Avira Server Security

HowTo

AVIRA

Table of Contents

This document shows you the ideal approach on how to install and configure Avira Server Security. It contains important and helpful settings and recommendations of the Avira Support for the configuration of the program. Furthermore you find useful hints, e.g. the procedure in case of a virus attack.
You can find all installation files and product manuals as PDF-documents on our website:

http://www.avira.com/en/support-download

1. Setup Modes

Once you have downloaded the installation file of Avira Server Security, start the setup file “avira_server_security_en.exe”.

If you have downloaded the zip package, extract the files to a separate directory, navigate to the directory “en-us” and start “setup.exe”.

Now the assistant appears. Then, click on *Next*. You have the option to choose the setup type:

1.1. Complete

Avira Server Security is installed completely with the service Avira Server Security and the console Server Security Consoles. You can’t select a target folder for the program files.

1.2 Custom

You can decide if you want to install the service Avira Server Security and/or the Server Security Console.
You can install the Server Security Console on a workstation so you have the option to reach the server service by remote access.

Note
Installation of the service Avira Server Security: If you want to reach the protected server with the Server Security Console by remote access, make sure that the following ports have been opened:

139 (NetBIOS SSN)
137 (NetBIOS NS)
138 (NetBIOS DGM)

You can choose a target folder for the program files that need to be installed.
Then, the dialog window “Install license” appears. Choose the directory where you have saved the license file (hbedv.key). You can also test the Avira Server Security

for 30 days.

Thereafter, the installation will start.
It is possible that the installation of the Microsoft Visual C++ 2008 will also start in case the kit hasn‘t been installed before.

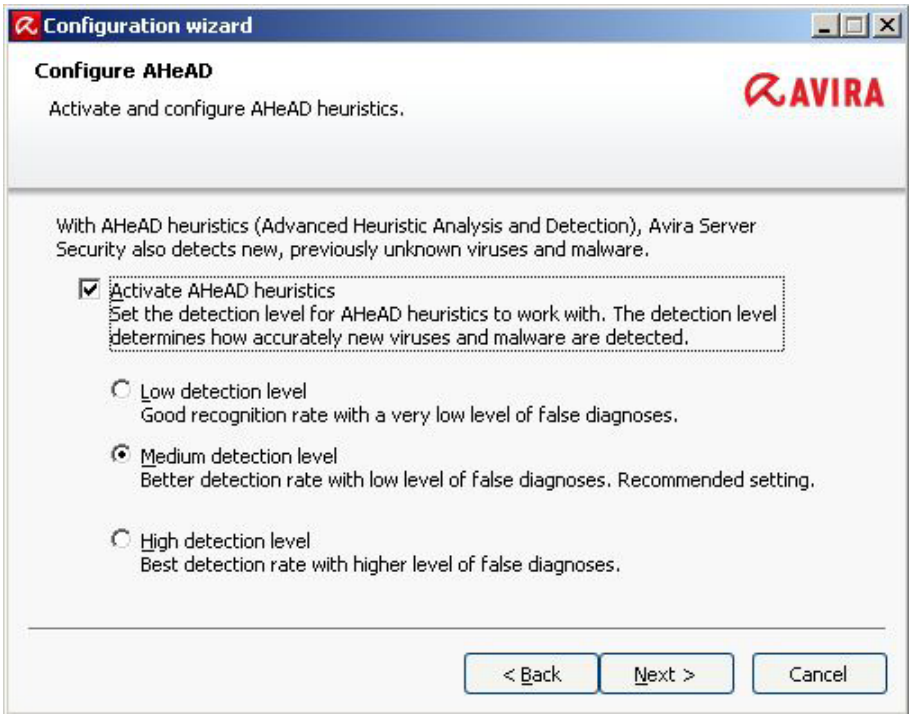
Note
Avira Server Security uses runtime libraries of the Microsoft Visual C++ 2008 – re-distributable kit. The installation of Microsoft Visual C++ 2008 - redistributable kit is required for the usage of Avira Server Security.

The link for the downlad of the redistributable kit is:

http://www.microsoft.com/download/en/details.aspx?id=5582

As soon as you have finished the installation, the configuration assistant appears. The assistant guides you through the basic settings of the Avira Server Security.

In the following dialog window you will be able to configure the engine and the de-tection level of the AHeAD technology. The chosen detection level is applied to the settings of the AHeAD technology of the scanner (direct scan) and the Real-Time Protection (on access scan).

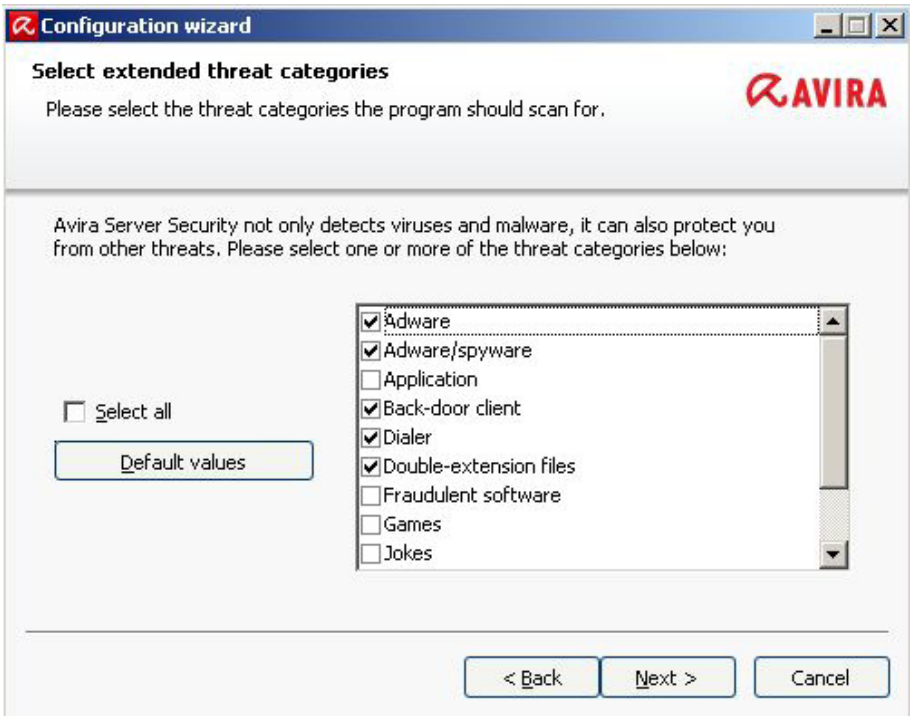


Note
Please be aware that a high detection level detects a large quantity of unknown malware, but it also increases the risk of false positives.

What does heuristic mean?

Heuristic is a method of detection that is able to detect unknown viruses. A profound analysis of the code looks for functions which are typical for viruses. In case the examined code has suspicious characteristics, the suspicious file will be indexed by Avira. It doesn't mean that the code is really a virus, since false positives are a possibility.

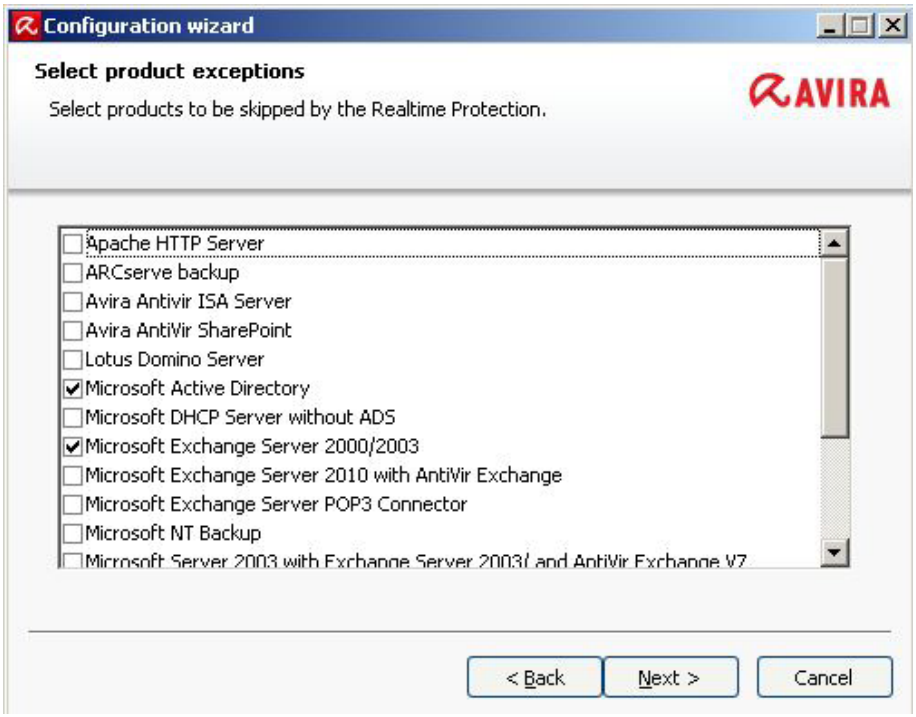
In the following dialog window you can select the extended threat categories.



These options are activated by default as the risks of adware/spyware and back-door control software, phishing and dialers are very high. However, many administrator tools are detected by Avira as "Security Privacy Risk". Avira cannot distinguish if a suspicious program is used intentionally by an admin. This is why we excluded application, SPR and games from the default settings.
You can find an overview of all threat categories and their meaning in the chapter Quick Tips at the end of this document.

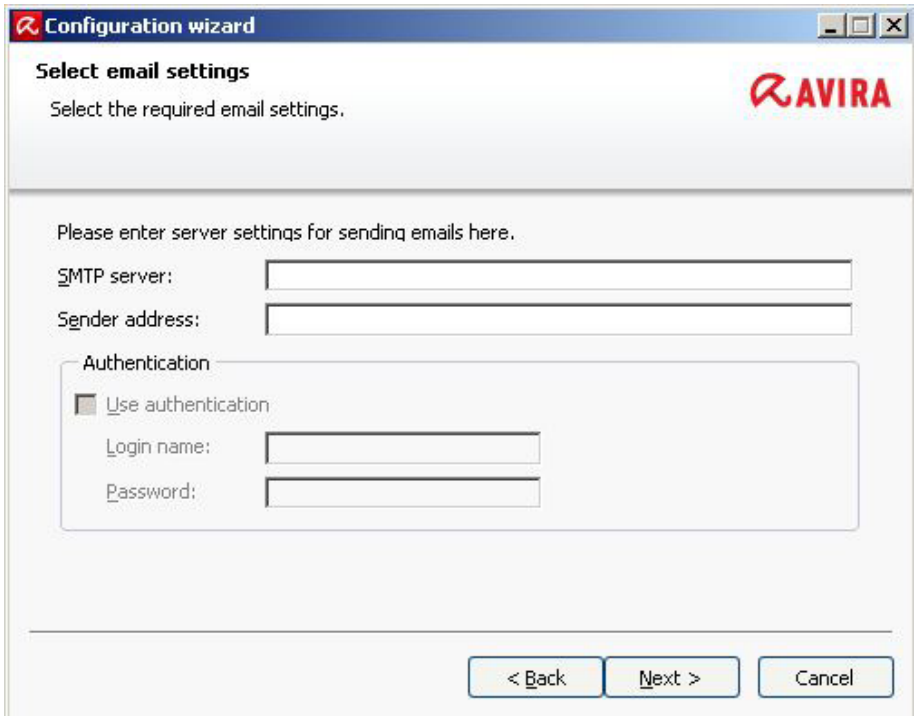
Afterwards, please select the products that you do not want to be monitored by the Real-Time Protection (on access scanner). Thus you can avoid losses of performance and side effects which can be caused by the Real-Time Protection.

Most programs are already predefined by Avira. In case you should use one of these programs, please exclude it from the scan by marking it.



In the next configuration dialog you can choose the settings for the email notifications. Server Security uses emails via SMTP to send warnings from the different modules Real-Time Protection, Scanner and Updater.

In case you don’t know the address of your SMTP server or you don’t want to use this option you can leave these boxes empty.



2. Configuration

2.1 Update configuration for the Avira Update Manager

In case you want to use several installations of Server Security or Professional Security in your network and update them from a central location, you can do that by means of the free module “Avira Update Manager”.
This is very helpful in case only one computer should have access to the internet but you want to update the virus definition files on all your computers in the network. Furthermore, you limit the traffic and you don’t burden the internet connections unnecessarily.

You can find the necessary tool in the following link:

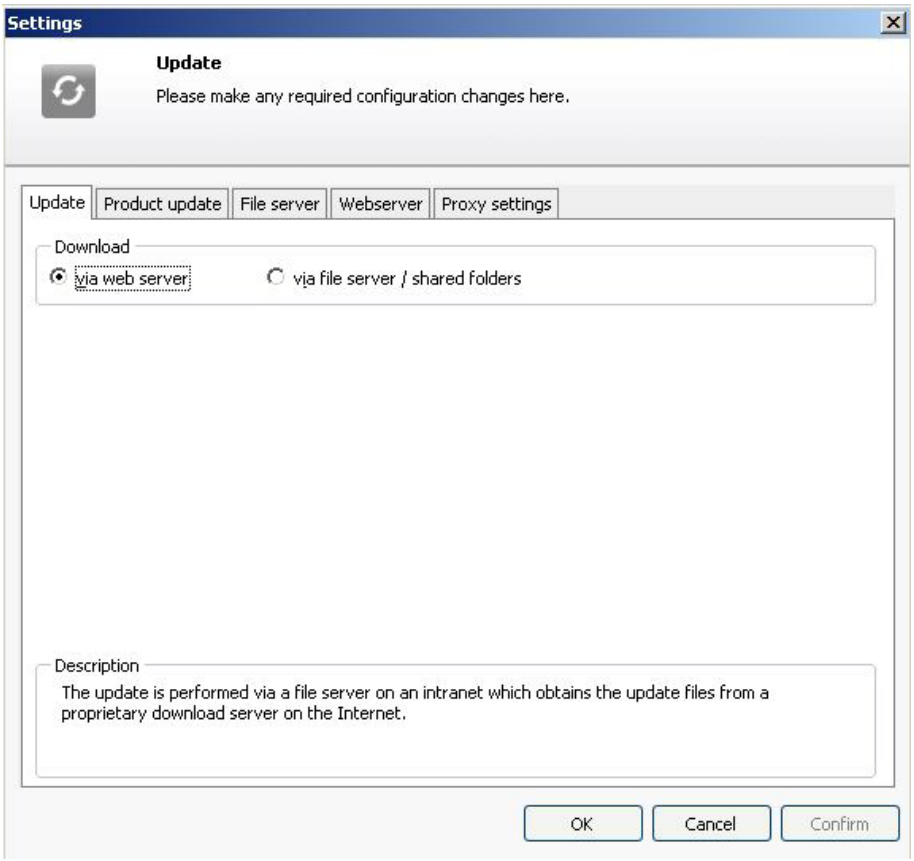
http://www.avira.com/en/support-download-avira-server-security

You can install this software on a common workstation or on a server. In case of an installation on a workstation, keep in mind that only 10 network connections are possible at one time. You will find detailed information about the installation and configuration of the Avira Update Manager in the corresponding manual, which is available at the link above.

After the installation of the Avira Update Manager and the configuration, the virus definition files of the Avira Server Security are downloaded at the scheduled intervals and saved into the root directory.
As the Avira Update Manager provides an integrated web server with the port 7080, all workstation in the local network can connect to this directory and load their updates there.

In order to configure the Avira Server Security, please, proceed as follows:

Open the configuration of the Avira Server Security.
Go to the menu point “Settings” and “Update”. Choose “Download” and the option “Via web server”.



Afterwards, go to the menu item “Webserver”. Here you have two options, “Priority server” and “Default server”.

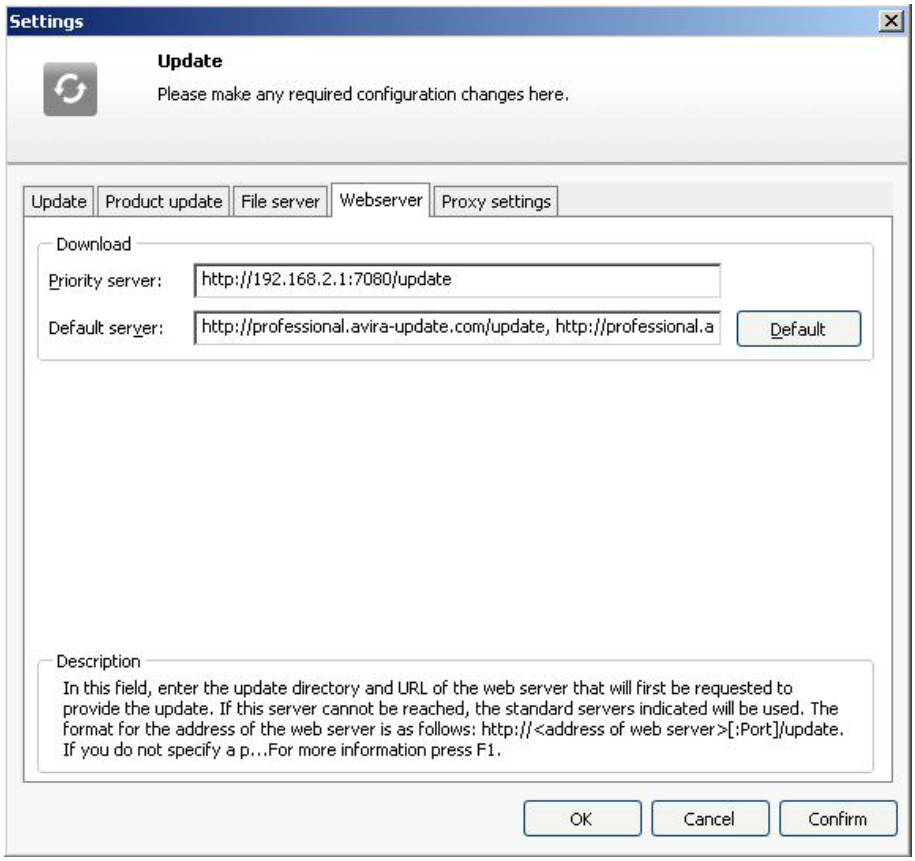
Initially, Avira Server Security will try to contact the priority server. In case there is no connection to the priority server available, Avira tries to establish a connection with the default server.
Therefore, the function “Priority server” should be used for the updates via the Avira Update Manager (AUM). This is very useful if notebooks are used in the enterprise network that need to be updated as well when they are outside the network.

In case the AUM computer is offline, the Avira Server Security contacts the default server automatically if you have configured the priority server (AUM address) and the default server (Avira download server).

The following information should be entered into this box:

http://[IP-address of AUM computer]:7080/update

Example:
http://192.168.2.1:7080/update



You can change the port of the Avira Update Manager if this port is already occupied in your network. Double-click the navigation menu of the Avira Update Manager on the corresponding server (default setting: “localhost”) > *Settings* > *Networks*. Here you can change the port of the server from 7080 to the required port.

The settings for the update configuration of the Avira Professional Security need to be changed accordingly.

It is important that the chosen path is enabled in the entire network and in each firewall of the workstations.

2.2 Configuration of product updates

You will find the item “Product updates” in the configuration settings of the update of Avira Server Security. Avira provides you with updates of the software in irregular intervals in order to correct program malfunctions or to offer new functions.
If you set automatic program updates here, keep in mind that a server reboot might be necessary. That reboot is automatically triggered by Server Security.

You can avoid this forced reboot by selecting the notification in case of product updates. You can configure that by navigating to the menu item of *Server Security Settings* > *Update* and the options in the menu point “Product updates”.

Afterwards, you can schedule when the product updates should be installed, e.g. in a time period when the server can be rebooted without causing any inconveniences.

2.3 Setting exceptions

Avira Professional Security is connected directly to the operating system. Especially the module Real-Time Protection scans all files during the real-time scan at each write or read access. It is therefore recommended to exclude special programs and their processes from the scan.

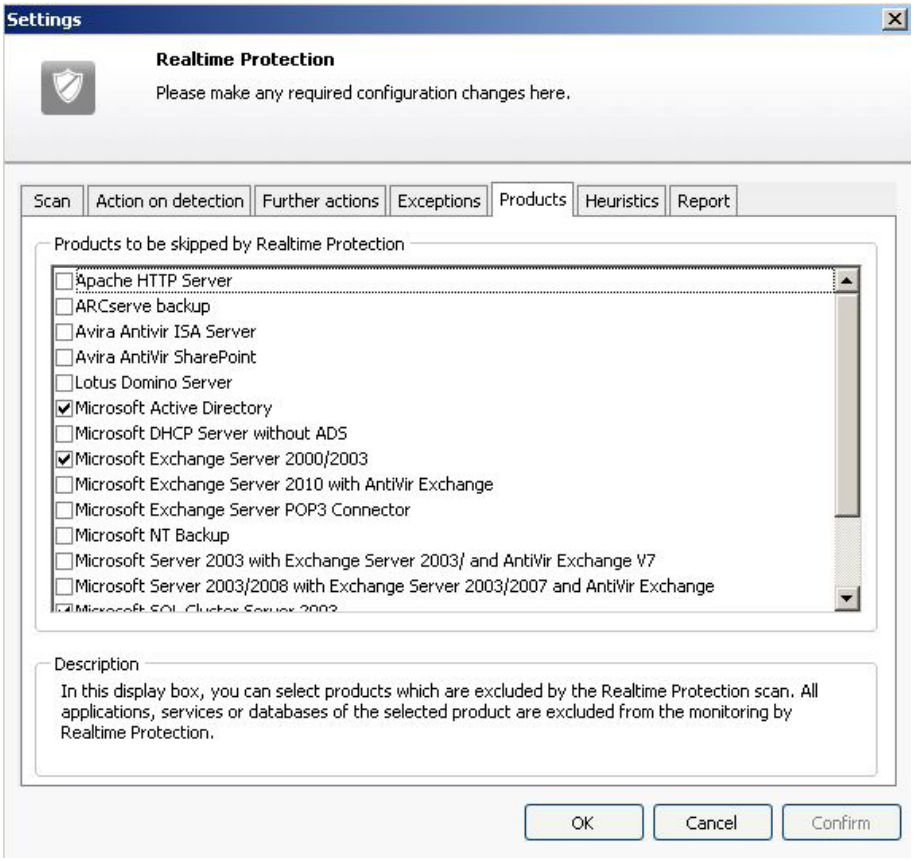
This affects e.g. all programs that run a database in the background like accounting programs, financial software, mail server or web server.

Furthermore, special backup programs are also concerned that require a data backup of your systems. During a backup a read access is made of all files of the computer and the Real-Time Protection constantly scans each file which is saved by the backup program. This can affect the performance of your computer.

In order to prevent a slowing down of your system and exclude the concerning programs from the scan, please proceed as follows:

- Start the configuration of Avira Server Security
- Go to the menu “Settings”
- Open the menu item “Real-Time Protection”
- Choose here the item “Products”

In the menu „Products“ you will find the programs that have already been predefined by Avira. These programs can cause a loss of performance if they are not excluded from the scan. In case you should use one of these programs, please exclude those from the scan by marking them.



In case you should use a special backup software or another software working with a data base that is not listed, please go to the item “exceptions”.
In the menu “Processes to be omitted by Real-Time Protection” you have to enter the paths of the program folders where the concerned software is installed. It is important that the entered path is followed directly with a “\” so that Avira recognizes the path as a directory and not as a file.

An example for a correct path entry: C:\ProgramXY\

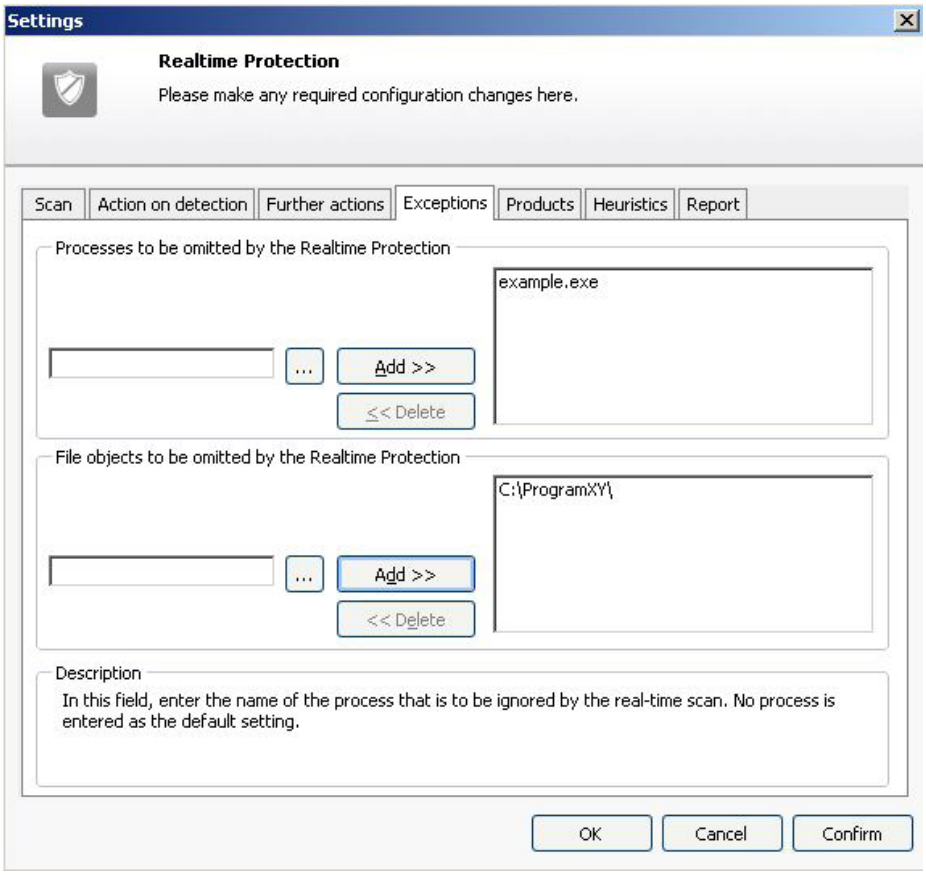
Furthermore, it is important to exclude also the processes of the excluded software from the scan.

These running processes like e.g. backup software, initialize accesses to files. In case the process itself is not excluded, the Real-Time Protection scans every read access.

This is why you should use the task manager to find out which processes are used by the software. Enter those into the dialog “Processes to be omitted by the Real-Time Protection”.

An active process, e.g. of a backup program needs read and write accesses to the hard disk. The Real-Time Protection would scan all these accesses if the process is not excluded from the scan. In case only the program directory is omitted by the

Real-Time Protection scan the Real-Time Protection will not be active in this directory. But this doesn't concern all active processes in the task manager.



It is also important for the execution of the scan to exclude the program folders of the corresponding software from the scanner. This can be done in the menu *Scanner* > *Scan* > *Exception*.

3. Jobs in the scheduler

The Avira Server Security offers an integrated scheduler for one-time or regular jobs, like e.g. updates and scans.
You should enter the settings for this scheduler after the installation, so that updates and scans are proceeded automatically.

Start the Avira Server Security GUI and select the point “Scheduler”. Click in the task bar on “Create new job using wizard”. Define a name (e.g. internet update or weekly scan) and a short description for the job.
Choose the kind of job (in case of an update choose “Update job”, in case of a scan choose „Scan job“).

In case of a scan job you can choose the profile which should be used for the scan. You find further information about scan profiles in chapter 4 of this document.

Afterwards, configure when the job should be executed. (e.g. immediately, daily, interval, single).

Please check if the job is shown as “Ready” in the overview.

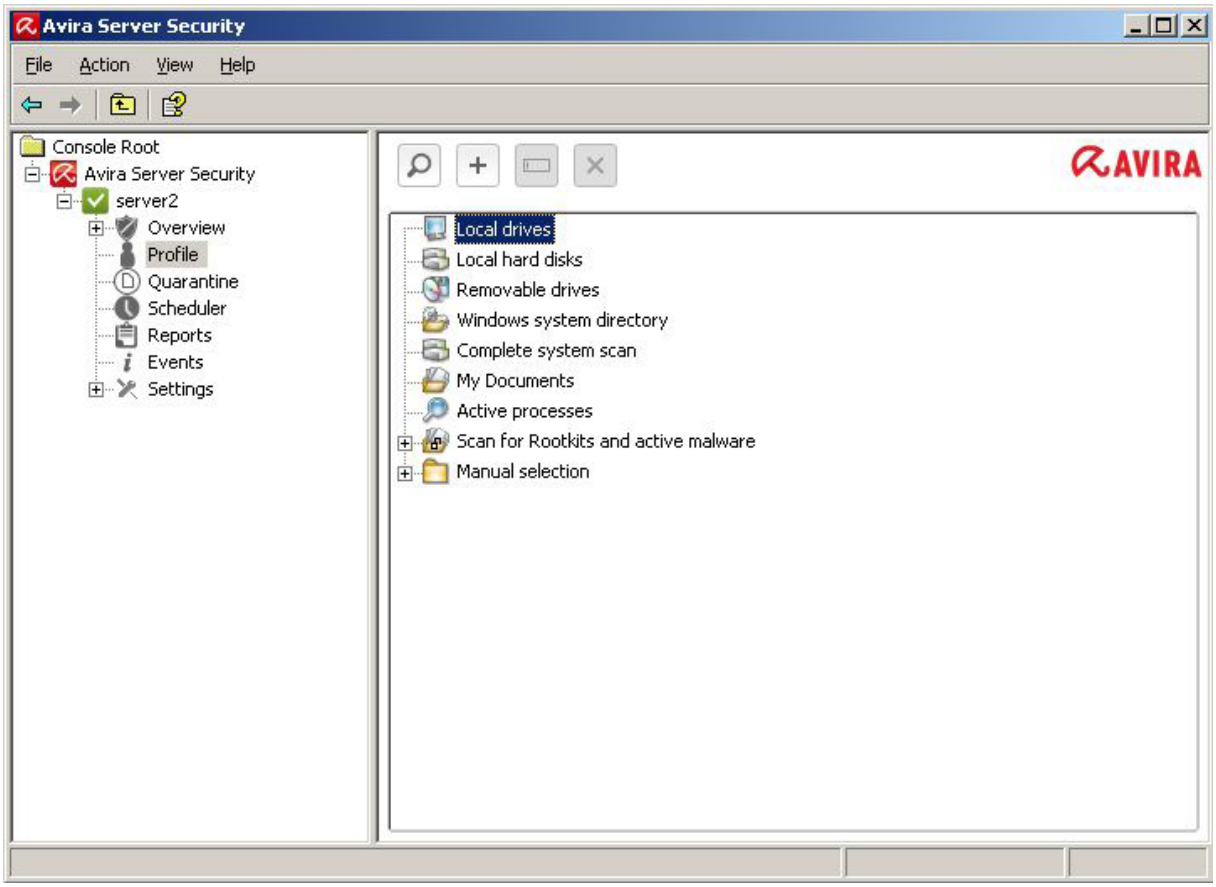
We recommend an hourly update and a weekly scan.

We produce about 5 updates daily of our virus definition files and/or the engine. With an hourly update you can make sure to benefit from these security updates.
The weekly system scan is also important for your security. Very frequent system scans could cause a loss of performance. Large time periods without scans might increase the risk of viruses on the PC which could be detected after the scan.
If you make an update after a gap of several weeks or months, Avira can detect a virus which might have already been active for a certain time on the server in case the Real-Time Protection hasn’t already found it.
Therefore, a weekly system scan is a good balance between low system load and an optimum of security of the system.

4. Different scan profiles

In case of a possible virus attack or a general control, Avira offers predefined scan profiles and the possibility to create individual scan profiles. Using those profiles, you can make the virus scan more effective by scanning only special sectors, drives or directories of the system.
Below, we would like to give you an overview of the predefined scan profiles and the possibility to adapt the scan to your individual demands.

You can find the profiles for the scan in the menu “Profile” beneath in the control menu of Avira Server Security.



Which scan profile is the best depends on which data need to be checked or excluded from the scan.

In case of a virus attack that can be located on the local drives, the profile “Local drives” shortens the scan considerably. The profile “Local drives” also scans cd drives and removable media.

New unknown USB sticks that get connected with the PC should also be checked. As a complete system scan is not necessary, you can use the profile “Removable Drives” in order to make sure that there are no viruses on removable media.

In case of a virus attack, you can check if a virus is already running. The scan profile “Active Processes” looks for active processes.

The following list shows an overview of the predefined profiles and different scenarios when they should be used:

Scan profile	Explanation	Scenario
Local Drives	This profile checks all local drives.	In case you don’t know on which drive a virus is.
Local Hard Disk	This profile only checks the local hard disk on your system.	If you are sure that the virus is on the local hard disks and not on removable drives and you want to check the local hard disk directly.
Removable Drives	This profile checks all available removable drives.	If you want to make sure that a removable drive is not virulent.
Windows System Directory	Checks only the system directory of Windows (C:\Windows\System32)	If you want to make sure that the system files of Windows are clean. Many viruses write themselves into the system directory. This is a first important check if you suspect a virus attack.
Complete system scan	Makes a complete check with special scan options and will be synchronized with the GUI (server overview).	In case you don’t know if there is a virus attack and where it might be.
My Documents	Scans the folder “My Documents” of the user who is signed on.	Windows saves downloads and similar files into “My Documents”. Therefore you can look here for viruses first.
Active Processes	Scans all running processes.	Check if there is a virus among the running processes.

In order to adjust the scan for special drives and directories you can use the default profile “Manual Selection” or you can create individual scan profiles.

5. Quarantine

If a virus or a suspicious file is found during a scan, the file is moved to the quarantine, depending on the setting. The file is packed into the especially encrypted format (*.qua) and moved to the quarantine directory INFECTED on your hard disk, so that no direct access is possible anymore.

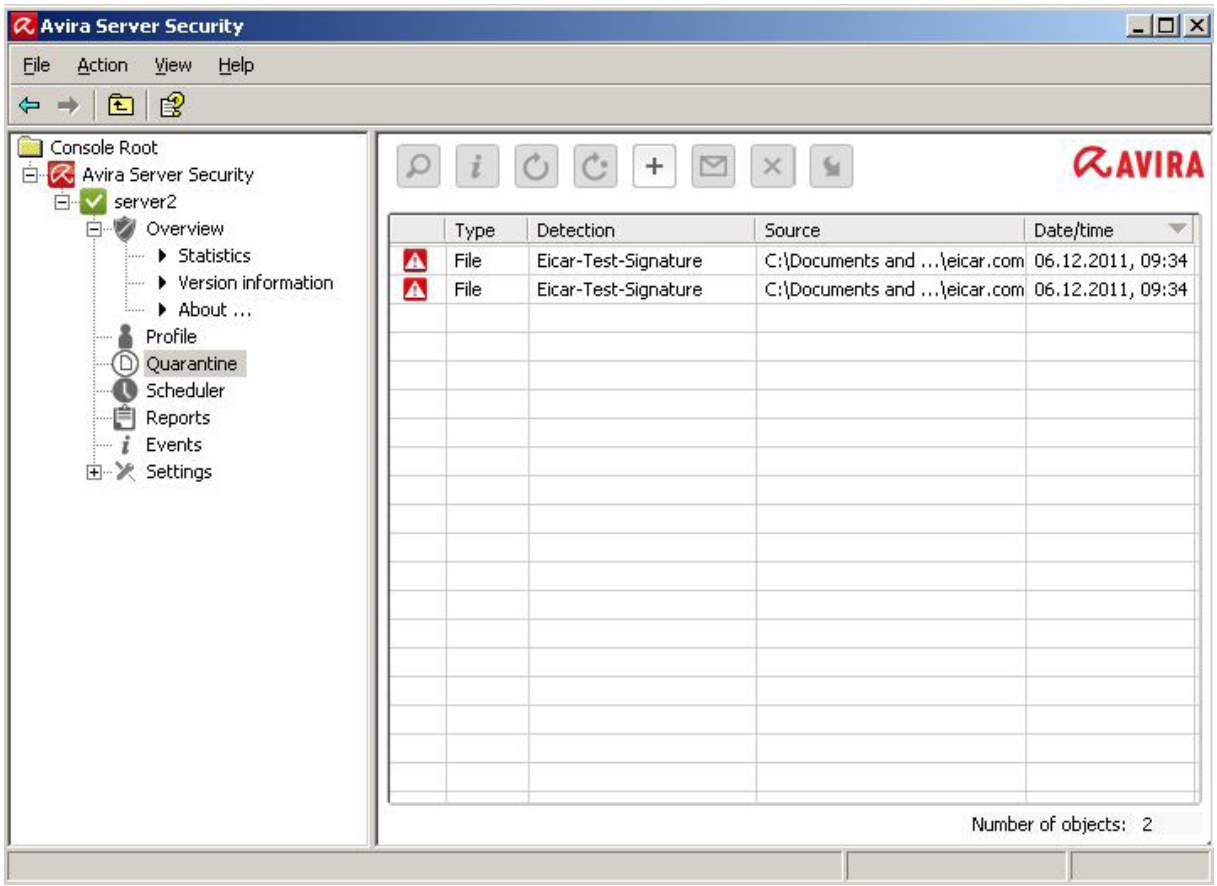
This directory by default located in Windows 2000/2003 server at:

C:\Documents and Settings\All Users\Application Data\Avira\AntiVir Server\infected

In the case of Windows Server 2008, it is located here:
C:\ProgramData\Avira\AntiVir Server\INFECTED

The files in this directory can be repaired later in the quarantine manger or they can be sent to the Avira Malware Research Center, if necessary.

You can get to the quarantine administration of the Avira Server by starting the Server Security GUI and selecting the menu item “Quarantine”.



Note
In the following cases, we recommend an analysis by the Avira Malware Research Center:

Heuristic Detection (suspicious files):
A scan has detected a suspicious file. It has been moved to the quarantine. An analysis of the file has been recommended by the Avira Malware Center in the Windows dialog of the virus detection or in the report file.

In case of heuristic detections the name of the detected file begins with “HEUR/…” in order to show a detection of the Advanced Heuristic Analysis and Detection (AHeAD) or ends with “.gen” if it is a generic file.
A generic detection routine is used in order to detect common characteristics of different variants.
The generic detection routine has been developed in order to detect unknown variants of already known viruses and is being continously enhanced.
In case of a heuristic detection of the AHeAD the file is suspicious because of its behavior. It is possible that the file is not a virus but it might be a new unknown virus. Therefore, the files should be sent to Avira for analysis.

Suspicious file:
You think a file is suspicious and you moved it to the quarantine. But the check of the file for viruses and malware is negative.

False positive:
You are quite sure that a detection is a false positive: Avira Professional Security detects a file which is very unlikely to be malware.

Note
The size of the file is limited to 20 MB unpacked or 8 MB packed.
You can upload several files by marking all files you want to upload and by clicking on the button “Send object”.

You should also scan the suspicious files after a few days (between 5 and 10) with the latest virus definitions (press “F2” or right click and “Rescan object”). If the files are detected again, they are very likely to be real viruses and should be deleted. If they are not detected as malware they have been false positives and can be restored.

6. Quick Tips

6.1. Procedure in case of a virus attack

If the Real-Time Protection or the scanner should detect a virus on your system, you should scan the whole system for infected files. As many programs have exclusive read and write access on different files, a scan in safe mode is reasonable.
As the safe mode is not available on server operation systems we recommend you to boot with our rescue CD and to clean the PC with this CD in case of a definitive attack.

You can find the rescue CD at the following link:

http://www.avira.com/en/support-download

6.2. Manual insertion of the license file

After renewing the license you can copy the license file (hbedv.key) directly into the main directory of Avira. (C:\Program Files\Avira\AntiVir Server).
You can also enter the license file in the server console by clicking on Server Security with the right mouse button and choosing the point “Update license file”.

6.3. Keeping the configuration for several installations

You can install the Avira Server Security on several PCs and use a defined configuration on all the PCs by means of the “avnetnt.ini”. You can find it in the following path:

Windows Server 2003:
C:\ Documents und Settings\All Users\Application Data\Avira\AntiVir Server\config\avnetnt.ini

Windows Server 2008:
C:\Programm Data\Avira\AntiVir Server\config\avnetnt.ini

You can copy this file afterwards from one PC to another and set the configuration (it is necessary to deactivate the process protection and the Avira services).
Or you enter the path to the avnetnt.ini via the command line during the installation e.g. in case of a logon script. The avwin.ini is imported during the installation.
You can find more detailed information about that in the Server Security manual in the chapter “Command line parameters for the setup program”.

6.4. Extended threat categories

Dialer programs for chargeable numbers (Dialers)

Installed on a computer, these programs – shortly called dialers – establish a connection using a premium rate number that has high discrepancies in pricing.
Some dialers replace the default EDI connection from the Internet user to the ISP (Internet service provider) and call for each connection a chargeable and usually very expensive 0190/0900 number.

Games
Research has shown that the working time used for computer games has reached an economically significant dimension. Therefore, more and more businesses want to keep workstations clear of games.

Jokes
Joke programs only want to scare or amuse people without being really dangerous. But be careful! Characteristics of joke programs can also originate from a virus or Trojan.

Security Privacy Risk (SPR)
Software that endangers the security of your system and doesn't process the desired program activities. It invades your privacy or spies on your user behaviour and is therefore not wanted.

Back-door client (BDC)
In order to steal data or manipulate computers, a back-door server program infiltrates using the "back-door" so that the user usually doesn't become aware of it. This program can be controlled by a back-door control software via the Internet or network.

Adware/Spyware
Software that displays advertising or sends the user's personal data to a third party is usually unwanted.

Unusual runtime compression
Files that have been compressed using unusual run-time compression can be regarded as suspicious.

Double-extension files
Executable files that hide their real extensions in a suspicious way can be malware.

Phishing

Phishing also known as brand spoofing, is a clever kind of data theft which targets customers or potential customers of Internet service providers, banks, online banking services and registry authorities. By forwarding your email address on the Internet, filling out online forms or joining newsgroup and websites, you enable so-called “Internet crawling spiders” to steal your data that can then be used for fraud or other crimes.

Application (APPL)

This is an application that may pose a risk for the user and has a suspicious background. Avira Professional Security detects “Application (APPL)”. If you have chosen this option in the extended threat categories, you will receive a warning if Avira Professional Security detects such a behavior.

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 Q4-2011

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.

AVIRA

live free.™

© 2011 Avira Operations GmbH & Co. KG. All rights reserved.
Errors and technical modifications are subject to change.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

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