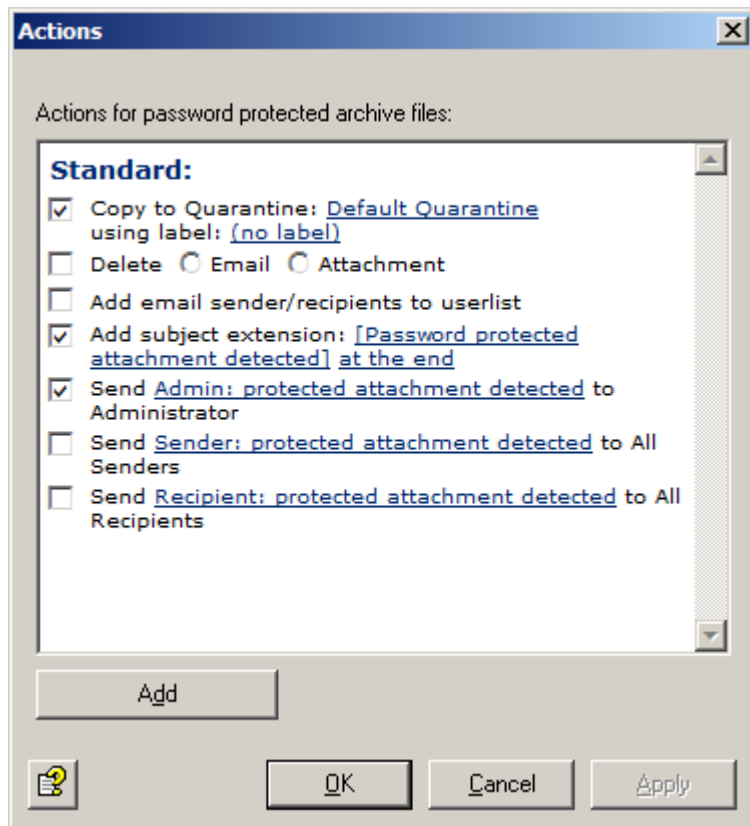
Subject extension: ☒ Add no subject extension
☐ [V]

Quarantined emails: ☒ Ignore emails resent from quarantine
☐ Check emails resent from quarantine

Options: ☐ Job is mission critical
☐ Write audit files to log directory
☐ Verbose processing log



2. Enable the job.
In this example, only the job-specific details are explained.
3. Select the actions.



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, the email is transferred to a subsequent virus scan job and then delivered to the recipient.

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.

5.4 Avira Attachment Filtering jobs

You can use different jobs for blocking various file formats under **Policy Configuration > Job Templates**.

- **Block archives, except ZIP files:** All compressed formats except ZIP files
- **Block suspicious 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.)
- **Block images:** Image formats

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

The result of this check is compared with the prohibited/permited fingerprints under Avira restrictions and is excluded or admitted accordingly. The actions from the job are then executed for rejected files, for example in 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 Avira 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/ blacklist
- Subject extension
- Notify administrator
- Notify sender
- Notify recipient
- Notify other freely selected persons
- Run an external application
- Add Avira tag and value
- Add header field and value
- Redirect email
- Remove header field

5.4.1 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 provider. 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.

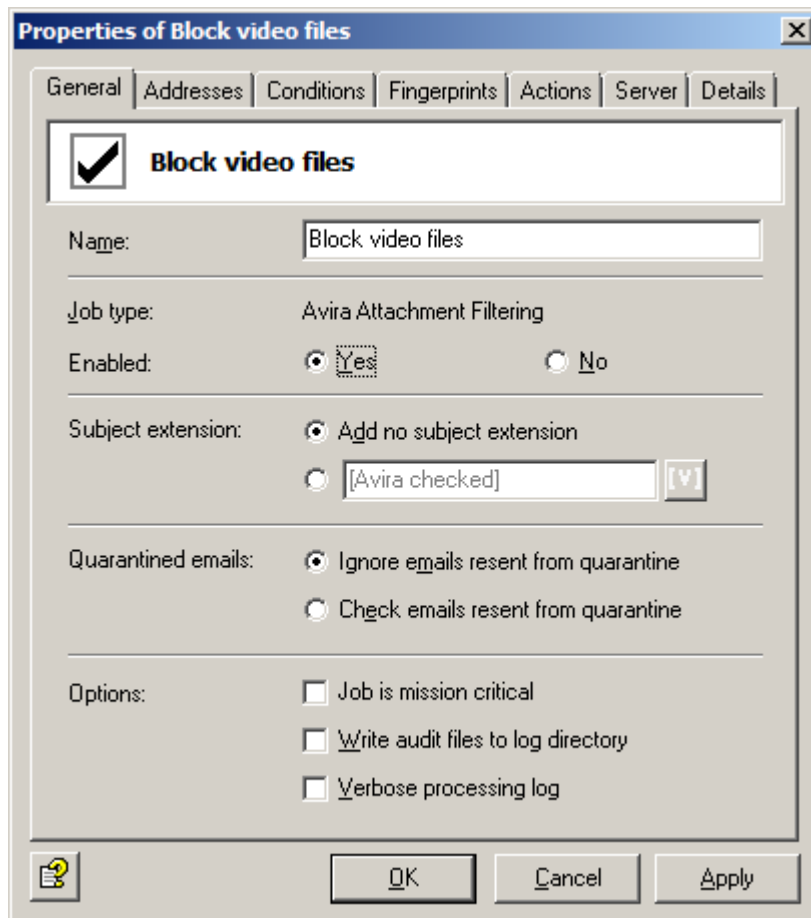
A series of predefined fingerprints for standard files is automatically provided with the program. For help with creating individual fingerprints, please contact the Support team.

5.4.2 Blocking video files

The following example is based on the sample job **Block video files**.

1. Drag and drop the sample job **Block video files** to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

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 shows the job is enabled.



The suggested text for the **Subject extension** is *deactivated*.

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

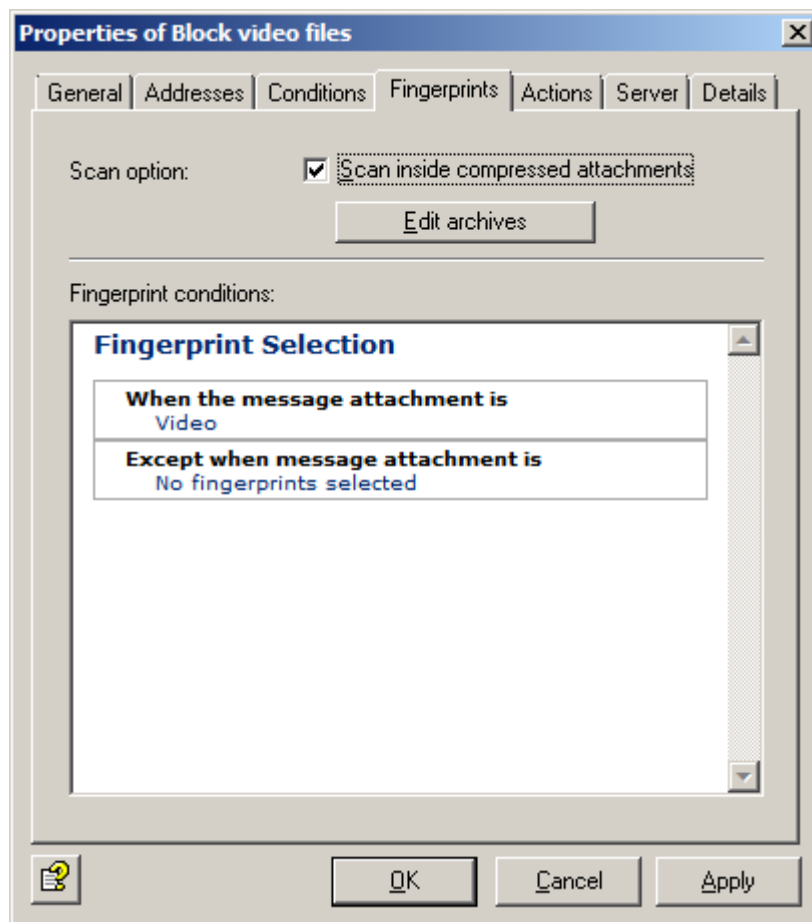
5. Set content conditions.

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

Warning

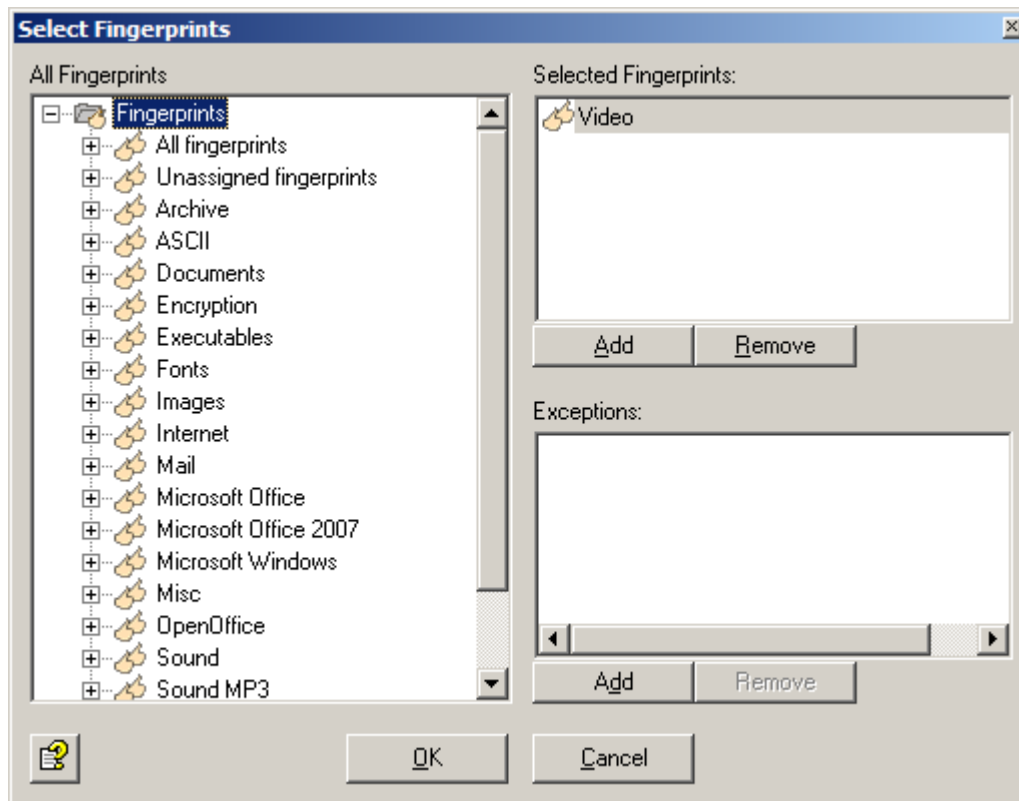
In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (**AND** connector).

6. Select the prohibited fingerprints from the **Fingerprints** tab.



Scan inside 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.

7. To set the fingerprint conditions, click the links **Video** and **No fingerprints selected**.



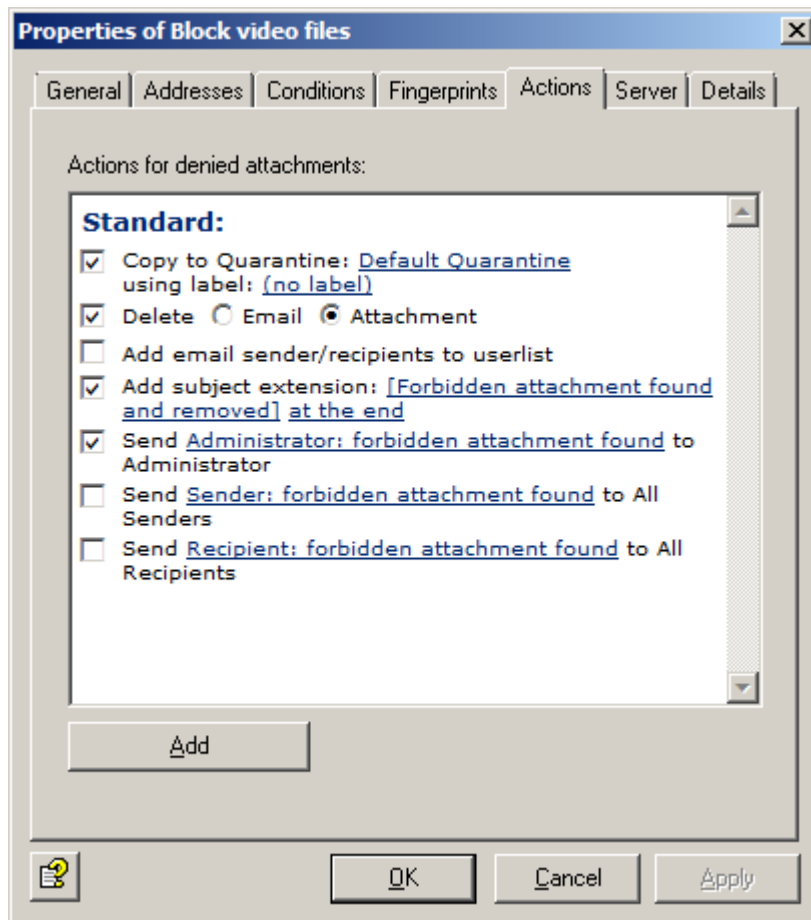
You can select a fingerprint category or an individual fingerprint from a fingerprint list.

8. 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 + (plus) sign.


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.

9. On the **Actions** tab, define the actions 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 administrators notifying them 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.

10. Click the **Add** button if you want to define further actions.
11. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
12. Write a description of the job on the **Details** tab.
13. Click the button **Save Configuration** .

5.5 Avira Email Size Filtering jobs

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

The following actions are possible for an Avira 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/ blacklist
- Notify administrator, sender, recipient
- Notify other freely selected persons
- Run an external application
- Add Avira tag and value
- Add header field and value
- Redirect email
- Remove header field

5.5.1 Restricting email size

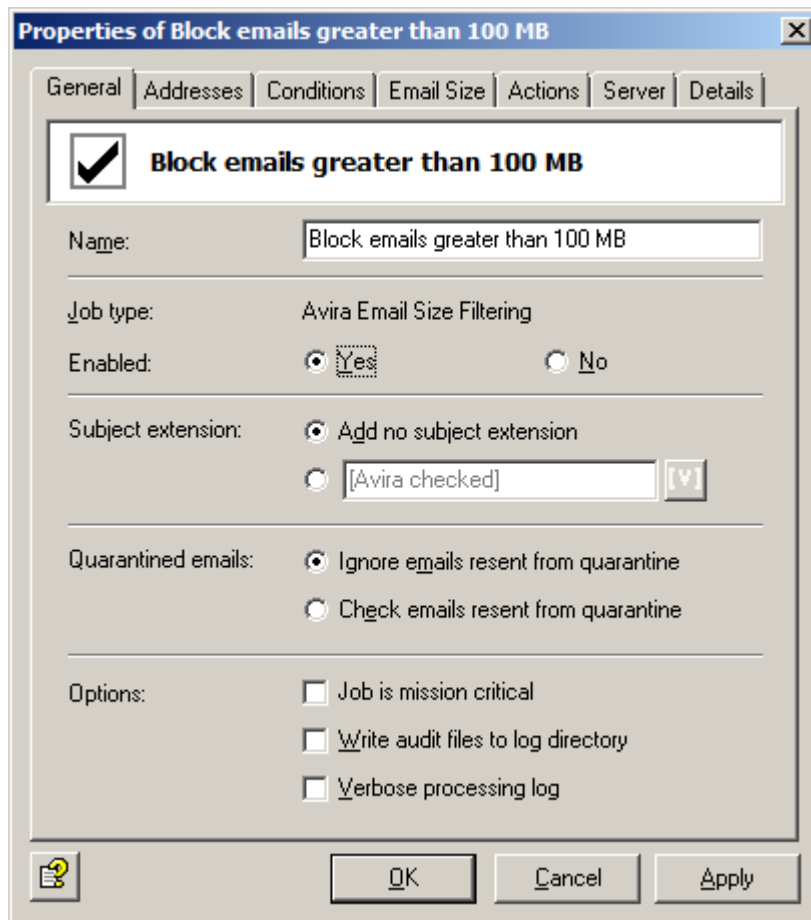
The following example is based on the sample job **Block emails greater than 100 MB**.

Note

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

1. Drag and drop the sample job **Block emails greater than 100 MB** to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

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 shows the job is enabled.



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

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

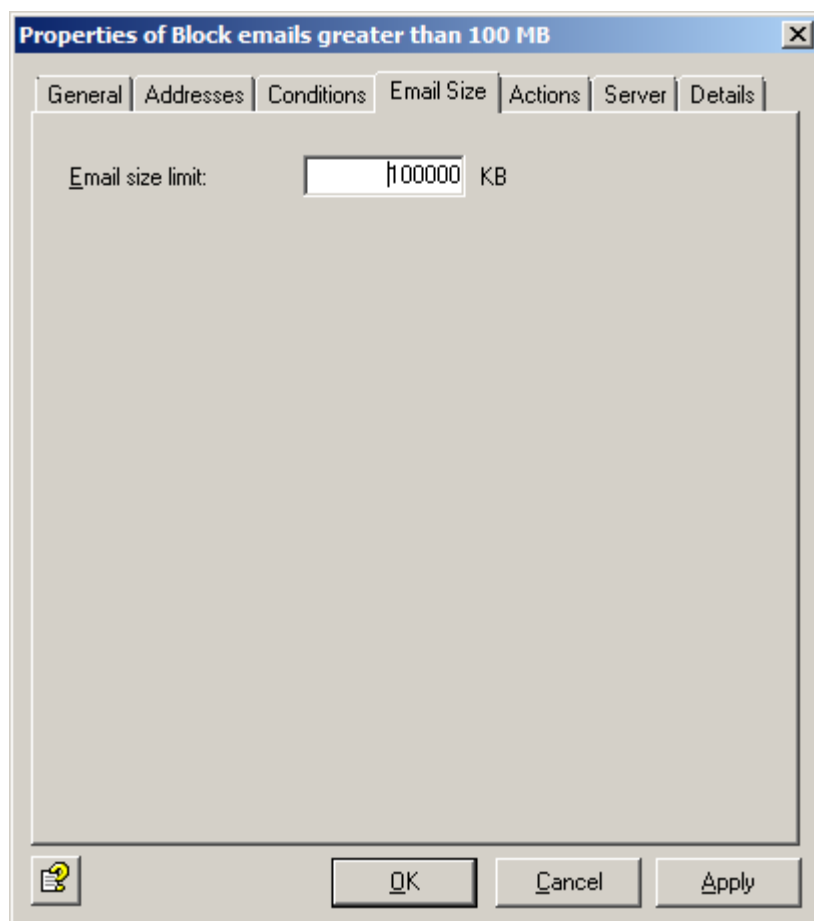
5. Set content conditions.

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

Warning

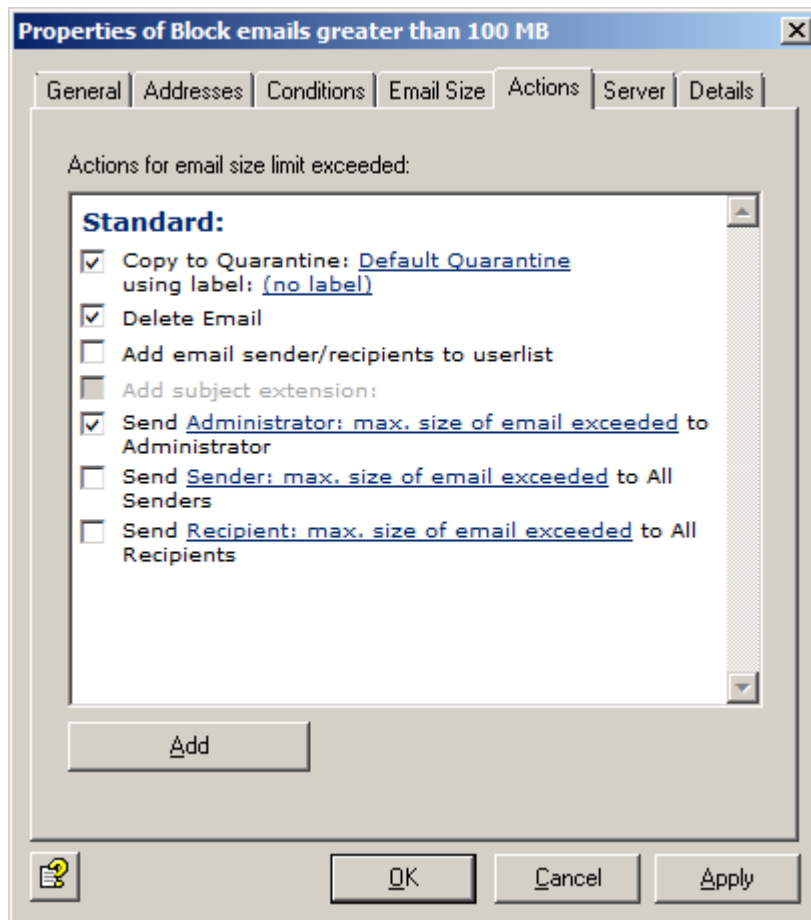
In order for the job to be executed, the content conditions must match the defined address conditions on the **Addresses** tab (**AND** connector).

6. On the **Email Size** tab, define the maximum allowed email size in Kilobytes.




For example: Each incoming and outgoing email may be a maximum of 100,000 Kilobytes in size.

7. On the **Actions** tab, define the actions to be carried out when the job has found an email that is too large.



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 administrators notifying them 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.

8. Click the **Add** button if you want to define further actions.
9. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
10. Write a description of the job on the **Details** tab.
11. Click the button **Save Configuration** .

5.6 Avira Attachment/ Size Filtering jobs

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.

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

You can 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

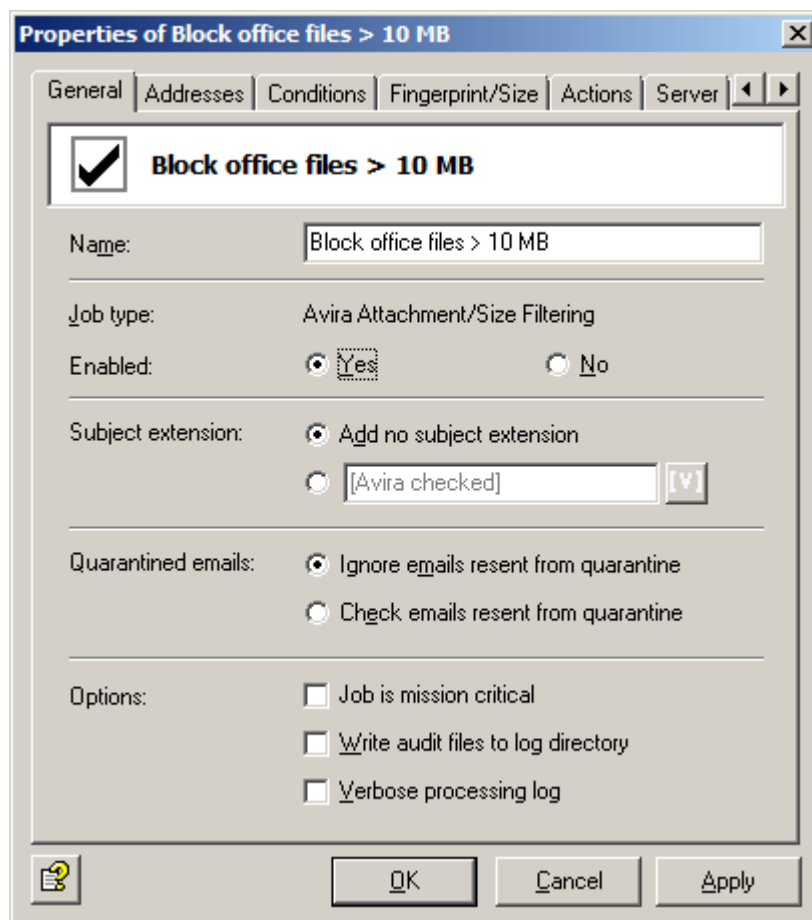
Unlike the scan for email size, the scanning of the attachment format and size only applies to the attachments. The subject line, message text and header data of the email are ignored in this scan.

5.6.1 Blocking Office files

The following example is based on **Block Office Files > 10 MB**.

1. Drag and drop the **Block Office Files > 10 MB** job to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

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 shows the job is enabled.



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

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

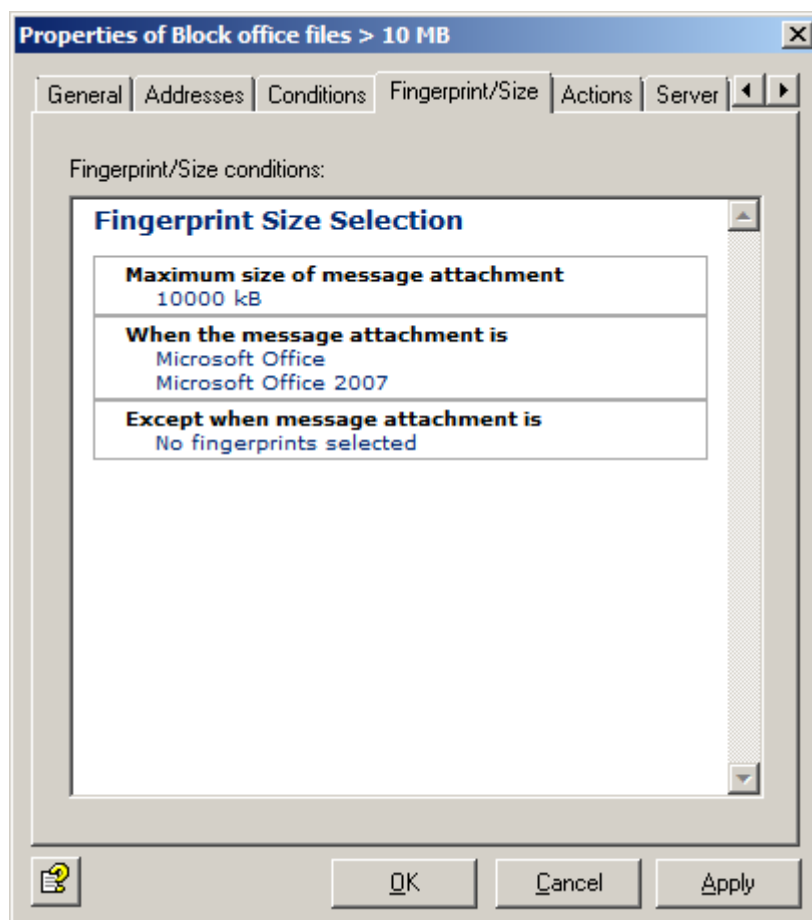
5. Set content conditions.

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).

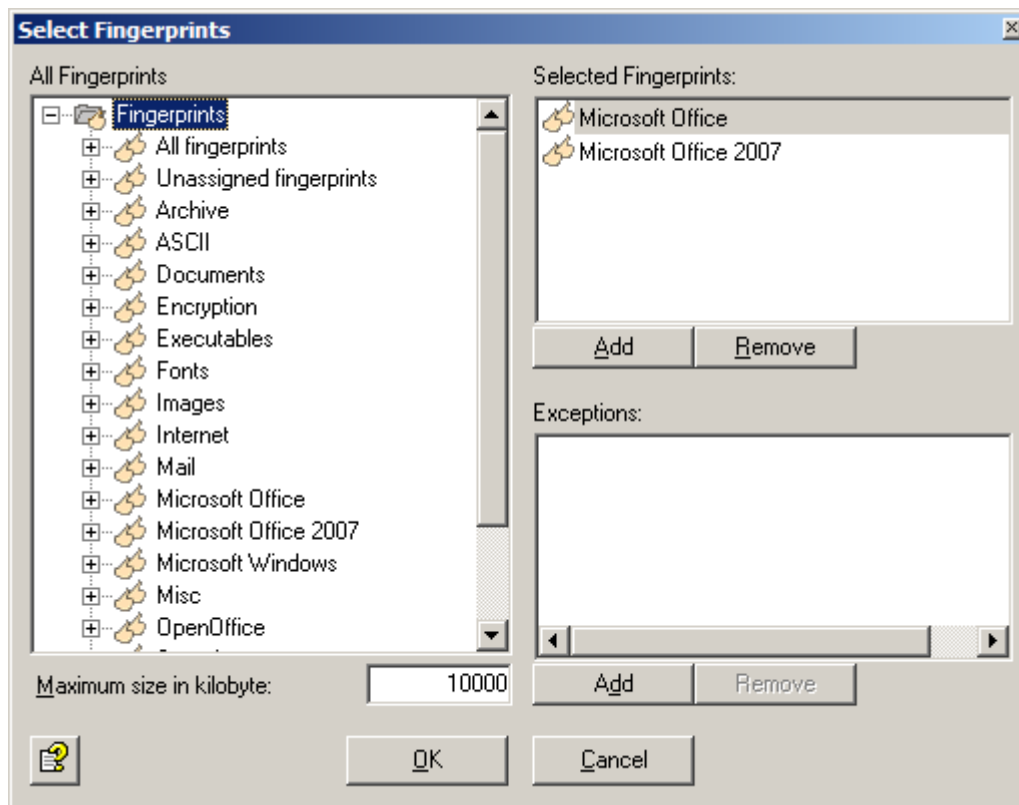
6. Define the maximum allowed email size and the fingerprint format on the **Fingerprint/Size** tab.



Note

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

7. 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.

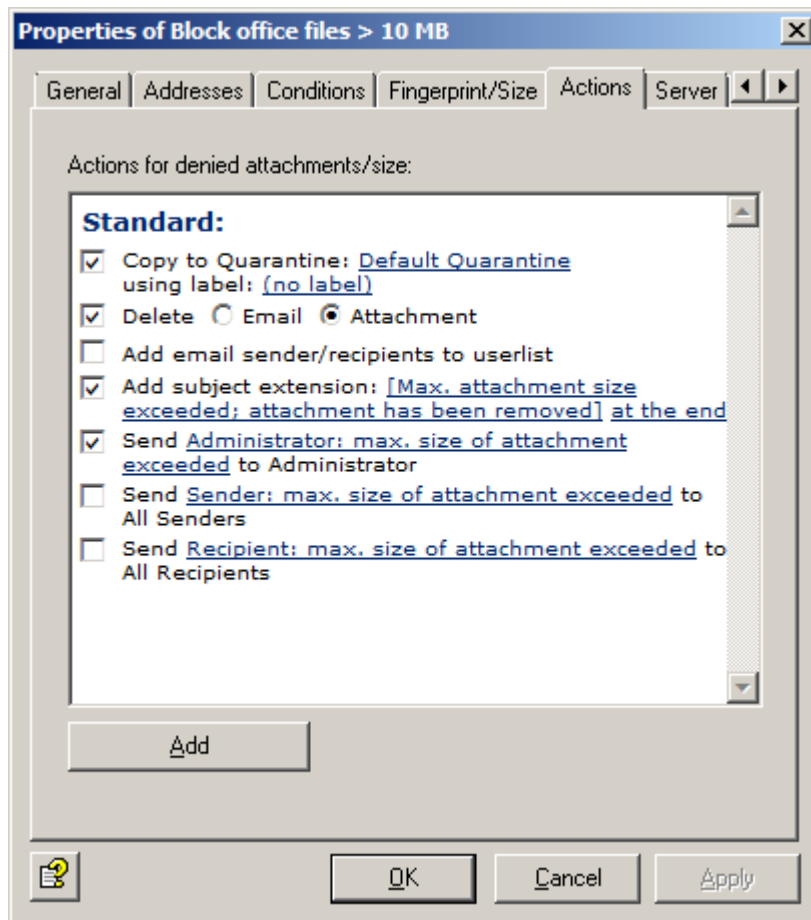


8. Use the **Add** and **Remove** buttons to assign whole categories or individual fingerprints to the list of blocked and/ or permitted fingerprints. Open the category in the left window by double-clicking or by clicking on the + (plus) sign.


Note

You can select a category, such as **Microsoft Office** 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.

9. On the **Actions** tab, define the actions to be carried out 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.

10. Click the **Add** button if you want to define further actions.
11. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
12. Write a description of the job on the **Details** tab.
13. Click the button **Save Configuration** .

Related topics:

[Fingerprints](#) - page 54

6 Avira Email Filter

Avira Email Filter allows you to check the text contained in emails or attachments, classify emails according to content, restrict email addresses in input/ output or limit the number of recipients per email.

Job types

- **Avira Email Filter Address Filtering**: Address filtering job
- **Avira Email Filter Content Filtering**: Content filtering job
- **Avira Email Filter Recipient Limit Filtering**: Filtering the number of recipients
- **Avira Unwanted Email Filtering**: Unwanted Email filtering

Note

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

The following actions are possible for an Avira Email Filter job:

- 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 tag and value
- Add header field and value
- Redirect email
- Remove header field

6.1 Address filtering

Address filtering 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 filtering:

- Mail-enabled Active Directory users
- Mail-enabled Active Directory groups
- Mail-enabled Active Directory contacts
- Freely definable SMTP addresses, including wildcards
- [INTERNAL] = Internal domains as defined in Avira Exchange Security
- [EXTERNAL] = All addresses that are not [INTERNAL]

- "Administrator" = The email addresses defined in Avira Exchange Security 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 filtering:

- **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 filtering is a simple way to filter out known unwanted addresses. The "usual suspects" can be intercepted by the job on the server and are immediately deleted.

Note

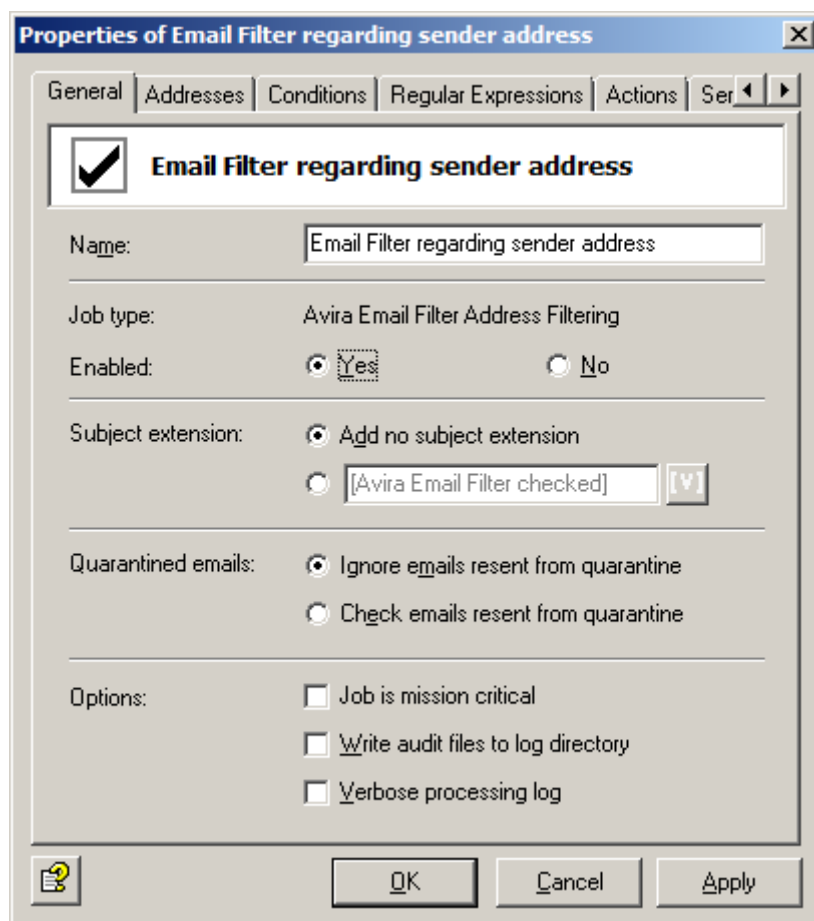
Because the initial restriction corresponds to the job restriction condition in address filtering jobs, a configured **Subject extension** when the condition is met is also added when the initial condition is not met, contrary to the other job types.

6.1.1 Blocking senders or recipients

The following example is based on the sample job **Email Filter regarding sender address**.

1. Drag and drop the sample job **Email Filter regarding sender address** to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

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 shows the job is enabled.



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

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

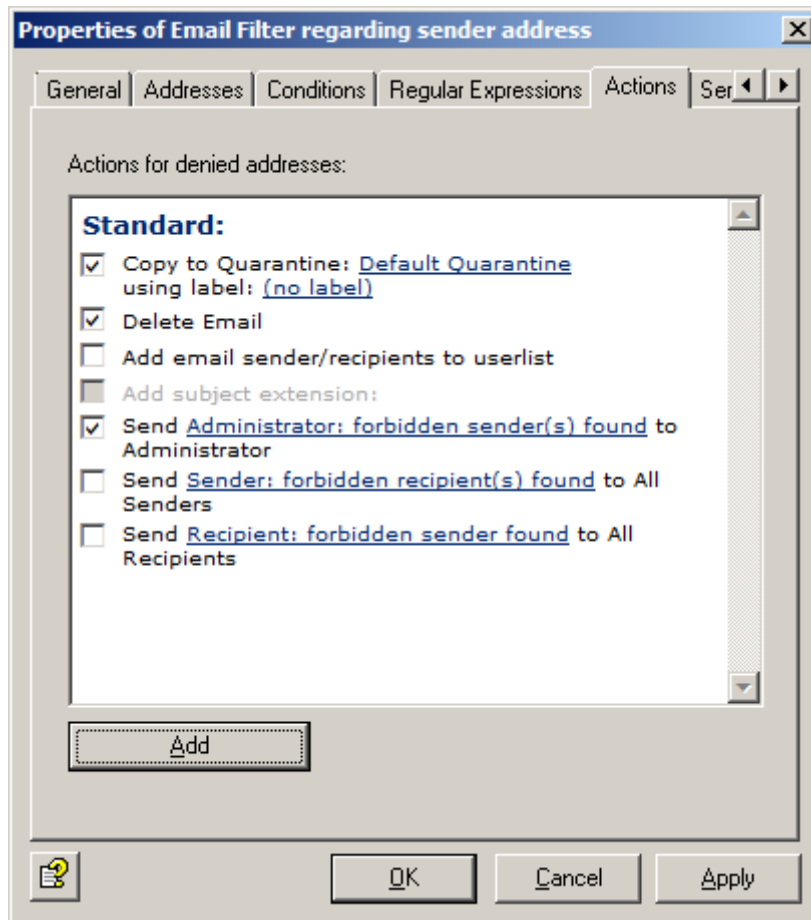
5. Set content conditions.

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).

6. On the **Actions** tab, define the actions to be carried out when the job has found an email with prohibited addresses.



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 administrators notifying them 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.

7. Click the **Add** button if you want to define further actions.
8. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
9. Click the button **Save Configuration** .

Related topics:

[Sending emails from quarantines](#) - page 24

[Mission critical jobs](#) - page 38

[Address lists](#) - page 117

[Job conditions](#) - page 142

[Making settings for an individual Avira Server](#) - page 106

6.2 Content filtering with dictionaries

Avira Email Filter uses predefined dictionaries to scan for unwanted text content.

The following components of the email can be checked:

- Subject
- Message text
- Attachments

The content filtering 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. For example:

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, containing relevant information about the Email Filtering job.

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

You can find different jobs for content filtering 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 emails containing personal records** Scan email for terms from resumes
- **Block emails with "Nigeria connection"** Scan email for special terms in the "Nigerian" emails

6.2.1 Setting up dictionaries

1. Click **Basic Configuration > Utility Settings > Dictionaries**.
To create a new dictionary, right-click **Dictionaries** and select **New > Dictionaries**.

2. Double-click a dictionary to open it in the right-hand window.

3. Assign a name to the dictionary on the **General** tab.

4. Assign a value rating from 1 to 200 for the dictionary.

The 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.

5. Click the input field for words and add the words/ phrases that you want to block.



The individual words/ phrases are separated from one another with a carriage return (**Enter** key).

The following wildcards can be used in dictionaries:

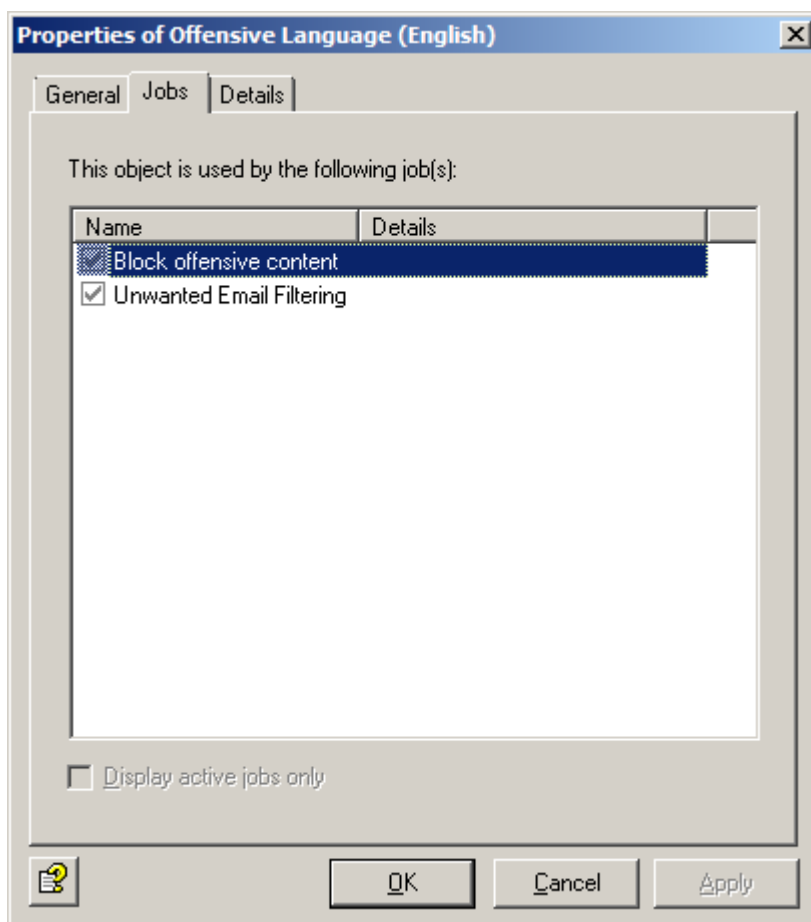
- **Asterisk (*):** The asterisk means that the word/ phrase searched for can also be a part of a bigger word but does not have to be. Examples: *check* finds the individual word "check" but also the words "checkpoint", "intercheck" or "intercheckpoint". check* finds "check" as well as "checkpoint". 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+ finds only "checkpoint". The plus sign must 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 the buttons  for ascending and  for descending.

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



Note

To use a dictionary in a 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 take effect.

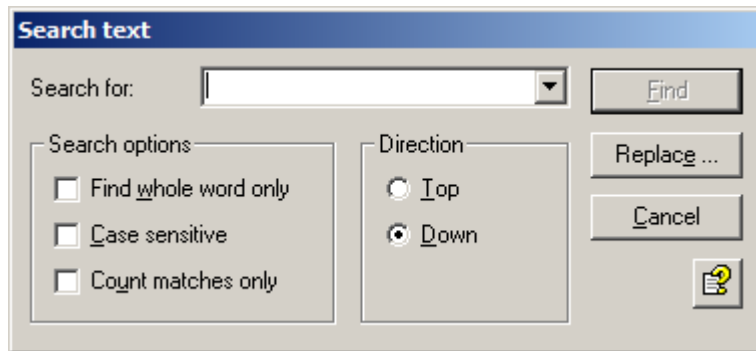
6.2.2 Searching for text in dictionaries

You can search for terms in dictionaries and eventually replace them.

You can also use the **Search text** feature for searching and replacing in your own addresses.

1.

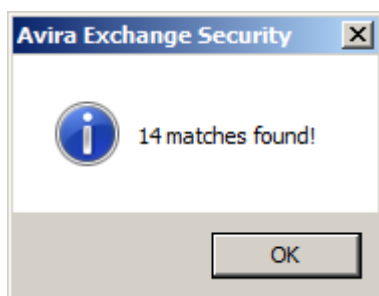
Double-click the dictionary to open it and then click the **Search text** button .



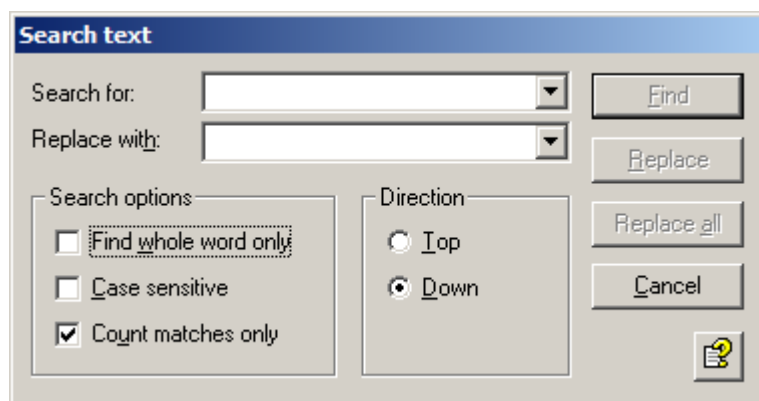
2. Type the text you want to search for and eventually select additional search options.

If you do not specify any additional option, the string will be searched 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 directly highlighted, but counted and the result is output in the form of a message.



3. If you want to replace a specific term with another one, click the **Replace** button and type the text you want to use as replacement.



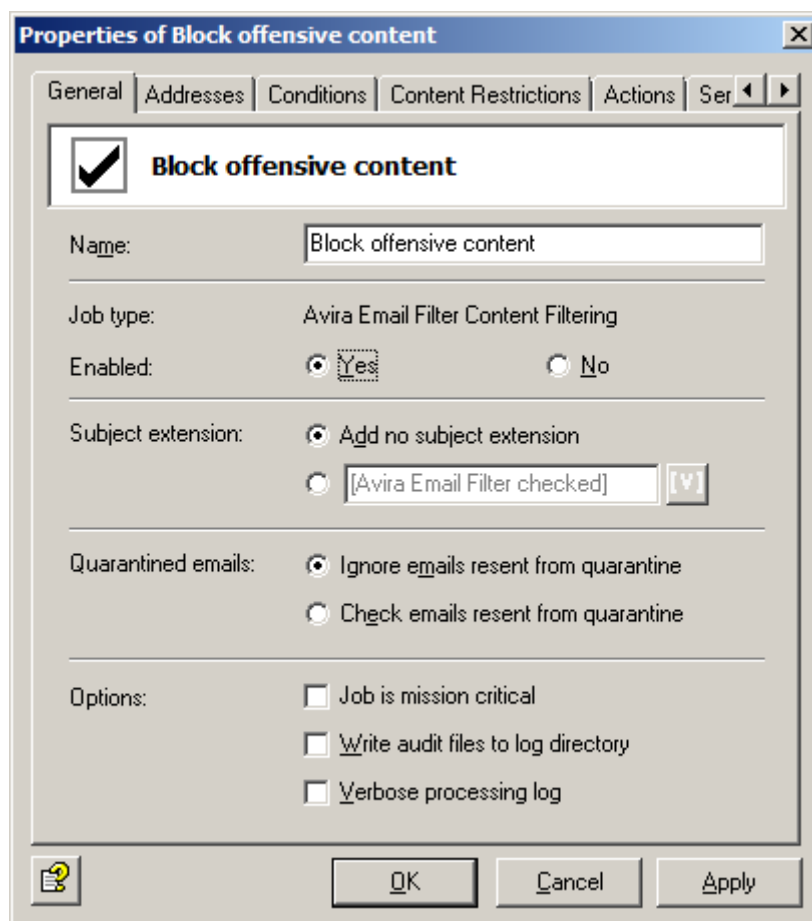
4. Click **Find** to start the search.

6.2.3 Blocking offensive content

The following example is based on the sample job **Block offensive content**.

1. Drag and drop the sample job **Block offensive content** to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

The job is enabled as soon as you save your settings with **OK** and close the job. The checkmark in the job icon immediately shows the job is enabled.



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

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

5. Set content conditions.

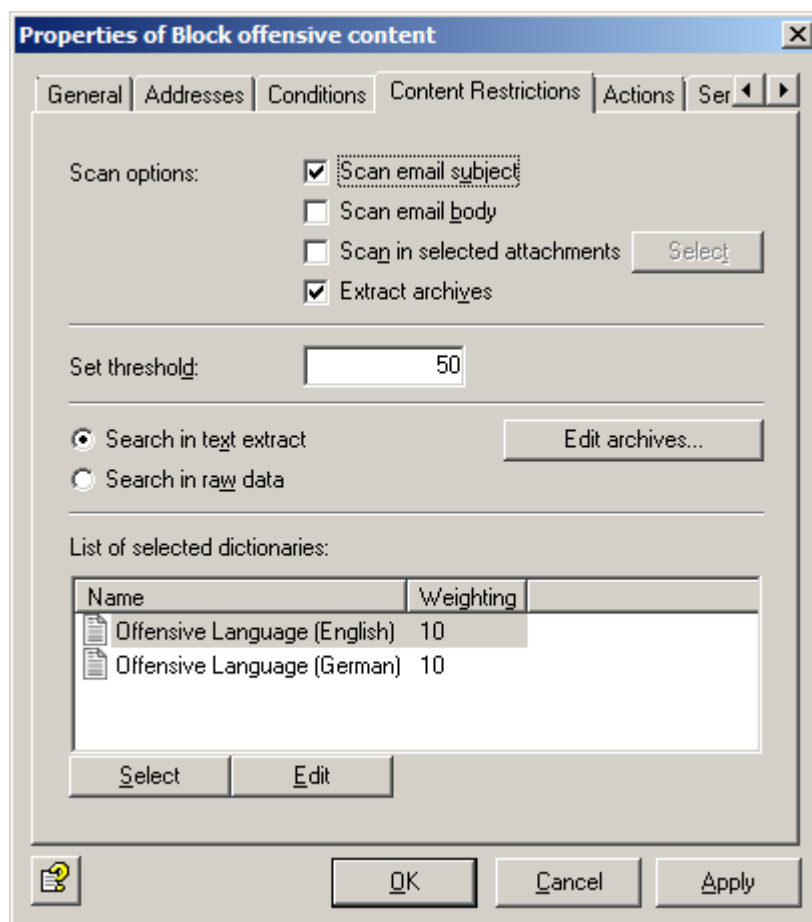
You can use the **Conditions** tab to set the conditions for executing a job.

Warning

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

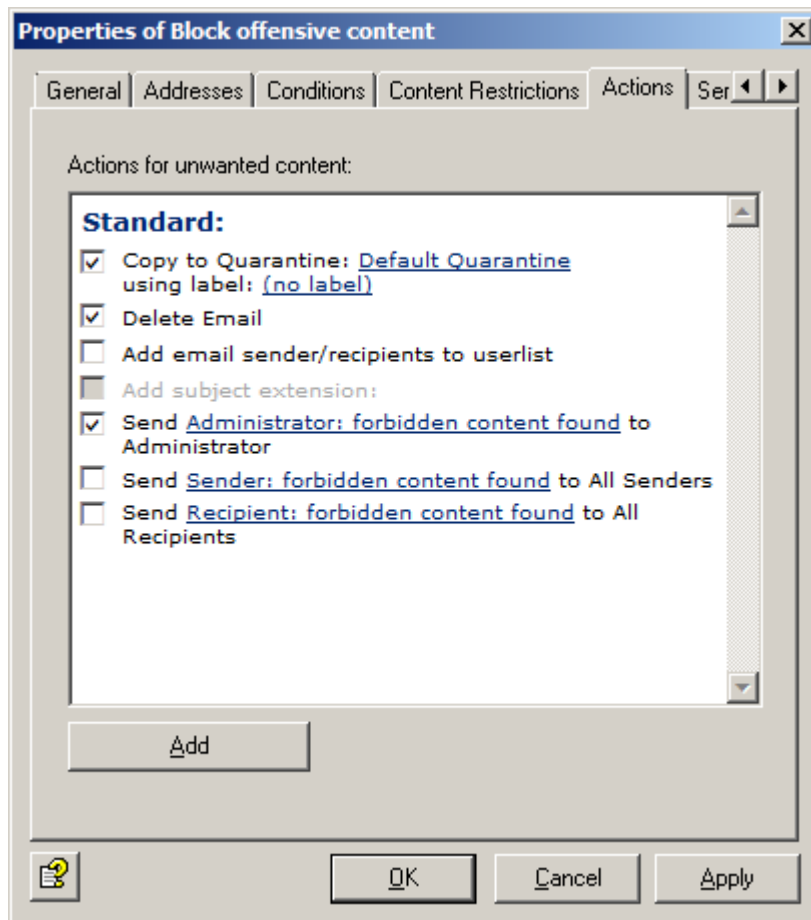
6. Select the dictionaries.

On 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.

7. On the **Actions** tab, define the actions to be carried out when the job has found an email that contains offensive content.



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 administrators notifying them 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.

8. Click the **Add** button if you want to define further actions.
9. Click the button **Save Configuration** .

Related topics:

[Sending emails from quarantines](#) - page 24

[Mission critical jobs](#) - page 38

[Address lists](#) - page 117

[Job conditions](#) - page 142

[Making settings for an individual Avira Server](#) - page 106

6.2.4 Calculation of content filtering threshold

Using one value rating

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 example: 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.

Using two dictionaries

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.

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.

Explanation: 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.

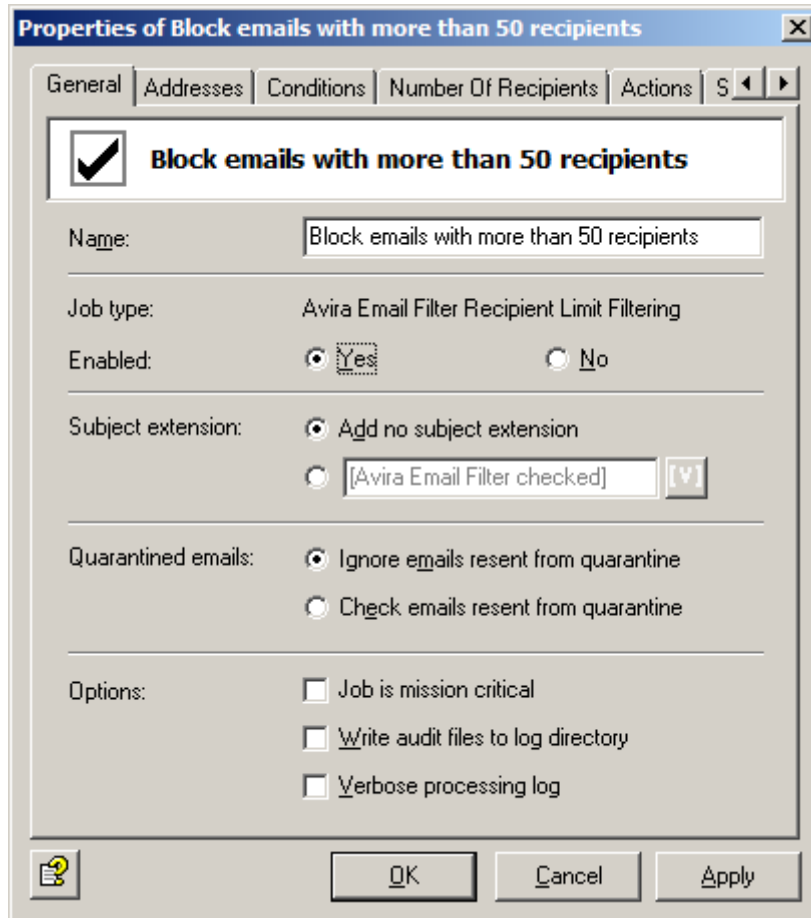
6.3 Limiting the number of recipients

You can 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.

The following example is based on the sample job **Block emails with more than 50 recipients**.

1. Drag and drop the sample job **Block emails with more than 50 recipients** to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

The job is enabled as soon as you save your settings with **OK** and close the job. The checkmark in the job icon immediately shows the job is enabled.



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

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

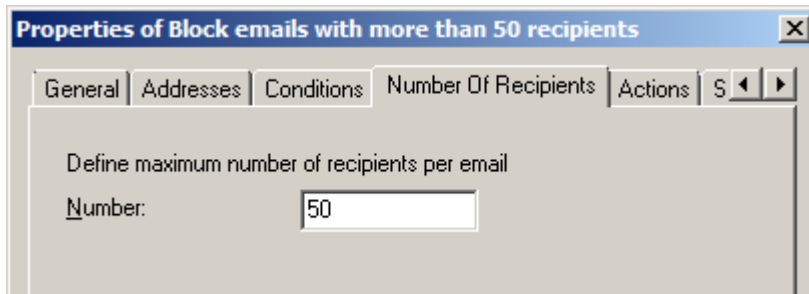
5. Set content conditions.

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).

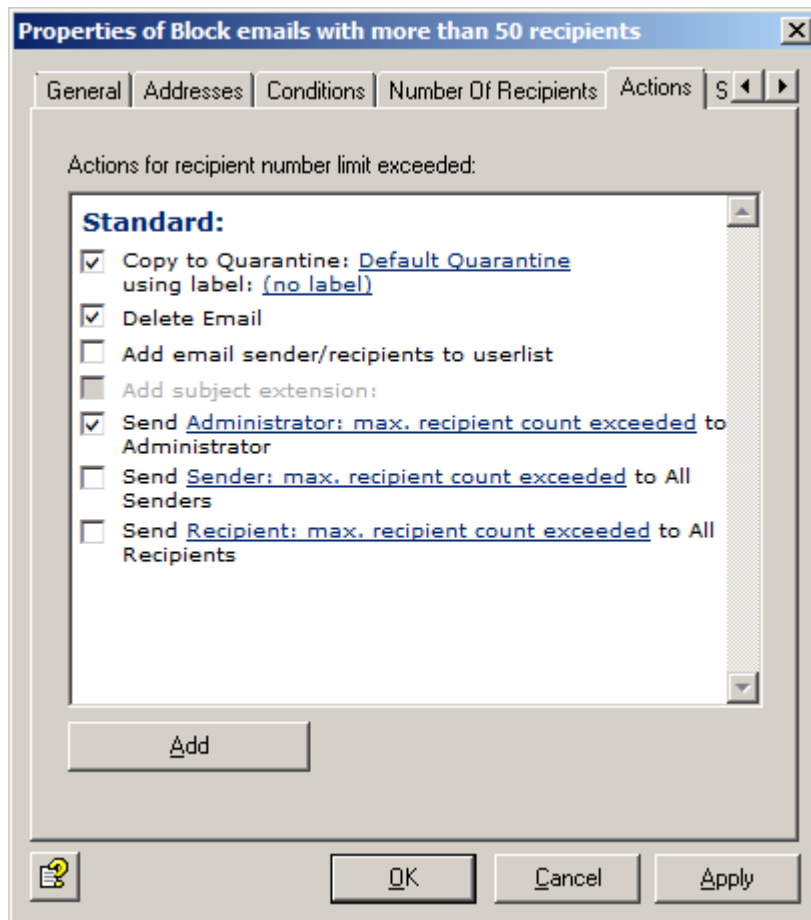
6. Enter the maximum number of recipients allowed per email on the **Number Of Recipients** tab.




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

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.

7. On the **Actions** tab, define the actions to be carried out when the job has found an email with a large number of recipients.



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 administrators notifying them 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.

8. Click the **Add** button if you want to define further actions.
9. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
10. Click the button **Save Configuration** .

6.4 Advanced Email Filter settings

Definite and combined criteria for unwanted email can be set in the email filtering job.

The **definite criteria** imply an immediate decision one way or the other (unwanted content or wanted content) and are immediately assigned the label "Unwanted Content Probability is 0% = **None**" or "Unwanted Content Probability is 100% = **High**".

The **combined criteria** are only applied if the definite criteria were not met. Several analysis mechanisms (criteria tests) are implemented in parallel for actual unwanted content detection with combined criteria and are then "combined" after the email has been analyzed.

A criterion is disabled by clicking in the checkbox.

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**.

In addition, most criteria can also be assigned an individual value for **Minimum** and **Maximum**. These two values relate, for example, to the dictionaries that the criterion uses to scan emails. If the minimum value is not reached, the criterion is ignored for the relevant email in the overall evaluation. If the maximum value is reached, the criterion decides: *"This is unwanted content!"*.

Warning

The message *"This is unwanted content!"* only applies to the specific individual criterion, whose maximum value is achieved by analyzing the email. Because this content 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.

6.4.1 Definite criteria

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 content checking in productive mode. The **definite exclusion criteria** (= Definite Criteria) thus precede the combined criteria so that there is no need to perform further content checks on the email once these criteria are met. The exclusion criteria are used to restrict the unwanted content checks to those emails that cannot already be excluded as unwanted email, for example because of the sender.

Definite no unwanted email criteria

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

Criterion	Description
Emails from these trusted senders (Whitelist)	Whitelist: Addresses of all known senders who are always permitted and who definitively do not send unwanted content. 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 User Whitelist entries	Email addresses contained in the user whitelist are allowed without being scanned for unwanted content.
Emails containing attachments	Emails with file attachments. Most unwanted emails do not have attachments. As an option

Criterion	Description
	you can enter a threshold value here. Example: Minimum value = 2, meaning all emails containing only 2 attachments are delivered without a unwanted content check.
Emails with a minimum size of Kilobyte	Unwanted emails are generally small. Accordingly, large emails are not usually unwanted. You can set a threshold value here, so that larger emails do not get checked for unwanted content.
Emails in TNEF format	TNEF emails. This Exchange-specific format has not been used by spammers to date.
Emails are encrypted and/or signed	Encrypted and/ or signed emails. At present, spammers do not send encrypted or signed emails
Microsoft Exchange "No-Spam" SCL Value	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 unwanted email filtering job as a definite "no spam" criterion.

Related topics:

[Writing the unwanted content result in the Exchange SCL field](#) - page 94

Definite unwanted email criteria

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 unwanted senders. The default configuration already contains a list of known addresses. You can define additional addresses of your own.

Criterion	Description
Emails from User Blacklist entries	Email addresses contained in the user blacklist are blocked without being scanned for unwanted content.
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 unwanted.
Exchange SenderID request returns "FAIL"	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. Email Filter checks the sender ID of the email and evaluates the result "FAIL" as unwanted. 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. See Details:SenderID .
GTUBE test pattern	This function checks for the GTUBE test pattern.

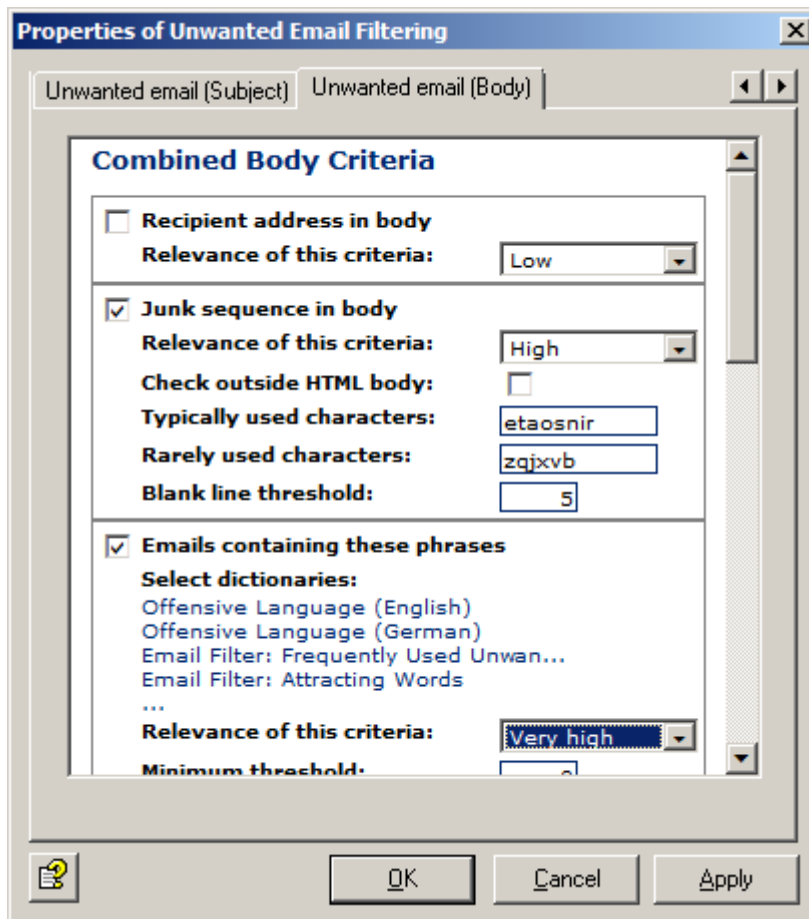
If emails are only to be deleted directly when they are definitely identified as unwanted, you must set the email filter probability for **High** to 100 percent and define a corresponding action. This ensures that only the emails in which the definite criteria (= the black list of character set) have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

6.4.2 Combined criteria

A number of the combined criteria occur frequently in unwanted content in the "gray zone". In itself, each combined criterion is normally just one indicator of whether an email has particular

features that indicate unwanted content. The more criteria with a high value for unwanted content in an email, the more certain it is that this is indeed an unwanted email. 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 unwanted content (= unwanted content probability).

Example of combined criteria



In the combined criterion **Emails containing these phrases** on the **Unwanted email (Body)** tab, you are using the dictionary **Email Filter: Frequently Used Unwanted Phrases**, among others, to scan the message text of all incoming emails for unwanted content. This dictionary is set with a value rating of 5. If a word/ phrase from this dictionary, for example “*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 “unwanted email 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 unwanted email 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” unwanted 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” unwanted email indicator.

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 job Avira Email Filter Content Filtering).

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

Combined information on probability for unwanted content

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 (= unwanted content 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 probability ranges for unwanted content (**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 unwanted content" 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 unwanted content" stamp could also have received the probability for unwanted content **None** or **Low** when calculated together with other criteria and therefore have received the "That is probably not unwanted content" 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 email.

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

For further information on combined criteria, please contact Avira Support.

Combined no unwanted content criterion

Criterion	Description
Emails containing these phrases	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 unwanted content detection products are included here and often only one unwanted content detection feature of each product is used. The specific disadvantages of the individual products are eliminated through combination with other criteria in the Avira Unwanted Email Filtering job.

Criterion	Description
Exchange SCL value	The Intelligent Message Filter (IMF) determines the probability of an email being unwanted content. The result of this

Criterion	Description
	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 unwanted content. With this criterion, the SCL value of an email can be included in the unwanted content evaluation of Avira Email Filter. For further information, see also http://technet.microsoft.com/en-us/library/bb124426%28v=EXCHG.65%29.aspx

Related topics:

[Definite no unwanted email criteria](#) - page 82

[Writing the unwanted content result in the Exchange SCL field](#) - page 94

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.
Digits in sender address(es)	Checks whether one of the sender addresses (SMTP or email header) contains numbers.
Number of recipients per email	Checks the number of recipients for an email.
Known X-Mailer	Checks whether the X-Mailer entry in the email is a known unwanted content client.
Known unwanted content results	Takes the result of a previous unwanted content analysis for the classification of emails as unwanted content or no unwanted content into account. The result (number of unwanted content indicators found) is written to the X-header of the email. Avira Exchange Security evaluates the X-header and writes the number of unwanted content indicators to the criterion. The evaluation takes place using the minimum/ maximum number of possible

Criterion	Description
	unwanted content indicators. The result may originate from an external system or may have been calculated from the Avira Exchange Security of another server.

Combined subject criteria

Criterion	Description
Missing subject	Checks whether the subject field exists and contains an entry.
Recipient address in subject	Checks whether the subject of the email contains the part of the recipient address before the @.
Junk sequence in subject	Checks whether long strings of hidden characters (spaces) and meaningless junk strings occur in the subject of the email.
Emails containing these phrases	Checks whether words from the typical unwanted content vocabulary are found in the subject field of the email.
Emails containing these concealed words	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 body	Checks whether the message text of the email contains the part of the recipient address before the @.
Junk sequence in body	Checks whether long strings of hidden characters and meaningless junk strings occur in the message text of the email.
Emails containing these phrases	Checks whether words from the typical unwanted content vocabulary are found in the message text of the email.
Emails containing these concealed words	Checks whether disguised words from the specified dictionary (dictionaries) are found in the message text of the email.

Criterion	Description
Emails containing suspicious HTML code	Checks whether HTML constructs are found in the message text of the email.
Emails containing suspicious HTML links	Checks whether unwanted links are found in the message text of the email.
Many 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	Check for unwanted content that is transported by means of embedded images (internal reference to attachments). For example, in configurations without Avira Email Filter, it is possible for all emails with embedded images to be considered unwanted content if embedded images are not a component of the regular email communication of the operational environment.

6.4.3 Advanced Email Filtering

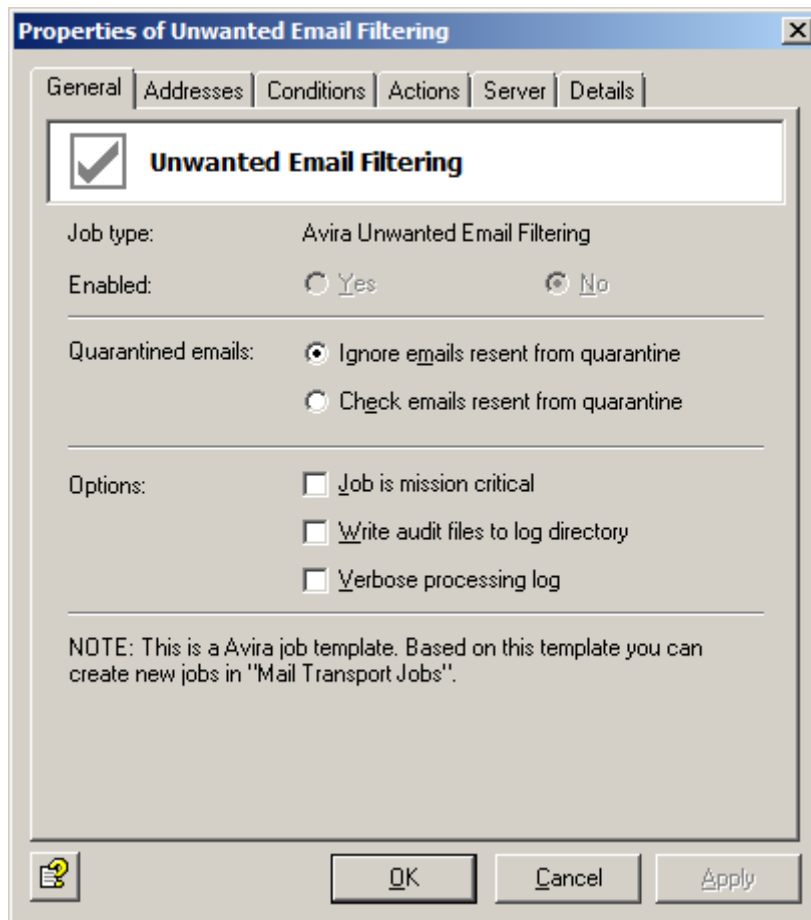
Warning

For your own security, the job **Filtering Unwanted Content with Avira Email Filter** is preconfigured and activated by default. This job can be found under **Mail Transport Jobs**.

You can also use the job **Advanced Email Filtering**, which examines emails on the basis of special email filtering instructions.

1. Drag and drop the sample job **Advanced Email Filtering** to the **Mail Transport Jobs** folder and open it there with a double-click.
2. Assign a name to the job on the **General** tab.
3. Click **Yes** to enable the job and make further general settings.

The job is enabled as soon as you save your settings with **OK** and close the job. The checkmark in the job icon immediately shows the job is enabled.



This job contains the **Subject extension** option on the **Actions** tab.

The scanning job can also double-check processed emails sent from quarantine: **Check emails resent from quarantine**.

Note

The Send option in **Send from Quarantine** applies to all jobs and has priority. Accordingly, if you resend an email with the Quarantine Send option **Deliver the email bypassing any Avira jobs on this server**, the email 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 Avira jobs on this server**.

4. Set 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.

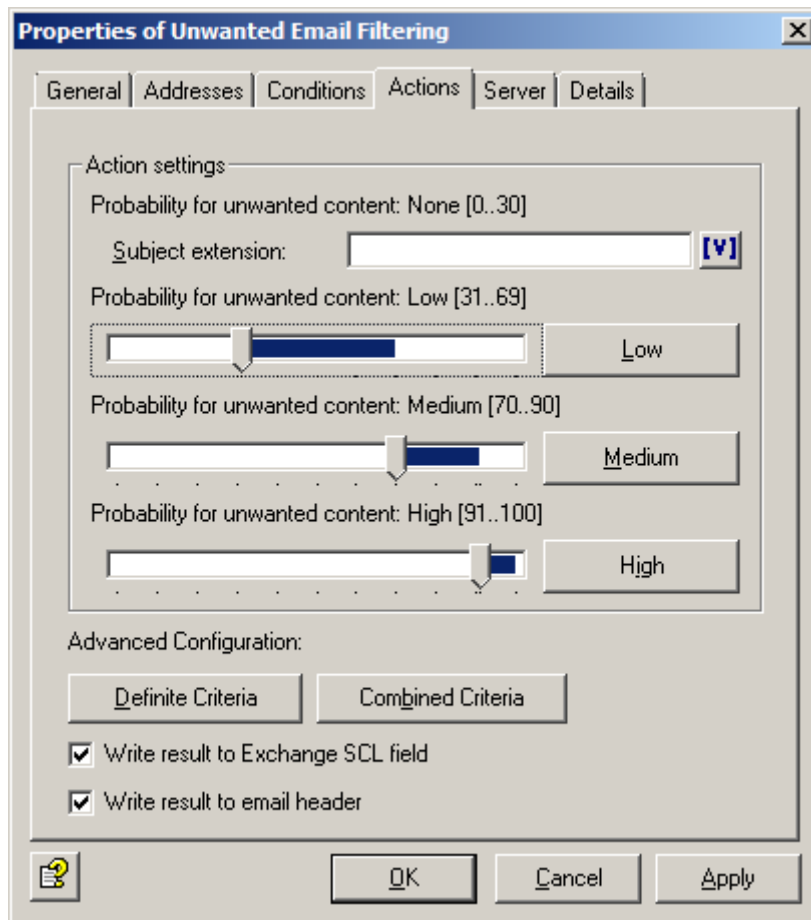
5. Set content conditions.

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).


6. On the **Actions** tab, define the unwanted content probabilities and what is to be done with any detected unwanted content.



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.

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 much unwanted content as possible in the **Email Filter: High** quarantine
- As many ham emails as possible in the **Email Filter: Low** quarantine
- As few emails as possible in **Email Filter: Medium**
- **Unwanted Content Probability: None** (example values = 0-30): Normally, no action is carried out in this range. Click the **[v]** button to set a **Subject extension**, such as *Avira checked*.
- **Unwanted Content Probability: Low** (example values = 31-69): Click the **Low** button to set the actions.
- **Unwanted Content Probability: Medium** (example values = 70-90): Click the **Medium** button to set the actions.
- **Unwanted Probability: High** (example values = 91-100): Click the **High** button to set the actions.
- If you want to adjust the definite unwanted content criteria, click **Definite Criteria**.
- If you want to adjust the combined unwanted content criteria, click **Combined Criteria**.

- **Write unwanted content result in the Exchange SCL field**
 - **Write unwanted content value in mail header field**
7. On the **Servers** tab, click **Select** and choose a server from the list.
The server must be configured correctly in order to appear in the list.
8. Click the button **Save Configuration** .

Related topics:

[Sending emails from quarantines](#) - page 24

[Mission critical jobs](#) - page 38

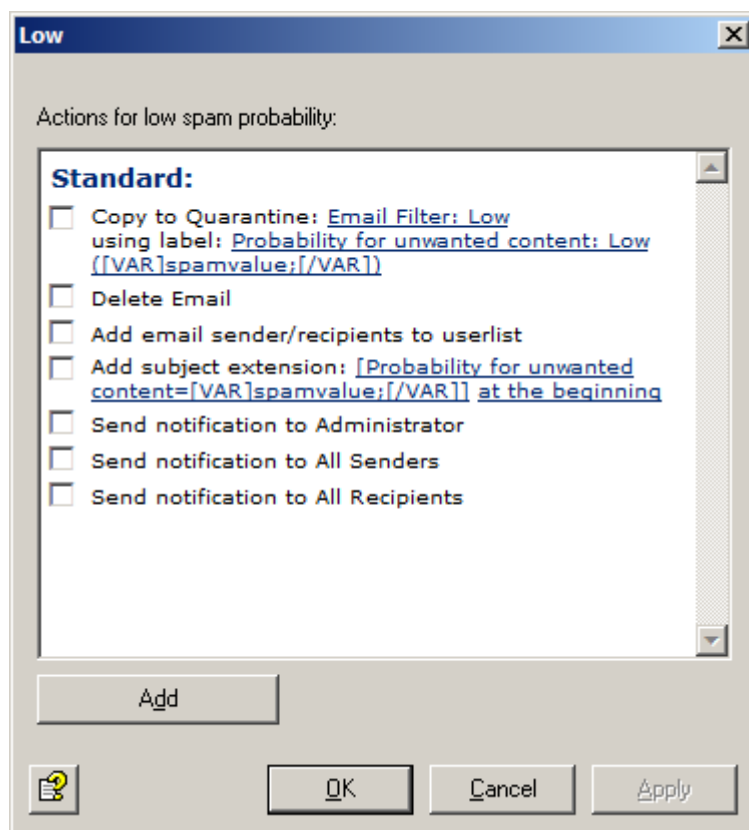
[Address lists](#) - page 117

[Job conditions](#) - page 142

[Making settings for an individual Avira Server](#) - page 106

Actions for low probability

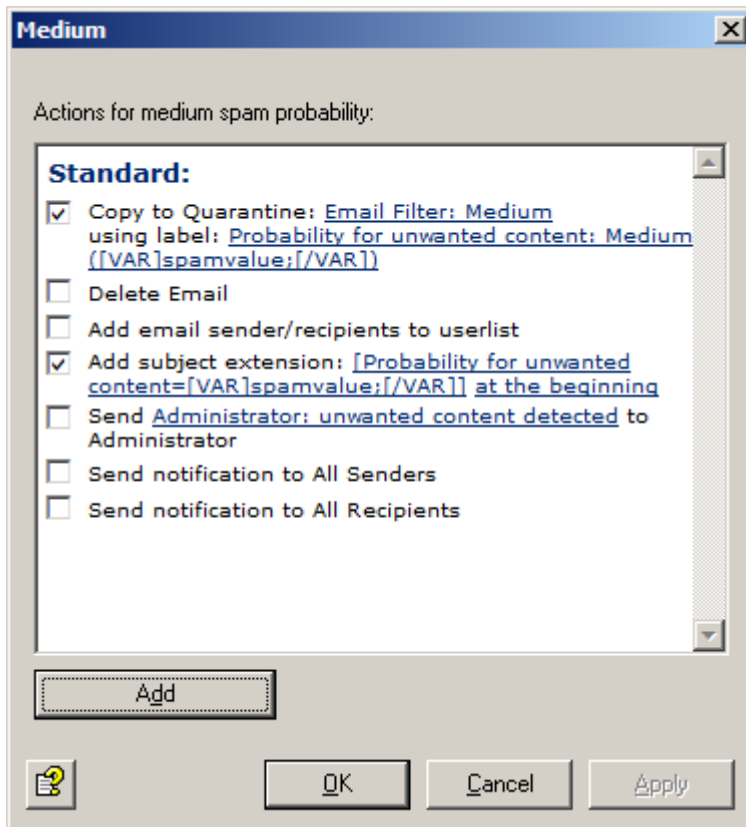
The only enabled action is to add the unwanted content probability to the subject line. In default configuration, there is no action.



Actions for medium probability

The higher you set the probability value, the more certain the recipient can be that this email is not very important. Medium unwanted content probability is intended for emails that may or may not be unwanted. Lower values in this setting mean that a medium probability can be assumed

for unwanted emails if only a few criteria have detected massive unwanted content indicators or numerous criteria have detected a small number of unwanted content indicators.



A copy of the email will be placed in quarantine and the administrator will be notified. In default configuration, there is no notification sent to the administrator.

The original mail is delivered to the recipient. In default configuration, the original mail is not delivered.

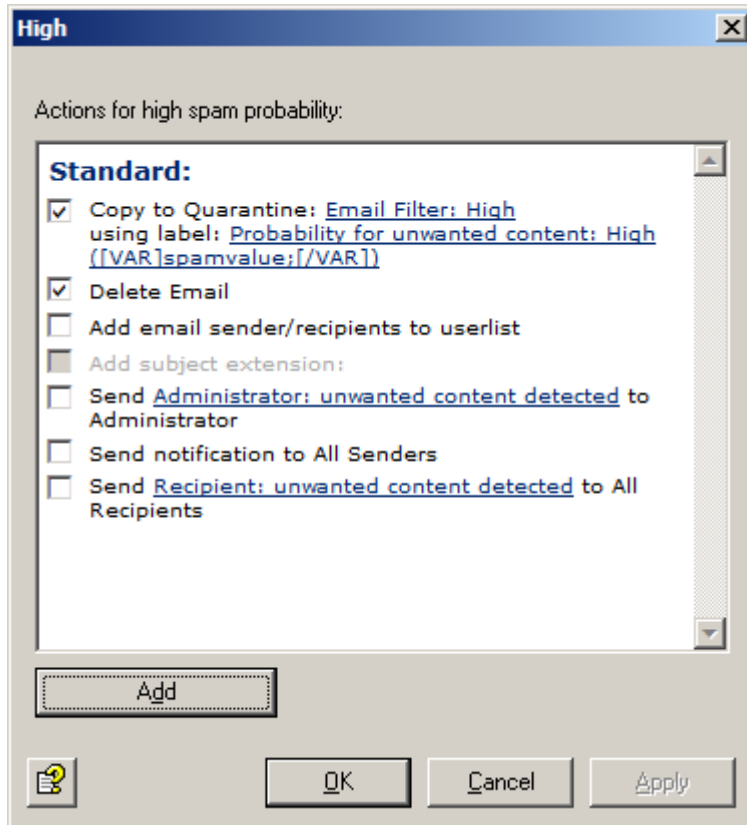
The subject extension notifies the recipient of the probability of unwanted content in this email (for example *Unwanted Content Probability = 75*).

It is recommended that these emails should be gathered in a separate quarantine area (**Email filter: Medium**) and that it should be left up to the users to decide what to do with these emails.

Users can be notified of the unwanted emails 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. The configured subject extension indicating the unwanted content probability value enables every user to decide how this email will be handled, possibly even with a filter in Outlook.

Actions for high probability

High probability for unwanted content is intended for emails that really are unwanted and hence should not be delivered.



The original email 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 unwanted emails, no notifications are sent to the administrator.

Writing the unwanted content result in the Exchange SCL field

Microsoft supplies its own spam filter, starting with Service Pack 1 for Exchange 2003 and Outlook 2003. This Intelligent Message Filter (IMF) determines the probability that an email is unwanted content.

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 unwanted content.

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 probability for unwanted content value for the Email filtering job as an SCL result.

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.

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 the redirection of emails to the junk mail folder. For more information about the Exchange SCL field, see <http://technet.microsoft.com/en-us/library/bb124426%28v=EXCHG.65%29.aspx>

Writing the Email Filter result in the email header

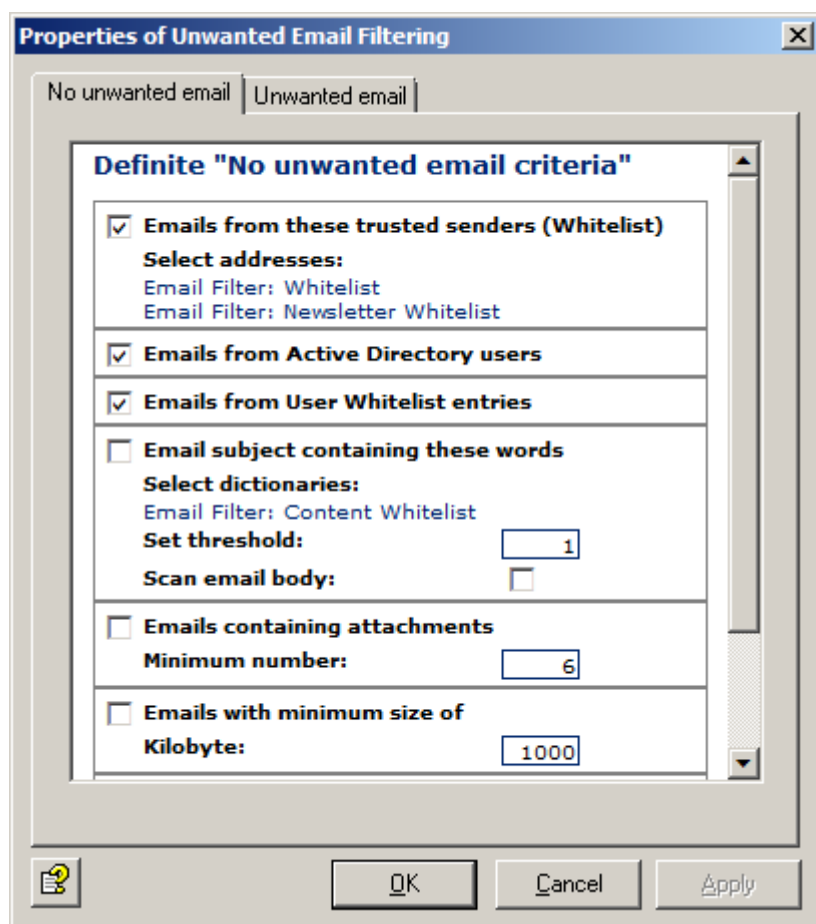
The email filter value is added to the email header for all three probabilities (Low, Medium and High).

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.

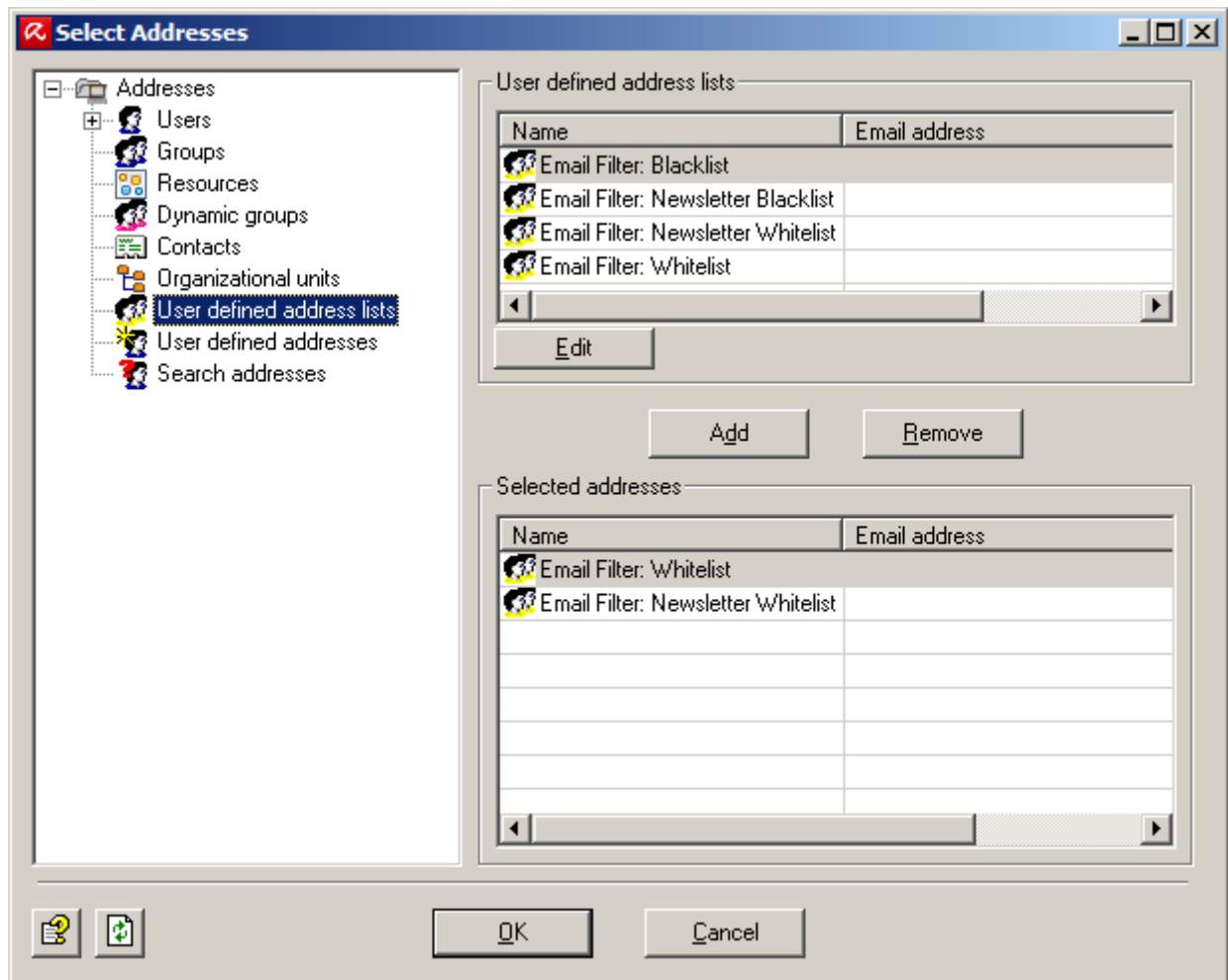
You can also define the result separately for each email filter probability by selecting **Add > Add X header field** on the **Actions** tab. In this case the result is not converted into a series of stars but is output directly as a value.

Setting definite No-Unwanted Email criteria

You should keep the whitelists up to date.



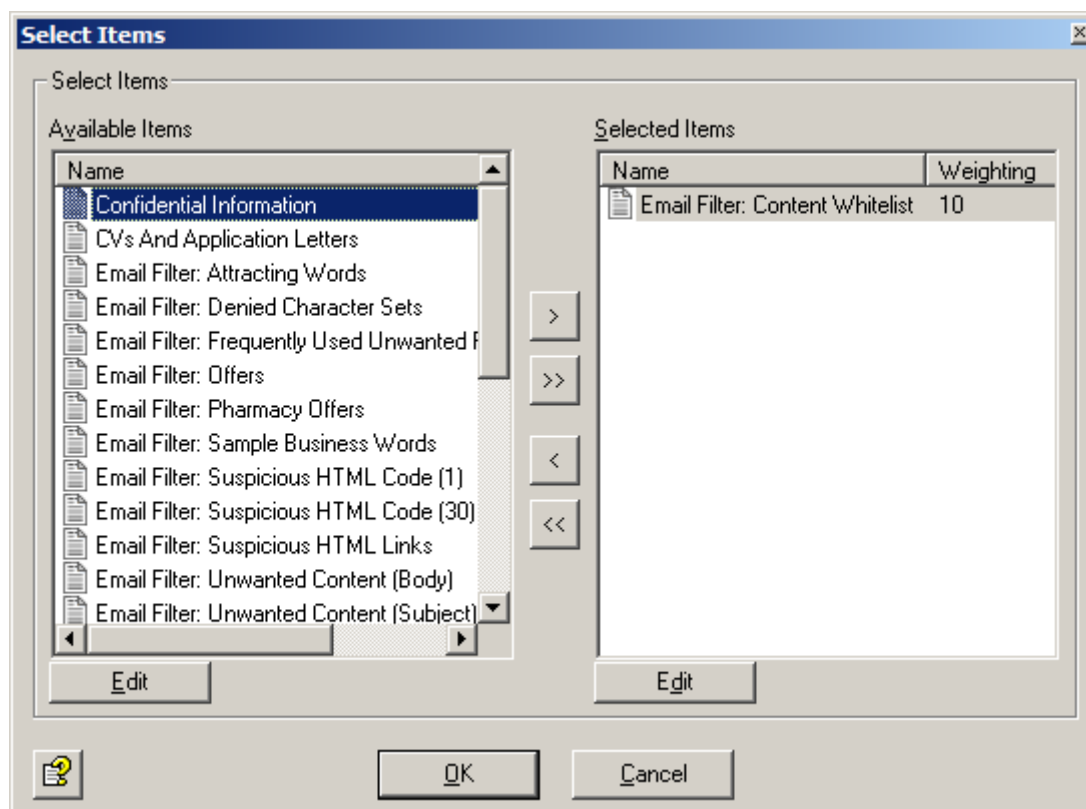
1. If you wish to allow emails from particular senders, click the links **Email Filter: Whitelist** and **Email Filter: Newsletter Whitelist** under the **Emails from these trusted senders (Whitelist)** criterion.



2. Select the addresses or specify your own email addresses which are always to be permitted as senders, then click **OK**.

The * (asterisk) and ? (question mark) symbols can be used as wildcards. This means that you can specify domains in the form *.domain.com.

3. If you wish to modify the dictionaries under the criterion **Email subject containing these words** on the **No unwanted email** tab, click the link **Email Filter: Whitelist**.



- Use the arrow keys to add and remove dictionaries in the list.
- Use the double arrows to add or remove all marked dictionaries.
- Click **Edit** to modify the properties of a selected dictionary.

Related topics:

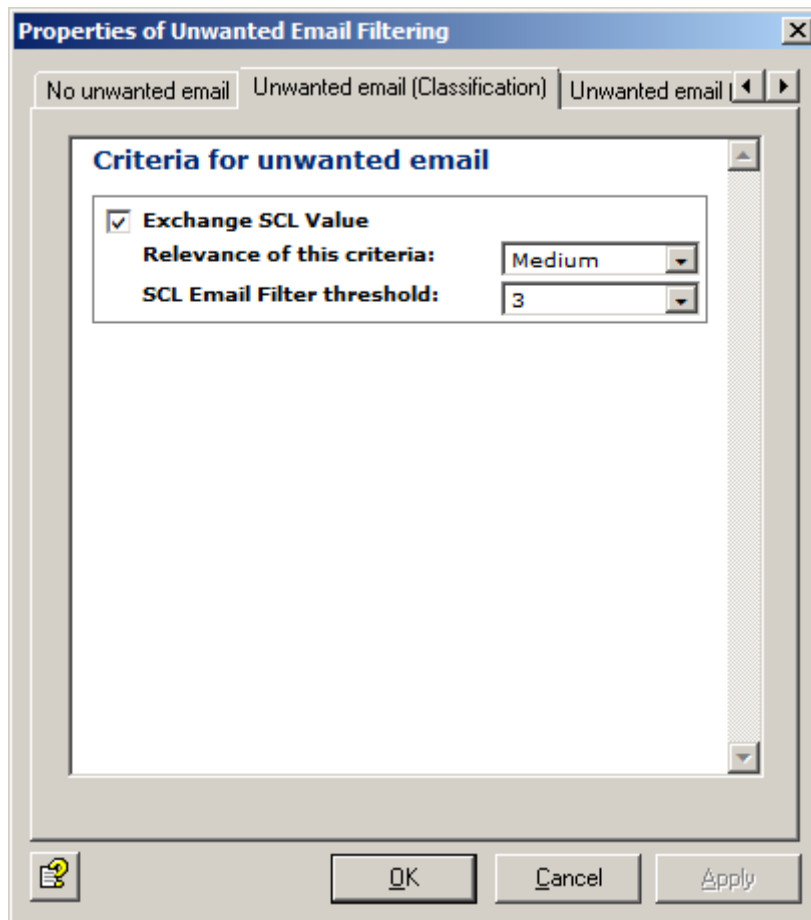
[Definite no unwanted email criteria](#) - page 82

[Setting up dictionaries](#) - page 71

Setting Combined Unwanted Email criteria

It is recommended to keep the default settings of the Advanced Email Filtering job.

1. If you want to activate the advanced email filtering, on the **Actions** tab click **Combined criteria > Unwanted email (Classification)** and enable the **Avira Email Filter results** criterion.



2. Select the value for **Relevance of this criteria**.

The value ranges from **Low** to **Very high**.

The values for the relevance and the coefficient are multiplied and together yield the result for this criterion.

3. Click **OK**.

6.4.4 Configuring Email Filter manually

If you do not want to use the job Avira Unwanted Email Filtering, it is recommended that you set up the following sequence in the job process to ensure an effective email filter configuration.

The jobs must be executed in the correct processing order so that the filtering is carried out as effectively as possible and the performance is optimized.

1. Set address filtering for known unwanted email addresses.
2. Set subject line filtering for text and for conspicuous features in the formatting, for example periods or spaces.

See **Basic Configuration > Dictionaries > Email Filter: Unwanted Content (Subject)**.

3. Set message text filtering for unwanted content links (also for redirections and click trackers).

See **Basic Configuration > Dictionaries > Email Filter: Suspicious HTML Links**.

4. Set message text filtering for unwanted text and known typical conspicuous features such as HTML comments in an HTML email text.

See **Basic Configuration > Dictionaries > HTML Unwanted Content Detector**.

7 Detailed configuration

7.1 Basic Configuration

The **Basic Configuration** is where general settings and the most important basic settings are made for the modules.

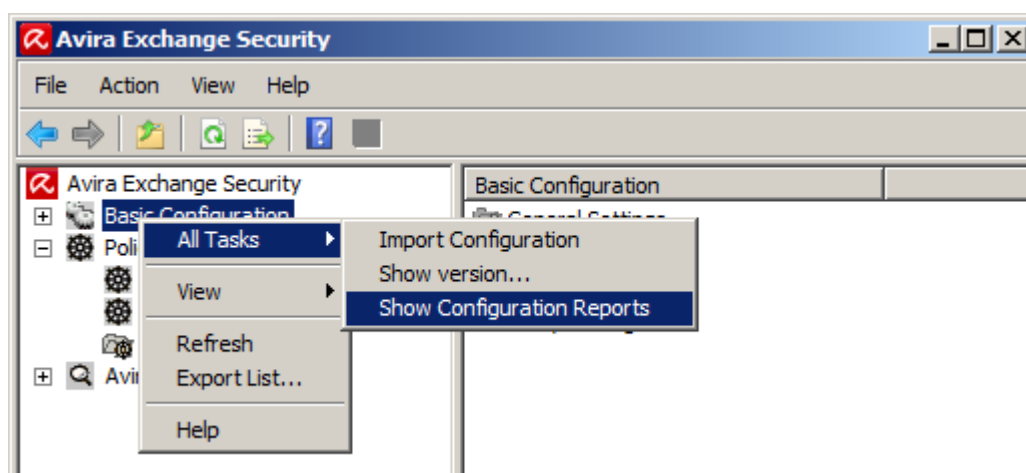
The basic configuration is used to manage:

- General settings, such as:
 - Proxy server
 - Address lists
 - Notification templates
 - Database connections to SQL servers
 - Avira servers
- Folders (quarantine folders)
- Utilities:
 - Word lists for the content filtering
 - Fingerprints for blocking attachments
 - Avira Scan Engine

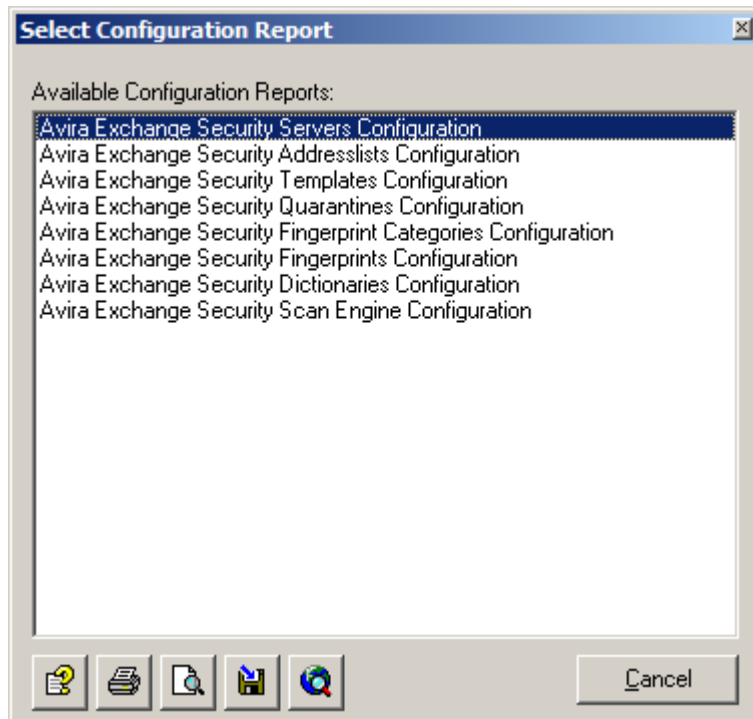
7.1.1 Generating configuration reports




A configuration report provides an overview of the current configuration.

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



2. Click the required report.



- Click the **Show report** button , to open the report as HTML file in the browser.
- Click the **Report preview** button , to open a print preview.
- Click the **Save report** button , to save the selected report as HTML file.

7.1.2 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.

Warning

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

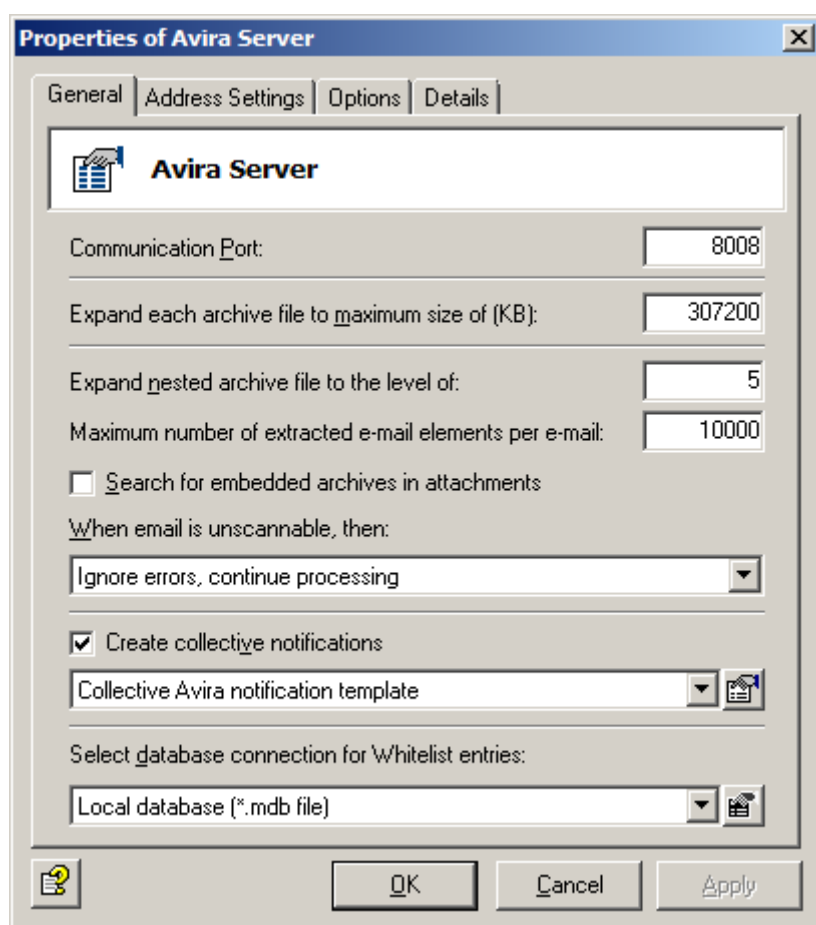
If a modified configuration version is available:

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

7.1.3 Making default settings for all servers

Under **Avira Server Settings** you can configure the default settings for all servers in Avira Exchange Security. Each server can also be configured on an individual basis.

1. Select **Basic Configuration > General Settings**.
2. To open the properties:
 - In the right-hand window right-click **Avira Server Settings** and select **Properties**.
 - Double-click **Avira Server Settings**.
 - In the left-hand window under **Basic Configuration** right-click **Avira Server**.
3. Click the **General** tab.



- **Communication Port:** Port 8008 is used as the default during installation. The value entered here applies to all servers.

Warning

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

- **Expand each archive...** and **Expand nested archive...:** Define the maximum allowed size for unpacked files on the hard disk and the maximum allowed unpacking depth for archives. Emails that exceed these values are transferred to the **BADMAIL** area.

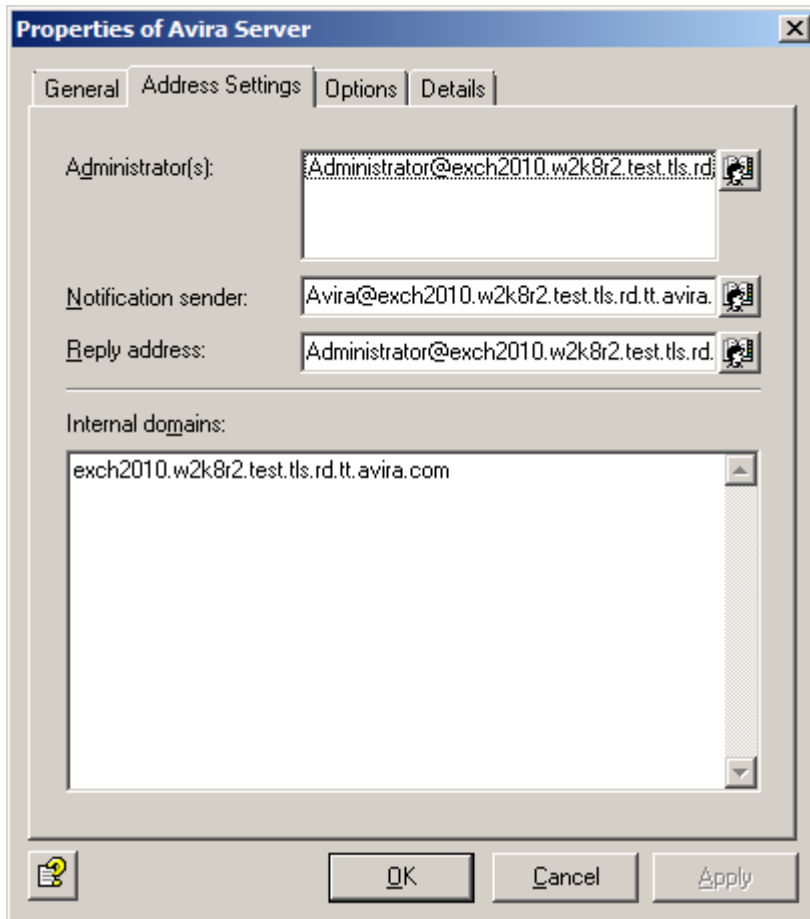
- **When email is unscannable:** Unscannable elements, for example emails including encrypted attachments, can be subject to cross-server actions which are automatically performed. Choose between two options from the drop-down. Either the fact that the email is unscannable can be ignored and the email is processed or the email is automatically moved to the **BADMAIL** directory.
- **Create collective notifications:** The recipients of this notification only receive one email that lists all incoming events. The collective notification is used as the template in this case. You can modify the template or create new templates (with **Basic Configuration** > **General Settings** > **Templates** > **Collective Notifications**).
- **Select database connection for Whitelist entries:** To create central user whitelists, you must first configure a database connection between the SQL server and the Avira Exchange Security server (**Basic Configuration** > **Database Connections**). As soon as this connection is in place, select the relevant configuration in this field.

4. Click the **Address Settings** tab to define email addresses and internal domains.

Email addresses and internal domains

Avira Exchange Security 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 Exchange Security administrator is used to enter the following basic settings:

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



- **Administrator(s):** The administrator addresses entered here receive important status notifications during the installation and the configured administrator notifications. The installation enters the queried administrator address as the default.
- **Notification sender:** The sender displayed in Avira notifications. The installation enters Avira Exchange Security with the mail domain of the queried administrator address as the default.
- **Reply address:** The recipient of the replies to these Avira Exchange Security notifications. The installation enters the queried administrator address as the default.
- **Internal domains:** The email domains specified here are seen as internal email domains, while all others are considered external email domains. This setting is used to differentiate between incoming and outgoing emails in the Avira Exchange Security rules on the basis of the sender and recipient addresses of an email. For example, an email filter job will only deal with incoming emails, while Avira 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, for example *.domain.com. The installation enters the mail domain of the queried administrator address as the default.

Collective notifications

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 Exchange Security 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.

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 option **Create collective notifications** under **General Settings > Avira Server Settings > General**.

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 multiple 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 Exchange Security servers in a central SQL database.

7.1.4 Creating an Avira Server

1. Under **Basic Configuration** right-click **Avira Server** and select **New > Avira Server**.
2. To be able to access a newly created server immediately in the **Avira Monitor**, update the view (right-click **Avira Monitor** and select **Update**, or use the icon in the toolbar).
3. Right-click the server's name, select **Properties** and configure the settings for the new server.

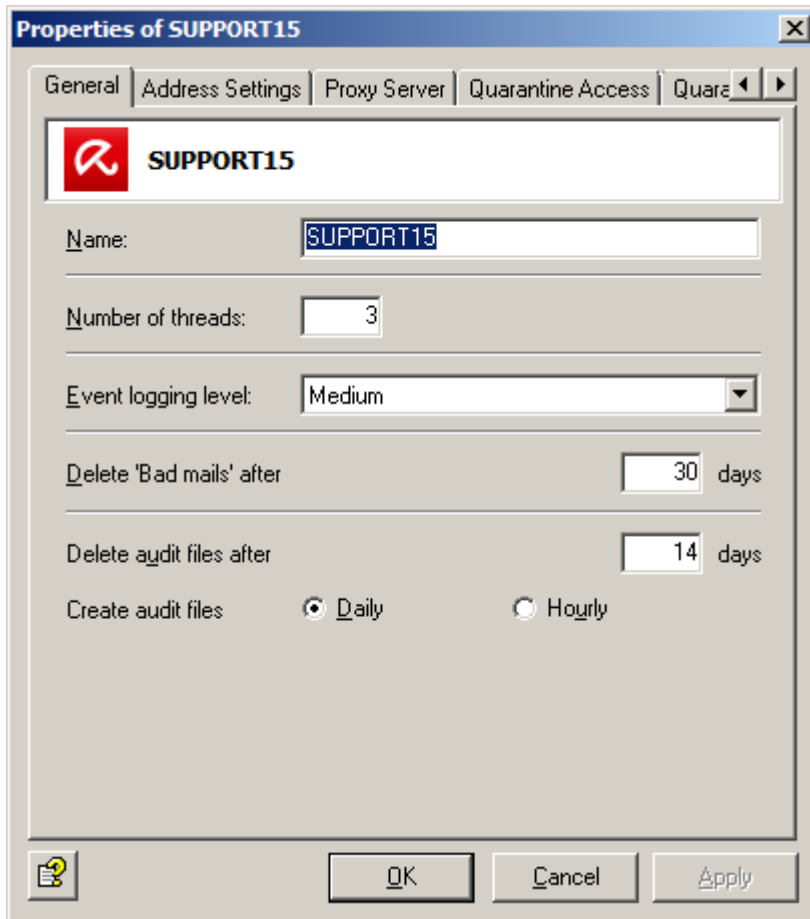
7.1.5 Making settings for an individual Avira Server

1. Under **Basic Configuration** click **Avira Server** and double-click the server you want to configure.
2. Make the general settings on the **General** tab.
3. Set individual email addresses on the **Address Settings** tab.
4. Set the proxy server on the **Proxy Server** tab.
5. Set the user access to quarantine in the **Quarantine Access** tab.
6. Make the settings for maintaining the quarantine in the **Quarantine Maintenance** tab.
7. Check the list of jobs defined on the server in the **Avira Jobs** tab.

Related topics:

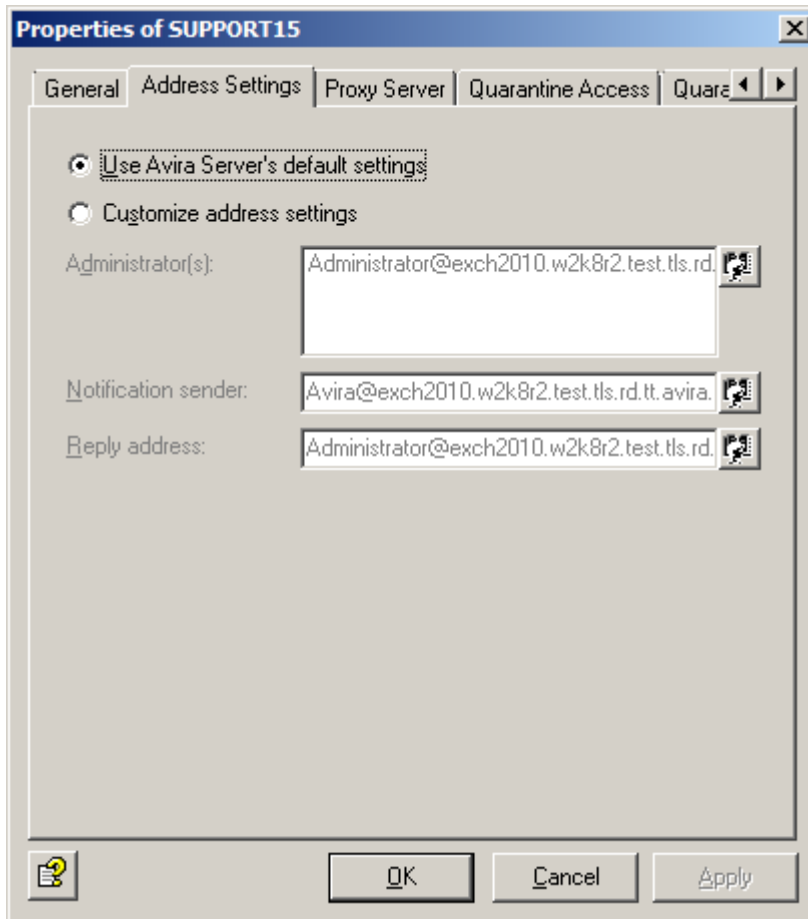
[Setting the access to Avira Monitor](#) - page 22

General server settings



- **Name:** Enter the name of the Exchange server. The current Exchange server name is automatically entered during installation.
- **Number of threads:** Define the maximum number of simultaneously processed emails. The number of emails that can be reasonably processed by Avira depends on the configuration and performance of your server.
- **Event logging level:** 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**.
- **Delete 'Bad mails' after:** Decide on the number of days for which the emails are to remain in the BADMAIL quarantine. The emails are automatically deleted after this number of days elapses.
- **Delete audit files after:** Define the number of days after which a job processing log is to be deleted in the *Log* folder.
- **Create audit files:** Select the frequency of creating audit files (daily or hourly).

Individual email addresses



- **Use Avira Server's default settings:** The settings for each server are taken from the properties of all Avira Servers that are set automatically during installation or that you have created individually.
- **Customize address settings:** If you need individual settings for a server, enable this option and enter the addresses in the relevant fields.

Proxy server settings

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

Note

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



Custom proxy server: Select the appropriate proxy server from the list.

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

Otherwise, you should enter the proxy server settings:

- **Name/IP Address:** The full name or IP address of the proxy server. Examples: `proxy.mydomain.de` or `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`.

If you want to delete a proxy server, right-click and selecting **Delete**. You cannot delete a proxy server that is already in use by an object.

User-specific access to quarantine

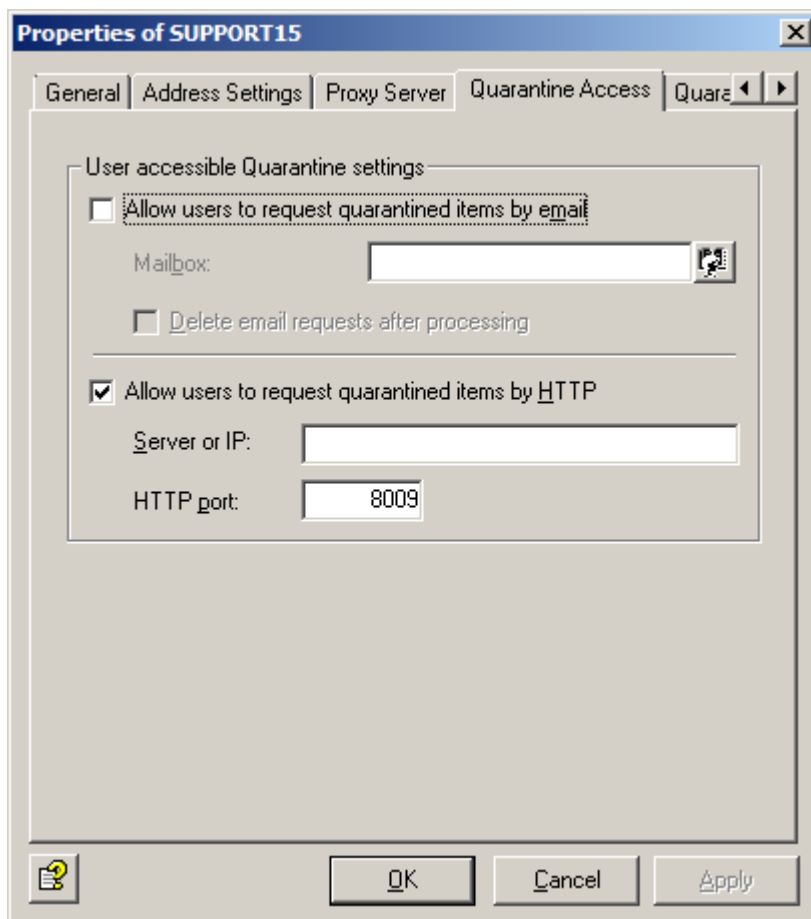
Avira Exchange Security allows users to access their own quarantine emails.

Which emails are available and which users have access can be configured individually for each quarantine. This function is particularly interesting in relation to email filtering, for email 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), **Remove** (flag email for deletion in the quarantine), **Add to user whitelist** or **Add to user blacklist**. User access is by means of an email request or a HTTP request.



- **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 Exchange Security 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. Avira recognizes request emails from users by the following:

- The email address (specified in the **Mailbox** field)
- The keyword for a user request in the email (User Request)

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

- **Delete email requests after processing:** The request emails are 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 the request is being processed. This request requires a free port. The standard entry is port 8009.

The response to users displayed by the browser is always the same (*OK_Response.html* in directory ...\\Avira\\Avira Exchange Security\\AppData). The user will not be notified if the requested email no longer exists, if for example it has already been deleted in the quarantine.

- **Configuring a Globale Quarantine Summary Notification:** In a server environment with several Avira Exchange Security servers using the same Avira Exchange Security configuration with the same quarantines, we recommend you, to configure a global quarantine summary notification that contains all notifications for all the quarantines of a user into one notification. Without global quarantine summary notifications each internal user receives an individual summary notification for each of his/hers quarantines from each involved Avira Exchange Security server.

Specify a global Avira Exchange Security server. This server collects all the required quarantine data from all involved quarantines to one global quarantine summary notification and sends it to the internal users.

1. Open the Avira Server settings: GENERAL SETTINGS -> Avira Server settings -> OPTIONS tab.
2. Under **Global Avira Server** select the Avira Exchange Security server that shall be defined as global Avira Exchange Security server
3. Under **User/Password** enter the name and the password for the user who has the administrative rights on all the quarantines of all Avira Exchange Security servers (e.g. the Avira Exchange Security administrator).

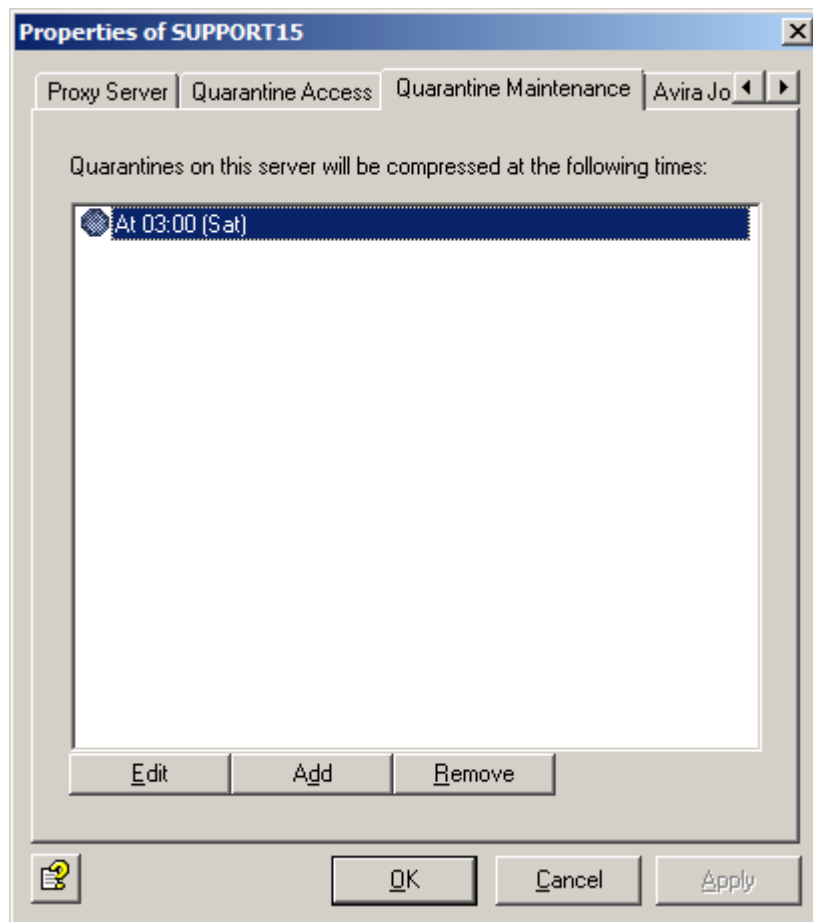
4. Define for which quarantines a global quarantine summary notification shall be created. Open the desired quarantines under FOLDER SETTINGS -> QUARANTINE and enable in the **Summary Notification** tab the 'Create globale quarantine summary notification' option.

Note

When this option is not enabled, each involved Avira Exchange Security server will send individual summary notifications for this quarantine.

Quarantine maintenance settings

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.

You can also compress a quarantine manually if necessary, by right-clicking on the relevant quarantine in **Avira Monitor** and selecting **All Tasks > Compress Quarantine**.

7.2 Database connections

Note

Avira Exchange Security 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 Exchange Security and on the MS SQL server that cannot be explained here. If you have specific questions, please contact our Support team.

You can use database connections to link external databases to Avira Exchange Security. 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 Exchange Security data in an SQL database. At present, the following versions can be used:

- MS SQL Server 2005
- MS SQL Server 2005 Express, when CPU and memory capacity are limited
- MS SQL Server 2008 R2

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 Exchange Security 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 Exchange Security Server, so that only one database connection is required.

7.2.1 Prerequisites for database connection

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

- Installations of SQL server and Avira Exchange Security 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 Exchange Security Server

If the SQL server and the Avira Exchange Security 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

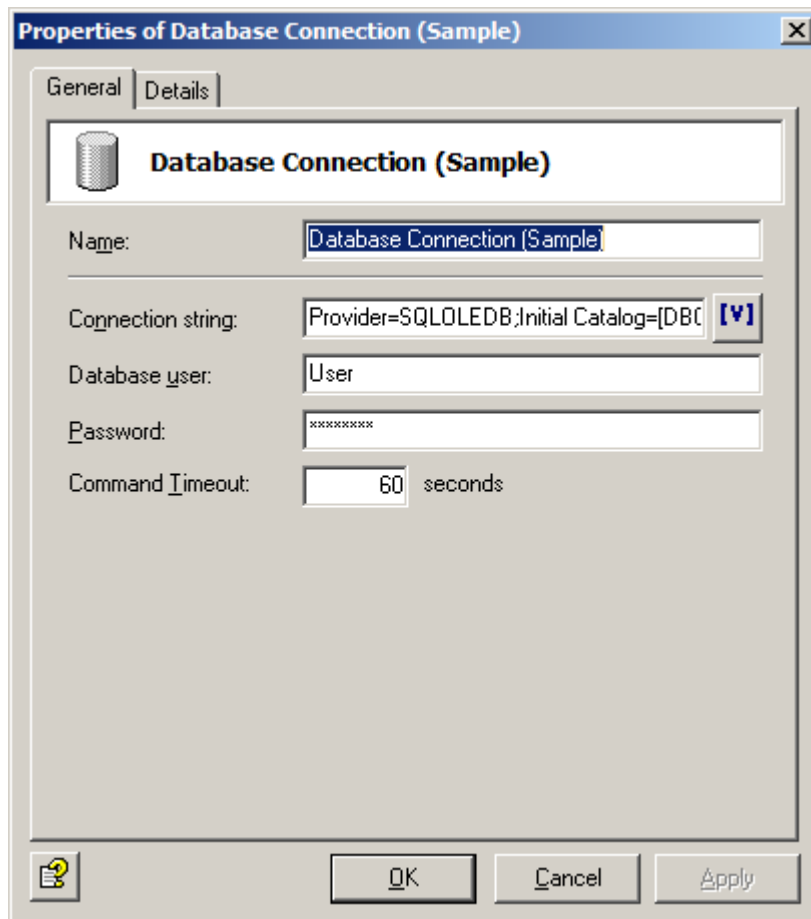
7.2.2 Configuring the database connection

The following sections describe the configuration of database connections between Avira Exchange Security 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.

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

1. Create a new database connection under **Basic Configuration > General Settings > Database Connections**.



2. Assign a name for the connection configuration and define the details for the ADO string in the **Connection string** field.

Enter the required values manually or use the stored Avira Exchange Security variables (server, database, etc.), which are then replaced by the relevant values during runtime.

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

3. Enter the name of the SQL user permitted to access the database in the **Database user** field, and the password in the **Password** field.

The values entered here can be read out using the variables `[ADOUser]` and `[ADOPwd]` in the ADO string.

4. In the **Command Timeout** field, specify the waiting period in seconds before the database connection is closed, if the database does not return data.

You should begin with a value of 60 seconds when using large databases.

7.2.3 Example of ADO string configuration

The following example is one of many configuration options for the ADO string. You can 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=[ADOUser];Password=[ADOPwd];Trusted_Connection=No;
InitialCatalog=DBCatalog];Data Source=LOCALHOST
\SQLEXPRESS;
```

- **Provider=SQLOLEDB;** Obligatory parameter that specifies the provider. Enter the value manually (no Avira variable available).
- **User ID=[ADOUser];Password=[ADOPwd];** Obligatory parameter; enter the parameters **User ID=** and **Password=** manually in the string and set the Avira variables **Database user** and **Password**. The inserted **[ADOUser]** 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 Exchange Security Server as a trusted server, enter **Trusted_Connection=No;** manually (no Avira Exchange Security 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 Exchange Security 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 Exchange Security 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 Exchange Security **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.

7.2.4 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 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 Exchange Security Servers in a central SQL database.

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

The configuration of the database connection depends on the server environment.

1. Enter the central SQL server under `Data Source=`
The `[DBCatalog]` variable for the whitelist database is replaced with the fixed database name in the ADO string of the database connection.
2. Under **Avira Server Settings > Properties** select the SQL server in the field **Database connection for whitelist entries**.
This field contains all data sources entered under database connections for selection.
3. Open the email filtering job **Advanced Email Filtering**, go to **Actions > Definite Criteria** and enable the field **Emails from senders in user whitelist**.

7.2.5 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. Enter `Source=` under data on every LOCALHOST server, so as to be able to access the locally installed SQL server.
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.

2. If you want to set a quarantine to be **mission critical**, go to **Quarantine**, right click **Properties** and enable **Quarantine is mission critical**.

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. Similar to jobs, the **mission critical** option is also available for the quarantine 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; whether the job ignores the email or moves it to the bad mail directory, depends on the **mission critical** setting in the job itself.

7.2.6 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.
 - On **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 Avira 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.
- If the database service fails, you should also check the configuration options for quarantine (**mission critical**).

7.3 Address lists

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

Related topics:

[Message details](#) - page 27


[Adding a sender to an address list](#) - page 26

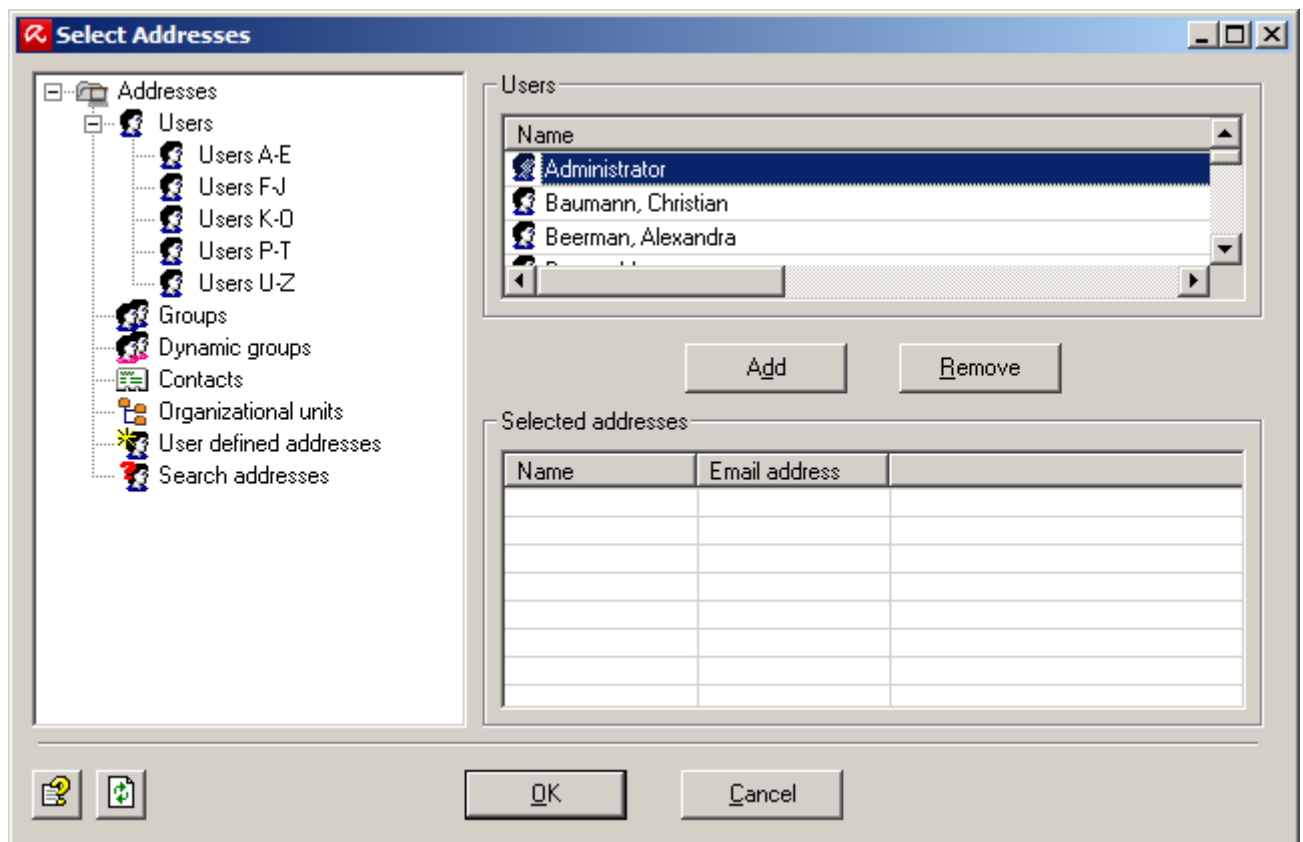
[Sending emails from quarantines](#) - page 24


[Avira Monitor](#) - page 22

[Email addresses and internal domains](#) - page 104

7.3.1 Creating address lists

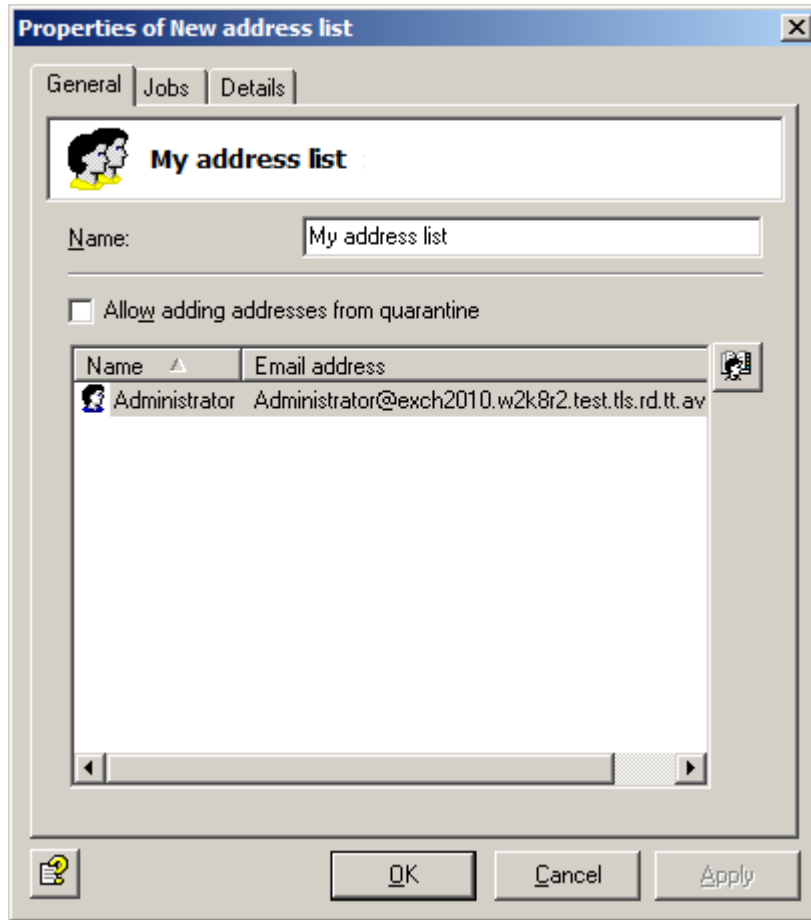
1. Open **Basic Configuration** > **General Settings**.
2. Right-click **Address lists** and select **New** > **Address List**.
3. Type a name for the address list.
4. Click the **Select Addresses** button: .
5. Click **Add** to select the required addresses under the various headings.



- 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 the 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**.

The properties of the address list are opened.



7. If direct access to this address list is to be permitted from a quarantined email, enable the option **Allow adding addresses from quarantine**.

When you view a quarantined email in **Avira Monitor** you can use the **Add** button to add the sender address of the quarantined email to various address lists.

By default, the following address lists are released for direct access:

- Email Filter: Blacklist
- Email Filter: Newsletter Blacklist
- Email Filter: Newsletter Whitelist
- Email Filter: Whitelist

8. Click **OK**.

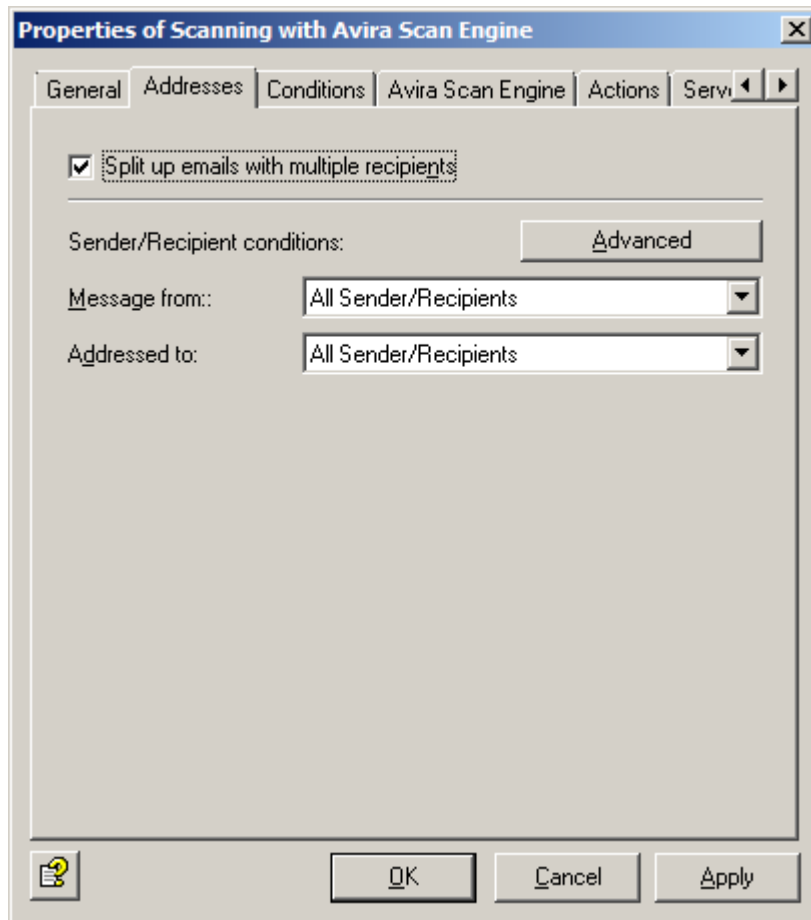
7.3.2 Deleting an address list

1. Open **Basic Configuration > General Settings**.
2. Right-click a list under **Address lists** and select **Delete** from the context menu.

7.3.3 Using address lists in jobs

In each job you can use the **Addresses** tab to choose the users to whom the job is to apply.

1. Click the **Addresses** in the job properties.



- **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.
- **Message from** and **Addressed to:** Choose whether the job applies to *All Sender/Recipients* or is to be restricted to internal or external senders/ recipients.

Note

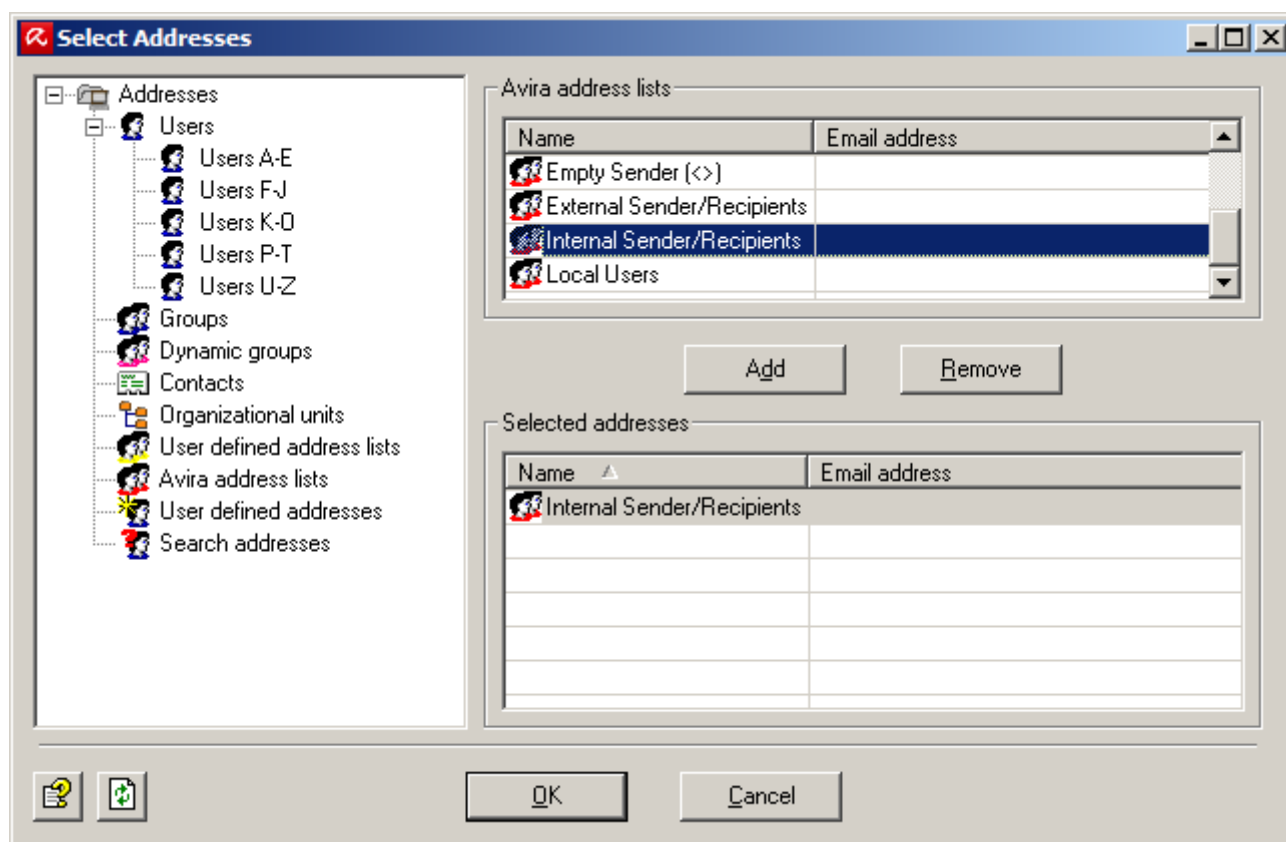
Both conditions in the **Message from** and **Addressed to** fields must apply, if an action is to be triggered (AND link).

2. Click **Advanced**.

Note

All specified conditions in the fields **Run this job when a message arrives from** and **And where addressed to** must apply if an action is to be triggered (AND link). If several addresses are entered within the same condition (**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.

3. 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.



4. Click **Avira address lists** in the navigation panel, to see the lists defined for Avira.

Avira address lists are fixed lists from which settings for the higher Avira Exchange Security servers are generated that are requested and entered upon installation, or that you have configured manually.

User defined address lists and **Avira address lists** are only displayed when an address is selected for a job.

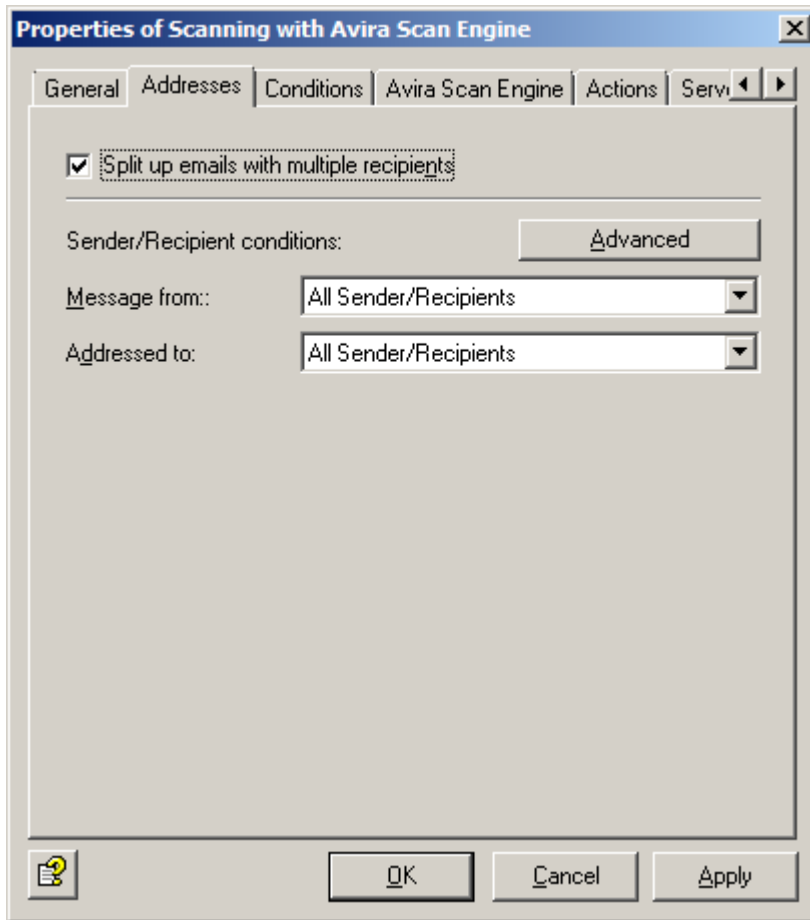
User defined address lists can be changed anytime; Avira address lists cannot be changed.

7.3.4 Address settings when 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:



7.3.5 Address settings when blocking 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.

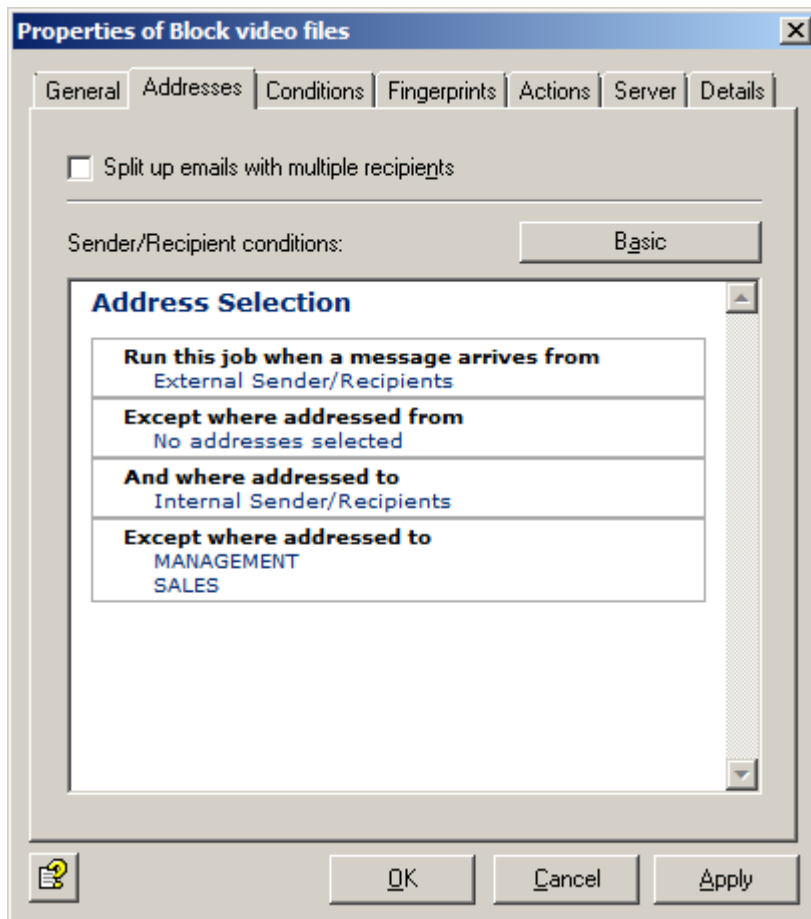
- **Run this job when a message arrives from** checks the sender(s). The exception **Except where addressed from** also applies.
- **And where addressed to** scans the recipient(s). The exception **Except where addressed to** also applies.

Implementation: The defined action in the job (in other words the blocking of attachments) will be executed under the following address conditions:

- **Run this job when a message arrives from:** *External Senders/Recipients.*
- **And where addressed 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 is how the address settings are displayed in the job:




This means that all video attachments sent by external senders to internal recipients will be intercepted unless the recipient is in the sales department team or a member of senior management.

7.4 Templates

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

When you create a new job, you can select the appropriate template for the job type. The report templates for the various jobs (content check, virus scan, etc.) are created in the **Basic Configuration**.

7.4.1 Creating notification templates

1. Go to **Basic Configuration > General Settings > Templates** to see preconfigured report templates for the various modules.
2. Right-click the template type and select **Properties**.
3. Type a text for the subject of the notification.
4. Click on the **Notification text - Edit** tab to edit the text of the notification.
You can change the layout of the text using the formatting menu bar. The information will then be converted internally into HTML commands. If you retrieve the source text with the **Source** button , you can also enter HTML commands directly.
5. If you want to see the jobs in which the notification template is used, click the **Jobs** tab.
6. Click **OK**.

7.4.2 List of notification variables

The following variables, which can also be entered directly with the arrow next to the **[V]** 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 variables

Category, variable type	Variable	Description
General: Sender	<code>[VAR]Mailsender[/VAR]</code>	Sender of the triggering email
General: Sender (SMTP)	<code>[VAR]From[/VAR]</code>	Sender SMTP of the triggering email
General: Subject	<code>[VAR]Subject[/VAR]</code>	Subject line of the triggering email
General: Date and Time	<code>[VAR]Date[/VAR]</code>	Date and time when the job triggered the action
General: Date	<code>[VAR]DateOnly[/VAR]</code>	Date when the job triggered the action
General: Recipient(s)	<code>[VAR]Recipients[/VAR]</code>	Recipients of the triggering email
General: Job Name	<code>[VAR]Jobname[/VAR]</code>	Name of the job that started an action
General: Unrestricted Recipient(s)	<code>[VAR]UnrestrictedRecipients[/VAR]</code>	Recipients of the triggering email not defined in the address (input) conditions

Category, variable type	Variable	Description
General: Quarantine folder	[VAR]Quarantine[/VAR]	The quarantine where an email has been placed
General: Key of quarantined 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 Report	[VAR]ToolReport[/VAR]	Short summary of the scan results
General: Avira 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

Avira variables

Category, variable type	Variable	Description
Avira: Attachment size	[VAR]AttachmentSize[/VAR]	Size of the prohibited/affected attachment
Avira: Attachment type	[VAR]FingerprintName[/VAR]	Name of the prohibited file type
Avira: Fingerprint category	[VAR]Fingerprintcategory[/VAR]	Category of the prohibited file type
Avira: Email size	[VAR]MessageSize[/VAR]	Size of the entire email
Avira: Attachment name	[VAR]AttachmentName[/VAR]	Name of the prohibited/affected attachments

Category, variable type	Variable	Description
Avira: Email size limit	[VAR]SetSizeLimit[/VAR]	Maximum email size defined in the job
Avira: Malware name	[VAR]Virusname[/VAR]	Names of the viruses detected
Avira: Scan engine	[VAR]VirusScanner[/VAR]	Names of the detecting virus scanners

Information store scan variables

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

Category, variable type	Variable	Description
		information store scan took place
IS Scan: Scan engine	[VAR]virusscanner[/VAR]	Name of the detecting virus scanner
IS Scan: Malware name	[VAR]virusname[/VAR]	Names of the viruses detected
IS Scan: Delivery time	[VAR]VSAPI_DeliveryTime[/VAR]	Date and time the message was delivered

Avira Email Filter variables

Category, variable type	Variable	Description
Content scan		
Avira Email Filter: Content analysis details	[VAR]DeniedContentTabHTML[/VAR]	Detailed information about the words/phrases found
Avira Email Filter: Mail part	[VAR]DeniedMailParts[/VAR]	Affected triggering attachments/message texts
Avira Email Filter: Restricted dictionaries	[VAR]DeniedWordlists[/VAR]	Triggering dictionary with value/threshold attained
Avira Email Filter: Restricted words	[VAR]DeniedWord[/VAR]	Triggering word with value/threshold attained
Unwanted email check		
Avira Email Filter: Unwanted Email analysis details	[VAR]SpamReportHTML[/VAR]	Detailed information about the individual spam criteria
Avira Email Filter: Probability for Unwanted Email	[VAR]SpamValue[/VAR]	Determined probability for unwanted emails in the form of a value (0 - 100). This value is compared with the individually set thresholds in the Advanced Email Filtering job.
Avira Email Filter: Level for Unwanted Email	[VAR]SpamLevel[/VAR]	Avira Email Filter enters a level for unwanted emails 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

Category, variable type	Variable	Description
		10, X-SPAMTAG:*** means the probability for unwanted emails 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		
General: Number of recipients	[VAR]NumberRecipient[/VAR]	Number of addressed recipients
Avira Email Filter: Recipient number limit	[VAR]SetRecipientLimit[/VAR]	Restriction on the number of recipients set in the job
Avira Email Filter: Restricted senders	[VAR]DeniedSender[/VAR]	Name of the triggering sender
Avira Email Filter: Restricted recipients	[VAR]DeniedRecipient[/VAR]	Name of the triggering recipients

Quarantine summary report variables

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

Category, variable type	Variable	Description
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.
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 variables

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").

Category, variable type	Variable	Description
Collective notification: Notification list	[VAR]NotificationList[/VAR]	HTML list of all notifications (body), each separated by a vertical separating line.
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)

Whitelist variables

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: Display 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 To	[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

Category, variable type	Variable	Description
		for which the notifications are generated
Userlist: Size	[VAR]CollectedSize[/VAR]	Overall size of whitelist notification
Userlist: Subject	[VAR]Subject[/VAR]	Notification subject
Userlist: Summary part	[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

7.5 Quarantine configuration

A quarantine is a folder in which all emails affected by the conditions are stored, if you defined this with the action **Copy to Quarantine**.

When you install Avira Exchange Security, a folder called *Quarantine* is created in the data directory (...\\Avira\\Avira Exchange Security\\AviraData). This folder initially contains some default quarantines and later all additional newly created quarantines.

Related topics:

[Setting the access to Avira Monitor](#) - page 22

7.5.1 Creating a new quarantine

Warning

The size of a quarantine is restricted to 1 GB.

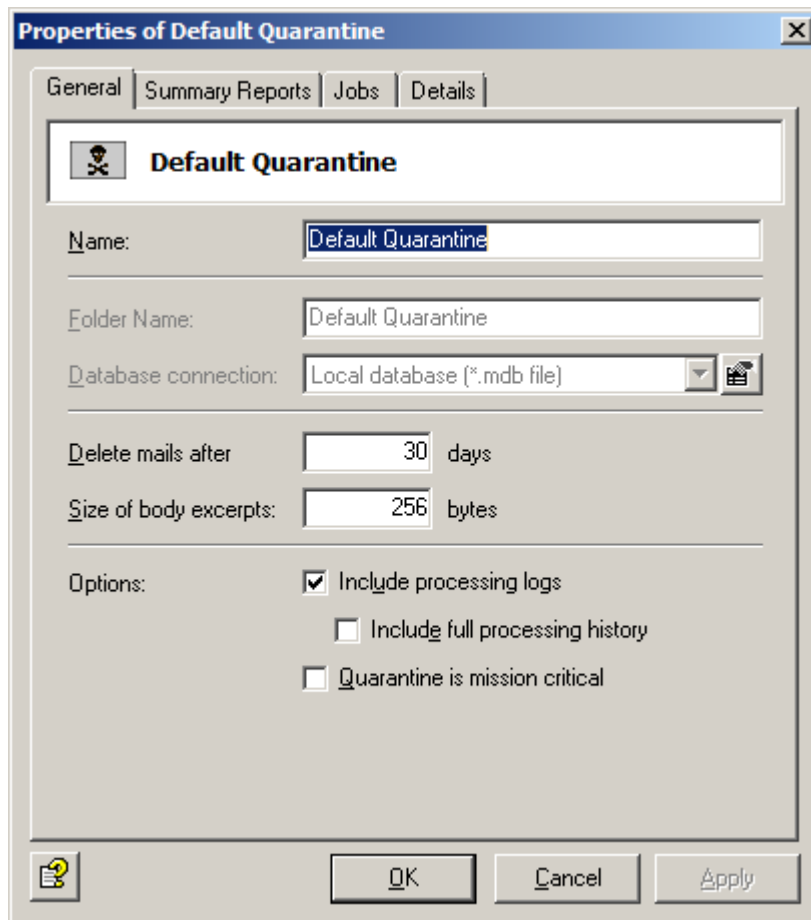
1. Go to **Basic Configuration > Folders > Quarantine**.
All available quarantines are displayed in the right-hand window.
2. Right-click **Quarantine** and select **New > Quarantine**.
The **Folder name** from the description is transferred. Only characters from A-Z and 0-9 are transferred; all other characters are converted to underscores.
3. Type a quarantine name, if you want to change the one suggested in **Folder name**.
Do not enter an absolute path. You only need to enter the folder name.
4. Save the configuration.
EMH automatically creates the new quarantine. It is also displayed in the Avira Monitor, if you update the view.

7.5.2 Configuring a quarantine

Warning

The size of a quarantine is restricted to 1 GB.

1. Go to **Basic Configuration > Folders > Quarantine**.
All available quarantines are displayed in the right-hand window.
2. Right-click an existing quarantine in the list and select **Properties**.



- **Name:** Give the quarantine a meaningful name.

The **Folder name** of the quarantine remains unchanged. It is only available for some, newly created quarantines.

- **Delete mails after:** Define how many days an email that was placed in quarantine should be kept before it is automatically deleted.
- **Size of body excerpts:** Specify what amount 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.
- **Include processing logs:** 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 Avira Monitor, you can access the respective email and view the processing log including detailed information on the **Processing Log** tab.
- **Quarantine is 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, for example whether the job ignores the email or moves it to the BADMAIL directory, depends on the "mission critical" settings in the job itself.

For as long as the quarantine error is not fixed, the error will be repeatedly reported to the job.

- 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 BADMAIL area and is not delivered until such time as the error is fixed.

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

3. Click the **Summary Reports**, to configure a quarantine summary report for this quarantine.

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

Related topics:

[Mission critical jobs](#) - page 38

7.5.3 Example of mission critical quarantine

Scenario: 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 is mission critical	Job is mission critical	Result
no	no	The quarantine error is ignored. The email cannot be copied to the quarantine and it is not delivered.
no	yes	The quarantine error is ignored. The email cannot be copied to the quarantine and it is not delivered.
yes	no	The job processing is canceled and the virulent (!) email is transferred unprocessed to the next job in the processing chain.
yes	yes	The email is moved to the BADMAIL quarantine and is kept there. The email is not delivered.

7.5.4 Quarantine Summaries

Quarantine Summaries provide information on emails that Avira Exchange Security 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.

Note

For connecting to the Avira Exchange Quarantine, you have to set the ports 8008 and 8009 in the Windows Firewall. If these ports are not open, it is not possible to connect via **Quarantine Summary Report** to the Avira Exchange application for request, release or adding a trustworthy sender to the whitelist.

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 Summaries**. The variables available here are exclusively related to the summary reports and their form.
- 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 variable **Summary Report: List of Quarantine Mails** (`[VAR]HTMList[/VAR]`), which is a mandatory entry in each summary report. The entries that this list contains are defined under **Basic Configuration > Folders > Quarantine > Properties of a Quarantine > Summary Reports > Add > Fields**.

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.

Related topics:

[Creating notification templates](#) - page 124

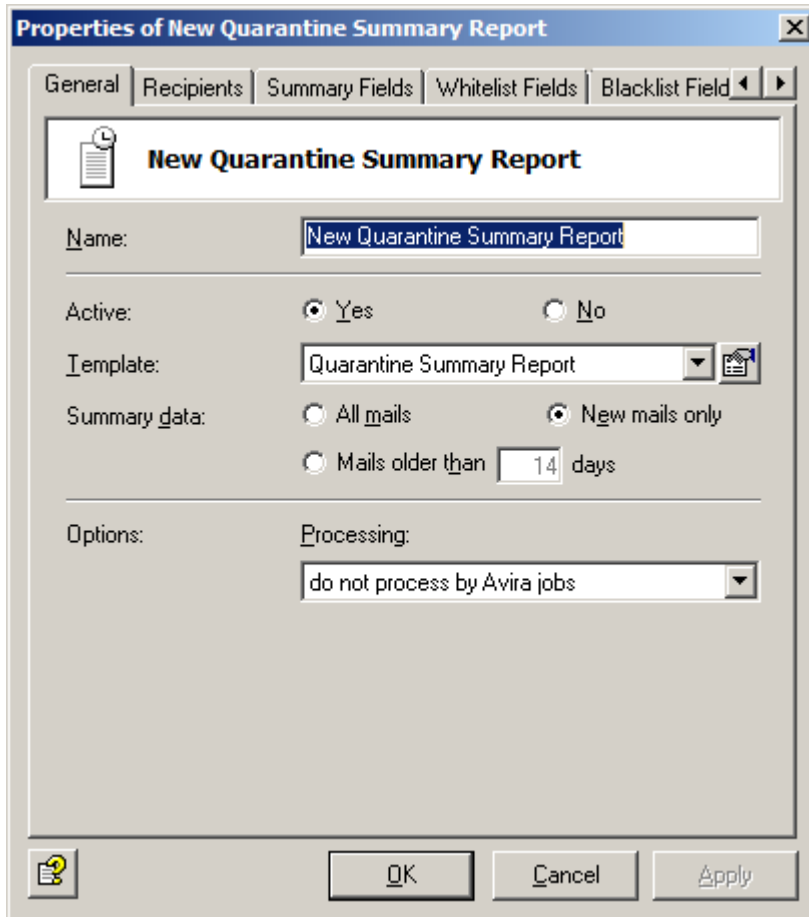
7.5.5 Setting a summary report

Summary reports are particularly intended for unwanted email quarantines and the recipients of these unwanted emails. The standard case is for the users to receive a list of all new unwanted emails that were addressed to them and that are in a specific email quarantine.

You can create several 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.

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

1. Open **Basic Configuration > Folders > Quarantine**.
2. In the right-hand window, double-click an email quarantine to open it. For example **Email Filter: Medium**.
3. On the **Summary Reports** tab, click **Add**.
4. Make the settings on the **General** tab.




Properties of New Quarantine Summary Report

General Recipients Summary Fields Whitelist Fields Blacklist Fields

New Quarantine Summary Report


Name:

Active: ☒ Yes ☐ No

Template: 

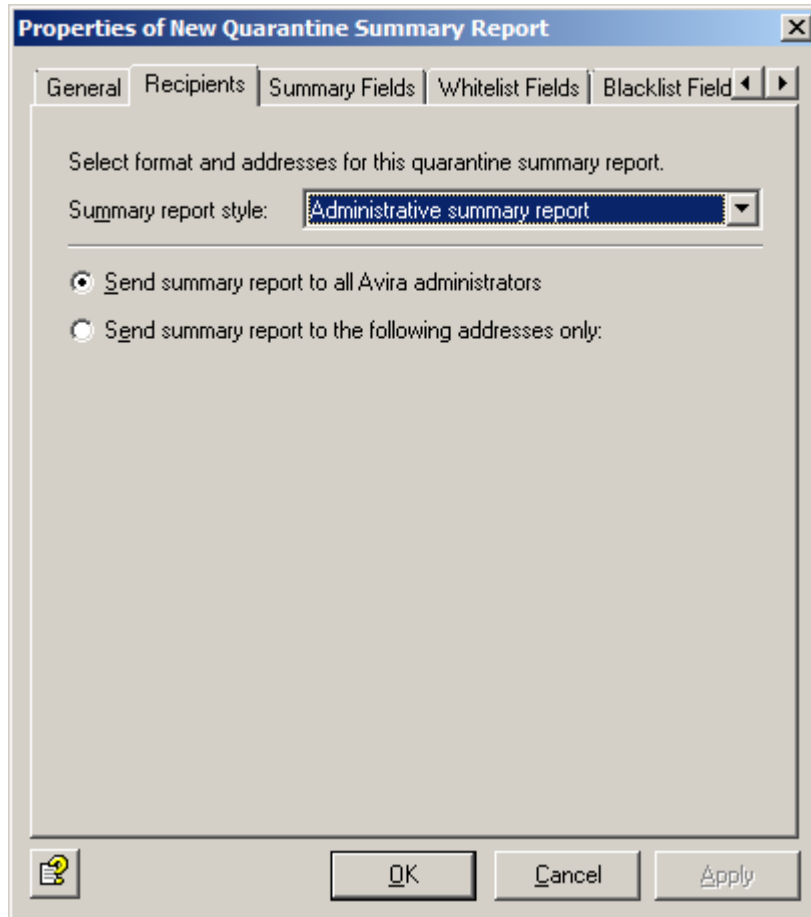
Summary data: ☐ All mails ☒ New mails only
☐ Mails older than days

Options: Processing:

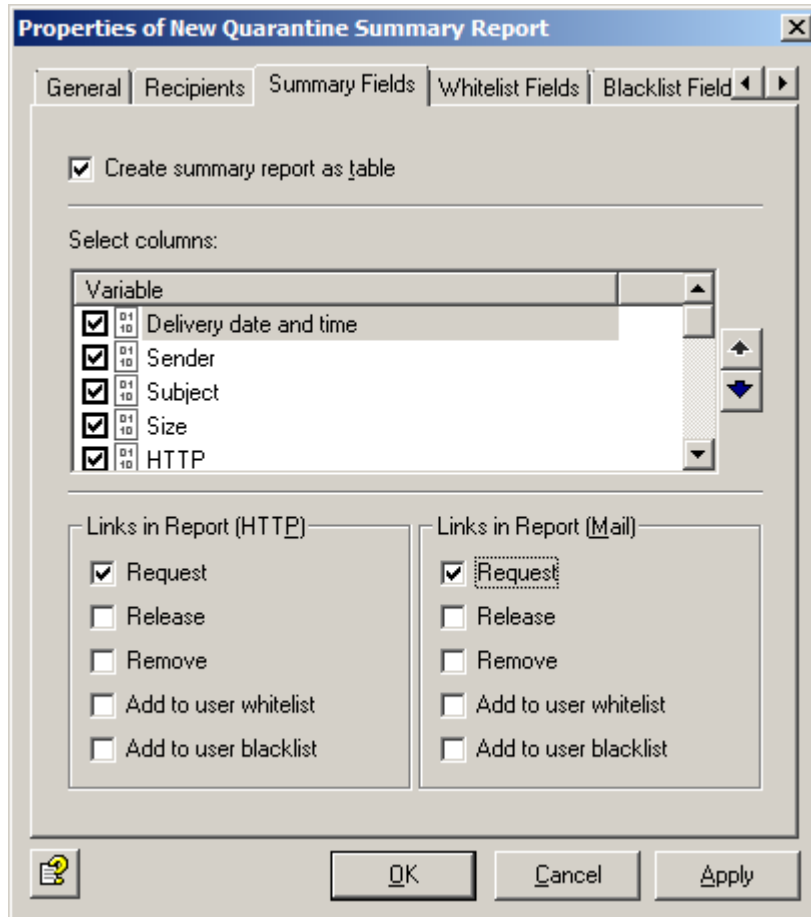


- **Name:** Assign a name for the summary report and click **Yes** to activate the report.
- **Template:** Select a summary report that you defined under **General Settings > Templates > Quarantine > Summary Reports**. The default in Avira Exchange Security is the template **Quarantine Summary Report**, 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 template **Quarantine Summary Report with Whitelist Support**. If you want to allow your users to place a sender from the summary report on their user blacklist, use the template **Quarantine Summary Report with Blacklist Support**.
- **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.
- **Processing: do not process by Avira jobs** means that the resent email which the user requested or released is no longer checked by the active Avira jobs. Each requested or released email is delivered unchecked to the recipient.

5. Select the format and addresses for the report on the **Recipients** tab.

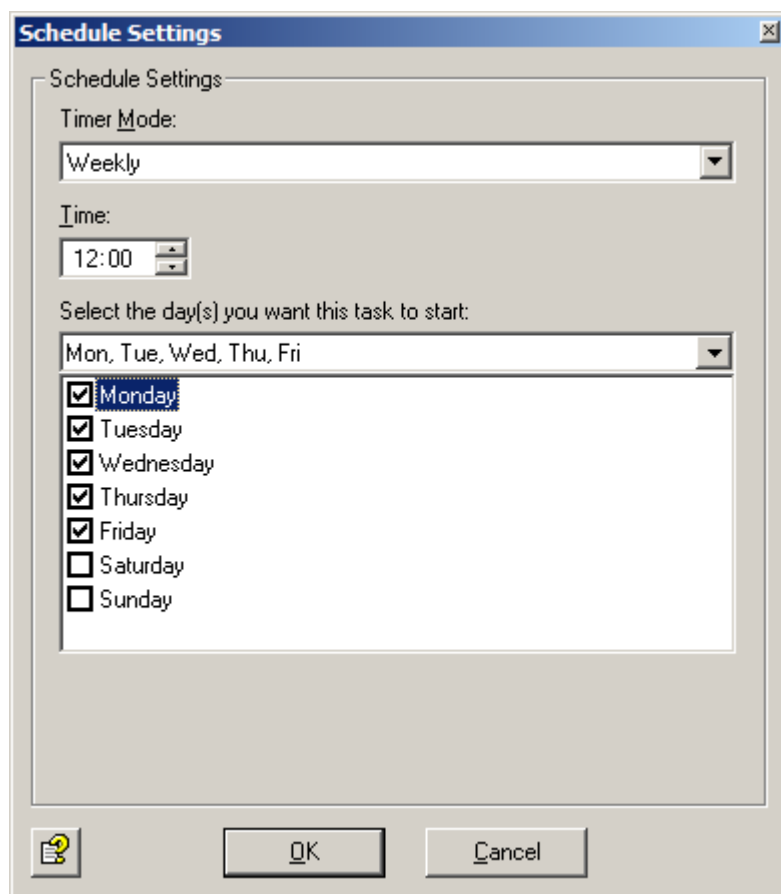


- **Administrative summary report:** All administrators receive the summary report of the quarantine emails.
 - **User-related summary report:** Define if the recipients or the sender of an email receives the summary report.
 - **Send summary report to the following addresses only:** Define the group of recipients for a summary report. The selected recipients, senders, groups or other address patterns are then listed in a text box.
6. In the **Summary Fields** tab, select which fields of the quarantine emails are to be written in the summary report.



- **Variable:** Select the variables to be added to the report.
- **Links in Report:** Select the actions a recipient can execute within the summary report by clicking the links in the report.
 - **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.

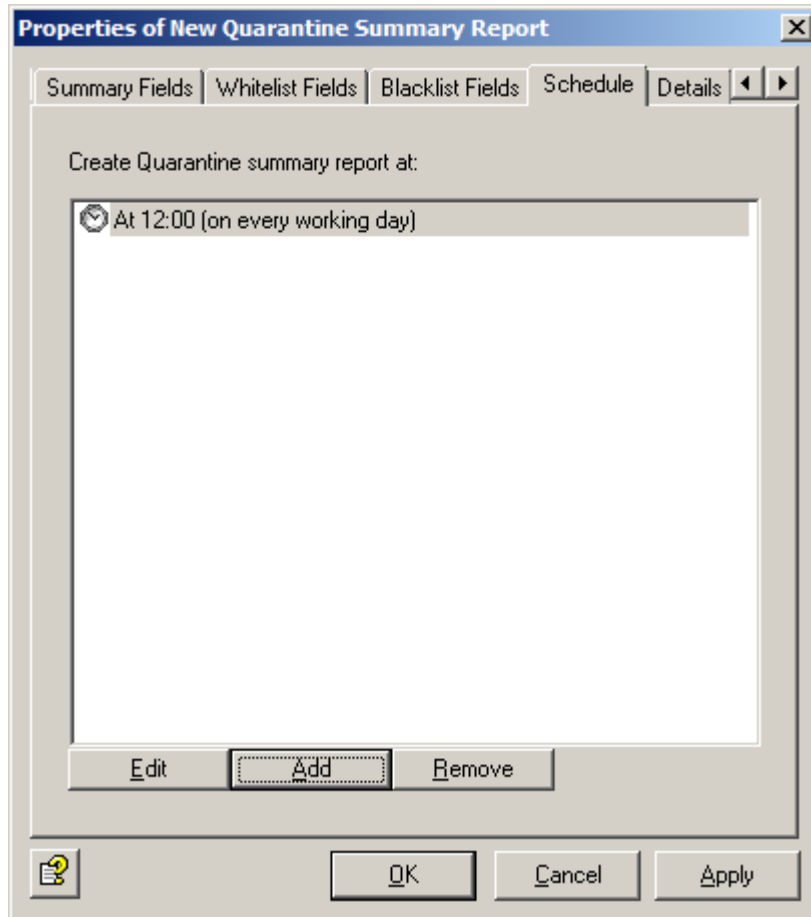
7. On the **Whitelist Fields** or **Blacklist Fields** tabs, select the fields from the quarantine emails that you want to appear in the whitelist or blacklist report.
8. On the **Schedule** tab click **Add**.



9. In the **Schedule Settings** dialog define the start of the summary report creation.
For example, a summary report of the **Email Filter: Medium** quarantine is generated and sent to the selected recipients every workday at 12:00 a.m.

10. Click **OK**.

Your new quarantine summary report is displayed in the **Schedule** tab.



Edit allows you to change the time or the day of the week. **Remove** deletes the selected summary report.

11. Click **Apply** and close the **Properties** dialog.

Related topics:

[List of notification variables](#) - page 124

7.6 Utility Settings

- **Fingerprints:** Avira: A comprehensive list of fingerprints used for file type recognition is supplied with Avira Exchange Security, divided into categories. It is generally not necessary to make any changes.
- **Dictionaries:** You can create dictionaries that contain word strings which you want to block during content and email filtering with Avira Email Filter. We provide some dictionary categories, which you can adapt to your own needs.
- **Avira Scan Engine**

Related topics:

[Fingerprints](#) - page 54

[Setting up dictionaries](#) - page 71

[Configuring and enabling Avira Scan Engine](#) - page 34

7.7 Policy Configuration

Under **Policy Configuration** you define the Avira 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 each job.

The sum of the Avira jobs is the company policy.

7.7.1 Example of a policy

Every incoming unwanted email is to be detected, deleted or sent to quarantine.

The unwanted emails should not reach the recipients. The recipients should be informed that they have received unwanted emails and the emails should be named so that they can decide for themselves which of these emails to receive. This is to be achieved with a daily summary.

All of this can be set up in the Avira Unwanted Email Filtering jobs.

7.7.2 Job types

You can find various job types, if you select **New** in the context menu of **Policy Configuration > Mail Transport Jobs**.

A series of standard jobs is provided with Avira Exchange Security 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**.

You can create any number of jobs.

The sequence in which jobs are 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 arrow buttons in the toolbar or right-click and select **All Tasks > Up/Down** to move the jobs to the required position.

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 do not need to permanently delete them from the configuration.

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

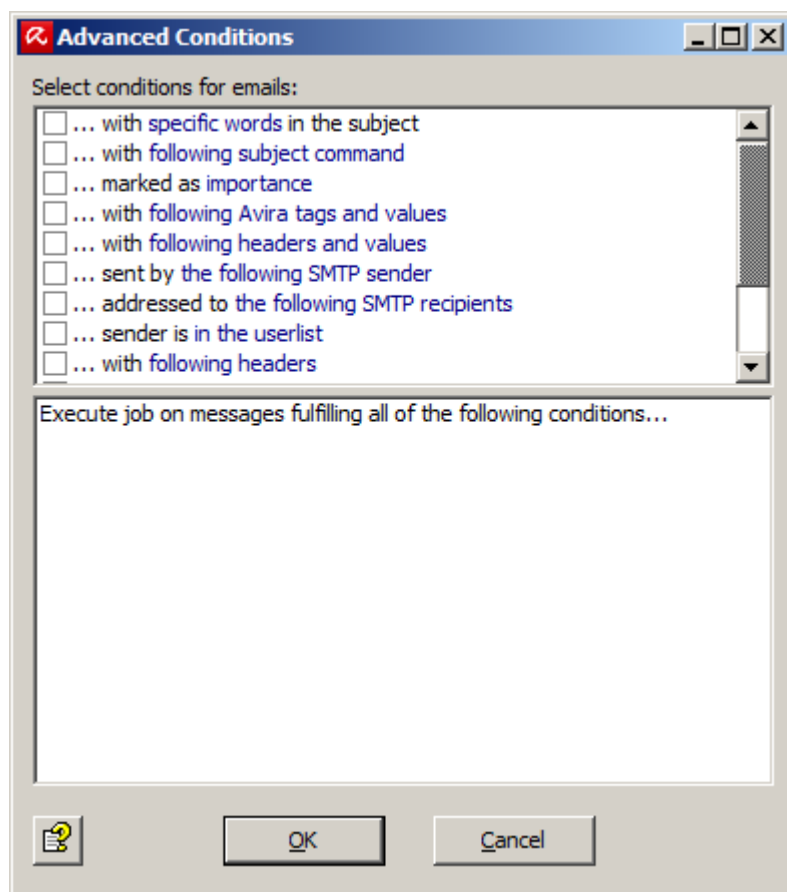
Job type	Description
Avira Scanning	Job scans the emails for viruses.

Job type	Description
Avira Email Size Filtering	Job checks the emails for a maximum allowed size (specified per email).
Avira Attachment Filtering	Job scans the emails for prohibited file attachments. The various file formats are identified using fingerprints.
Avira 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.
Avira 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.
Avira Email Filter Content Filtering	Job scans the emails and attachments for prohibited text content.
Avira Email Filter Address Filtering	Job checks the emails for address restrictions.
Avira Email Filter 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).
Avira Unwanted Email Filtering	Job uses various criteria to scan emails for unwanted content.

Address filters can be configured for all job types. For example, you can configure that all emails sent from the domains **@gmh.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 Avira Attachment/ Size Filtering job.

7.7.3 Job 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, for example 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 Exchange Security can for example add certain X-header fields with defined values to the emails.

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.















7.7.4 Job actions

In addition to the actions that belong to the function of a job, the following standard actions are 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.















Action	Meaning
Delete email	The infected/ blocked original email is permanently deleted from the server (a copy remains in quarantine if the copy 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	<p>Notifications can be sent to the following groups:</p> <ul style="list-style-type: none"> • Administrators • Senders • Recipients • Others
Start external application	An external, freely selected application is run.
Add header field and value	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.
Remove header field	The email X-header fields are removed. You can use this action, if you want to delete the X-header fields defined previously on other servers.











8 Toolbar buttons

Button	Description
	Back
	Forward
	Up one level
	Refresh
	Properties of the selected object
	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

9 Icons reference

Icon	Description
	Avira Exchange Security Management 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 Exchange Security address list (red collar), supplied with Avira Exchange Security 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 Exchange Security servers. Servers can be added, removed and configured. The shared properties for all servers are configured under General Settings > Avira Server Settings or, alternatively, by right-clicking on Avira Server > Properties . These include the standard email addresses and internal domain(s)

Icon	Description
	General Avira Server Settings under the General Settings node in the right-hand window.
	A single server, configurable under Properties
	Folders and Utility Settings. The quarantines are found under Folders 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 quarantine folders contain original mails for inspection. Detailed information can be retrieved for every email.
	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 Avira 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 Avira job or Avira Email Filter job, which can have various job types, configurable under Properties

Icon	Description
	An active job, configurable under Properties
	An inactive job, configurable under Properties
	The Avira Monitor for viewing all quarantine folders on each available server. The quarantine folders contain the copies of the original emails, including the attachments.
	A single quarantine item
	Invalid quarantine item
	Resent quarantine item
	Information store for quarantine item
	Time and day of quarantine update
	Folder for different Avira reports delivered with Avira Exchange Security
	Individual Avira report

10 Support information

Support service

All necessary information on our comprehensive support service can be obtained from our website:

www.avira.com/en/support

FAQs

You can also read the [Knowledge Base](#) on our website. Your questions may already have been asked and answered by other users in this section.

Please contact your Avira Partner - they will be more than willing to help you with any further questions regarding Avira products.

Contact address

Kaplaneiweg 1, 88069 Tettnang, Germany

Internet

You can find further information about us and our products at the following address:

www.avira.com

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 Operations GmbH & Co. KG.

Issued Q4-2013

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.*[™]