Avira Professional Security

HowTo

AVIRA

Table of contents

1. Setup 3
   1.1 Web loader 3
   1.2 Complete Installation Package 3

2. Configuration 10
   2.1 Installing modules / uninstalling modules 10

3. Creating jobs in the scheduler 18

4. Different scan profiles 20

5. Quarantine 22

6. Avira FireWall 24

7. Quick Tips 26
   7.1 Procedure in case of a virus attack 26
   7.2 Web-Filter of the Web Protection 26
   7.3 Reset LSP in case of problems with the Web- and Mail Protection 26
   7.4 Protocols which are checked by the Mail Protection 27
   7.5 Manual insertion of the license file 27
   7.6 Keeping the configuration for several installations 27
   7.7 Extended threat categories 28

This document will support you to install and configure Avira Professional Security in an optimal way. It contains important and helpful configuration possibilities and recommendations of the Avira Support. Also the provided tips e.g. for procedures in case of virus attacks are very useful.

You will find all necessary files for installation and the manuals as PDF files ready for download on our website.

1. Setup

On our website you will find two setup packages. The so-called web loader with approx. 800 KB and the complete installation package with approx. 45 MB.

1.1 Web loader

The web loader downloads all the up-to-date program files from the web servers before the installation is executed. This procedure guarantees that Avira Professional Security is installed with the up-to-date virus definition files.

1.2 Complete Installation Package

The installation package contains the installation program as well as all necessary program files. This installation package doesn't offer a language selection for the Avira Professional Security. So you have to select our English website first.

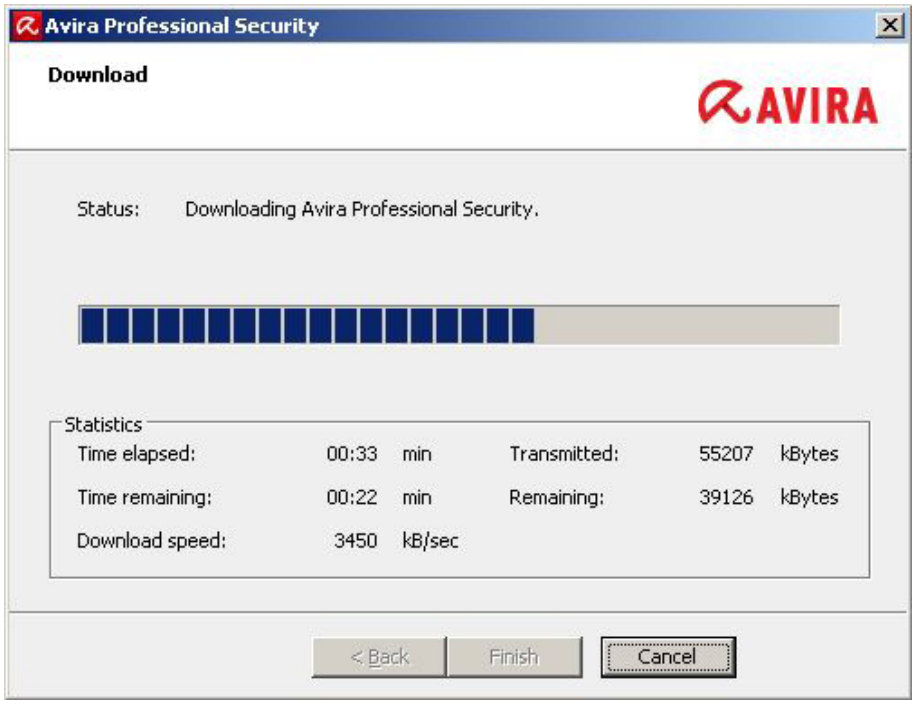
On the English website the corresponding software package is offered. Here, the included files might not be up-to-date.

We recommend an update immediately after the installation to make sure that all the files are up-to-date.

After having downloaded the installation files of the Avira Professional Security, please first start the installation of Avira Professional Security with a double-click: (*avira_professional_security.exe* or *avira_professional_security_en.exe*)

Please click on *Next* in the menu of the assistant that appears afterwards. In case you have chosen the web loader you can now select the language version you need.

Now the web loader downloads the necessary program files and virus definition files.



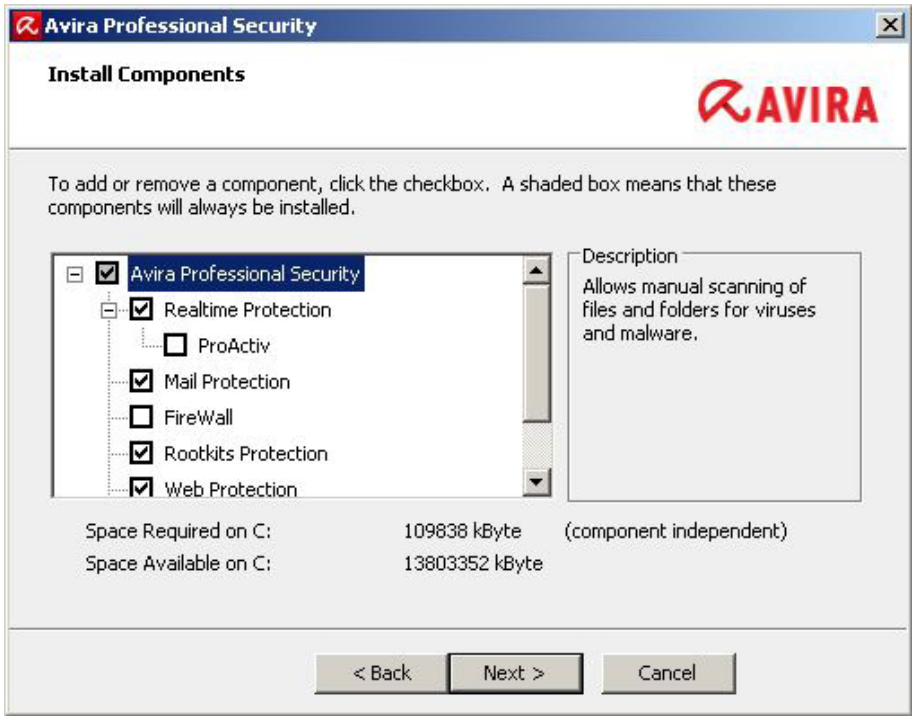
Afterwards, you can choose a setup type:

Express:
- Avira Professional Security will be installed completely with all program components (modules)
- The program files are installed in the given default directory: *C:\Program Files\Avira\AntiVir Desktop*

Custom:
- You can choose a target folder for the program files which have to be installed
- You have the possibility to choose program components / modules for the installation
- You can deactivate the creation of a desktop icon and a program group in the start menu

In the custom setup you can choose the following modules.

- **Realtime Protection** (permanent scanning of all file accesses in real time)
- **ProActive** (detection of attacks and unknown malware)
- **Mail Protection** (permanent scanning of all incoming and outgoing emails (POP3, IMAP, SMTP) including attachments)
- **FireWall** (Rule-based control over incoming and outgoing Internet traffic)
- **Rootkits Protection** (detection of potential rootkits)
- **Web Protection** (permanent protection against viruses and malware via browser)
- **Shell Extension** (direct scanning of files and directories in the Windows Explorer)



Avira ProActive is a new behavior-based detection technology developed by Avira which has been integrated since version 10. ProActive protects your computer against new and unknown malware that hasn‘t been detected yet by virus definitions and heuristics.

Avira ProActive monitors the system in real time and detects attacks as soon as they are started. Sensors are continuously supervising the system and are looking for unusual behavior. The ProActive component uses rule sets in order to identify malicious behavior. These rule sets have been developed by the Avira Malware Research Center and are constantly provided with new data by the Avira data base.

Avira ProActive sends information about detected suspicious programs to the data base. You have the possibility to deactivate this data transfer to the Avira data base. In case a program shows a malicious behavior, it is treated and reported just as malware.

Note
The ProActive Technology is not yet available for 64 bit systems

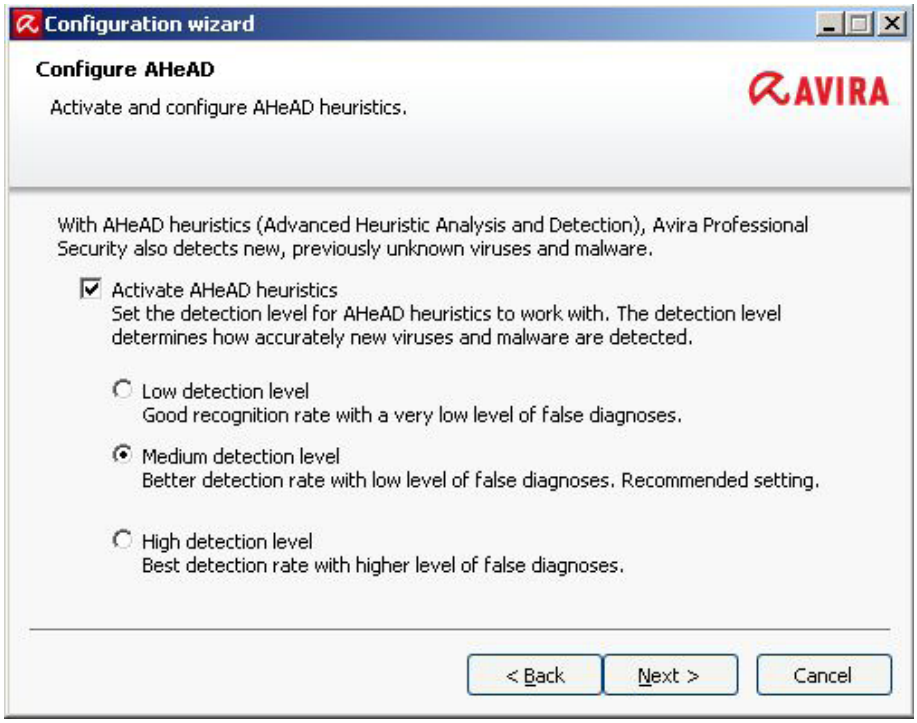
The Mail Protection is needed if you receive and send your emails via POP3, SMTP or IMAP.

You can delete the module Mail Protection in case one of the following prerequisites is met:

- If you have the email traffic already scanned on an email server, e.g. by AntiVir Exchange or AntiVir MailGate
- If you receive emails via web access. This means e.g. you get your emails directly on gmx.com or web.com etc.
- You protect yourself against viruses and malware which are downloaded on your computer from websites with the Web Protection.
- The Web Protection can be deleted as a module, if the http traffic is already scanned, e.g. by AntiVir ISA Server or AntiVir MailGate

Afterwards, the window “Install license” appears.
Choose the directory where you have saved the license file “hbedv.key”.
As soon as you have finished the installation, the configuration assistant appears.
The assistant leads you through the basic settings of the Avira Professional Security.

In the next dialog window you can configure the engine and choose the detection level for the AHeAD technology. The chosen detection level is used for the settings of the AHeAD technology of the scanner (direct scan) and of the Real-Time Protection (real-time scan).

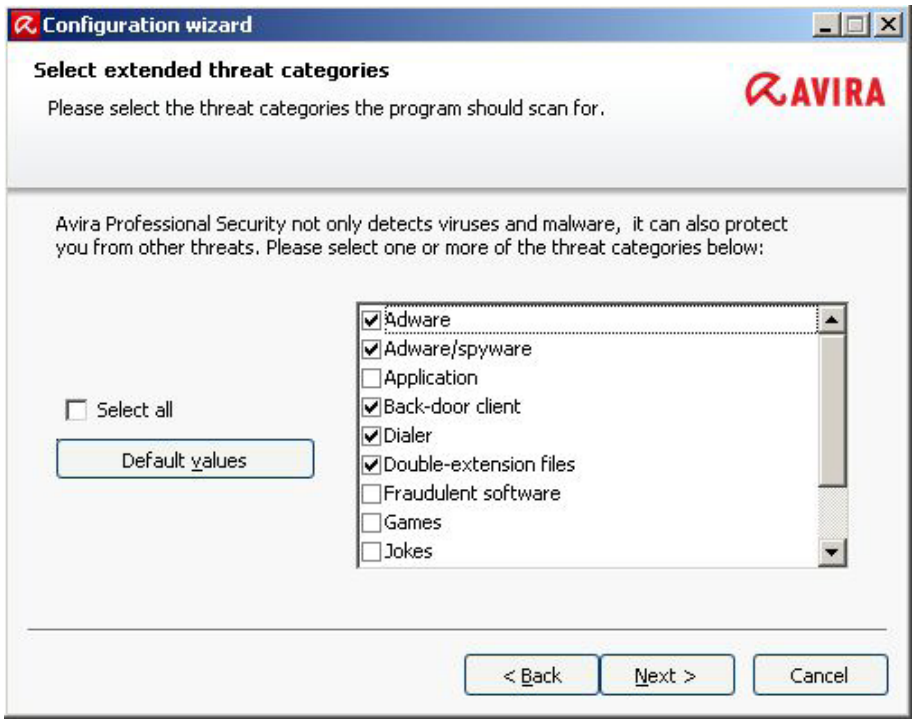


Note
Please be aware that a high detection level detects a large quantity of unknown malware, but also increases the risk of false positives.

What does heuristic mean?

Heuristic is a method of detection which 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, Avira indicates the suspicious file. This doesn't mean that the code is really a virus, but false positives are possible.

In the following menu you can choose the extended threat categories, which will be detected:

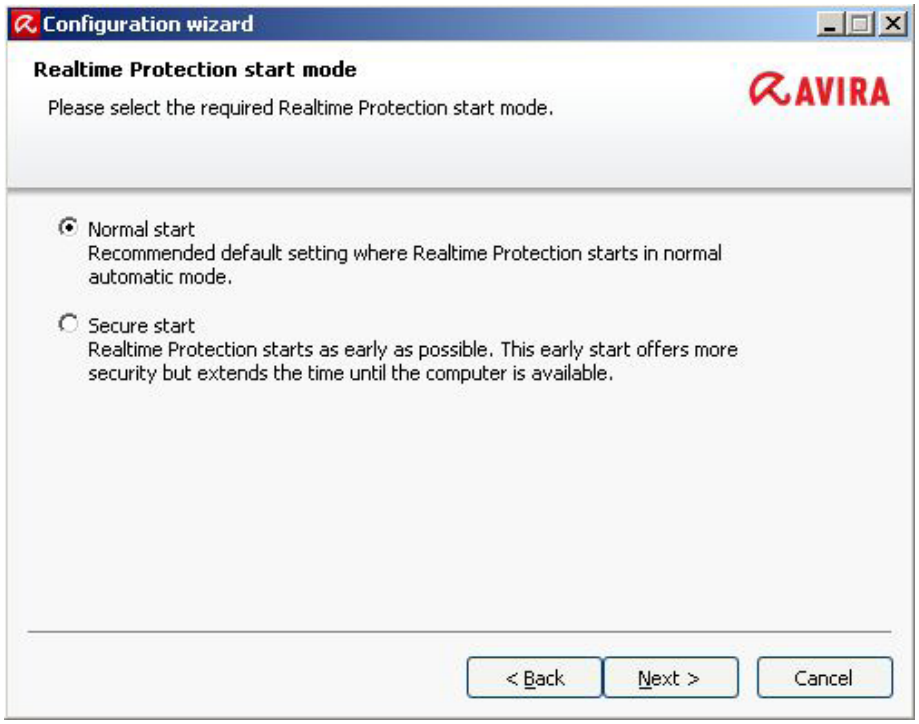


- These options are activated by default as the risks of adware/spyware and back-door control software, phishing and dialers are very high. However, many administrator tools are detected by Avira as "Security Privacy Risk". Avira cannot distinguish if a suspicious program is used intentionally by an 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 quick tips at the end of this document.

Please choose the start mode of the Real-Time Protection afterwards. You can choose between the normal and the safe start.

Using the "normal" start, the Real-Time Protection gets started in the normal, automatic mode. This is the recommended start mode.



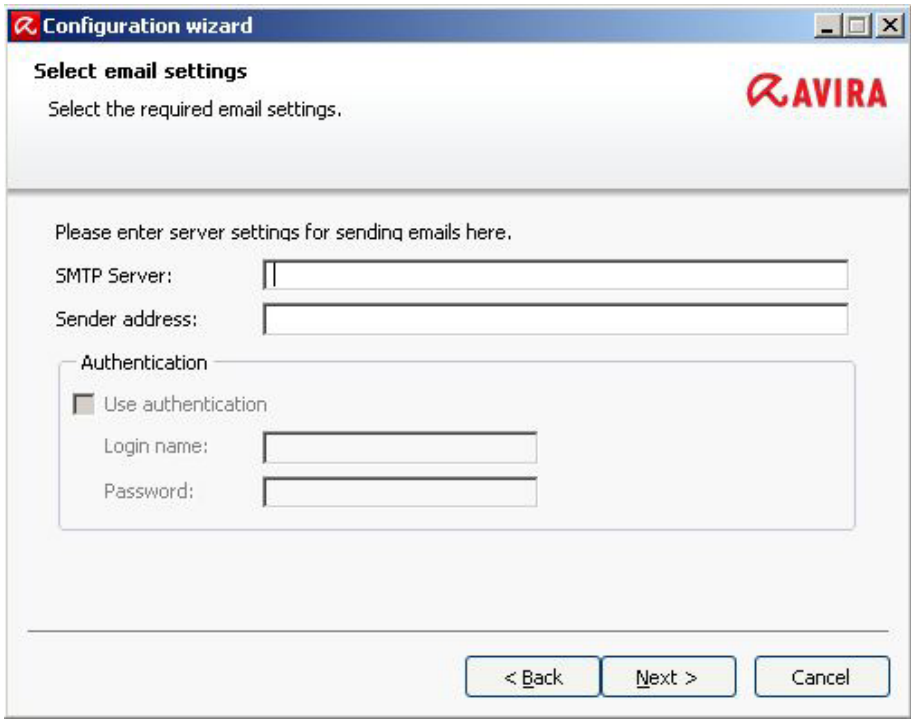
Using the “safe start”, the Real-Time Protection is loaded as soon as possible. This increases the security level but the start needs more time.

Some viruses are loaded directly with the operation system. So they might be already active before the Real-Time Protection is loaded.

Using the safe start, the Real-Time Protection is started at first. The start of the other component will not be continued until the Real-Time Protection is loaded completely and functions. So there is more time needed for the system start.

In the following configuration dialog, you can enter the server settings for the emails.

Avira Professional Security forwards its emails via SMTP in order to send email alerts 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 the relevant fields empty.



Afterwards, you can choose the option “Short system scan after installation” in order to scan your computer directly after the installation.

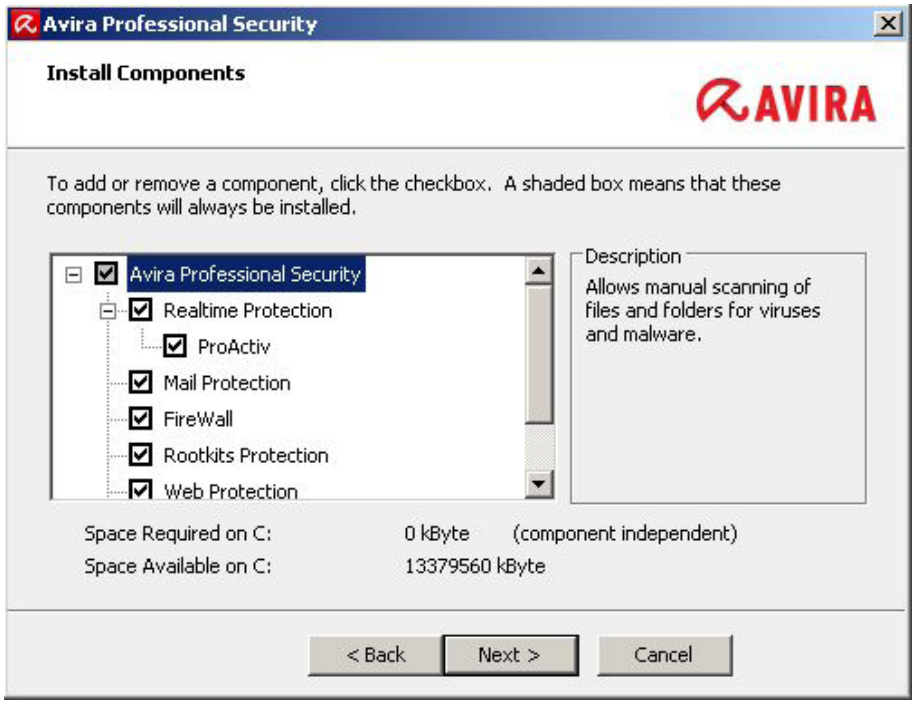
2. Configuration

2.1 Installing modules / uninstalling modules

Different modules can be chosen for the installation, to be added or deleted.

This might be necessary in order to save resources or to solve vulnerabilities. If you want to add or delete program components of the recent Avira Professional Security installation go to *System Control* > *Software*. In Vista the menu is called *Programs*.

Choose Avira Professional Security and click on *Change*. In the dialog of the Avira Professional Security, please choose the option *Change program*. You are guided through the change installation.



2.2. Configuration of the Update using the Avira Update Manager

In case you are using several Avira Professional Security installations in the network and you want to update them from a central location, you can use our free-of-charge module “Avira Update Manager”.

This is an option if e.g. only one computer should have access to the Internet but the virus definition files on all computers in the network need to be constantly up-to-date. Furthermore, you are saving traffic and don’t burden the Internet connection unnecessarily.

You can download „Avira Professional Security, Version 2012“ here.

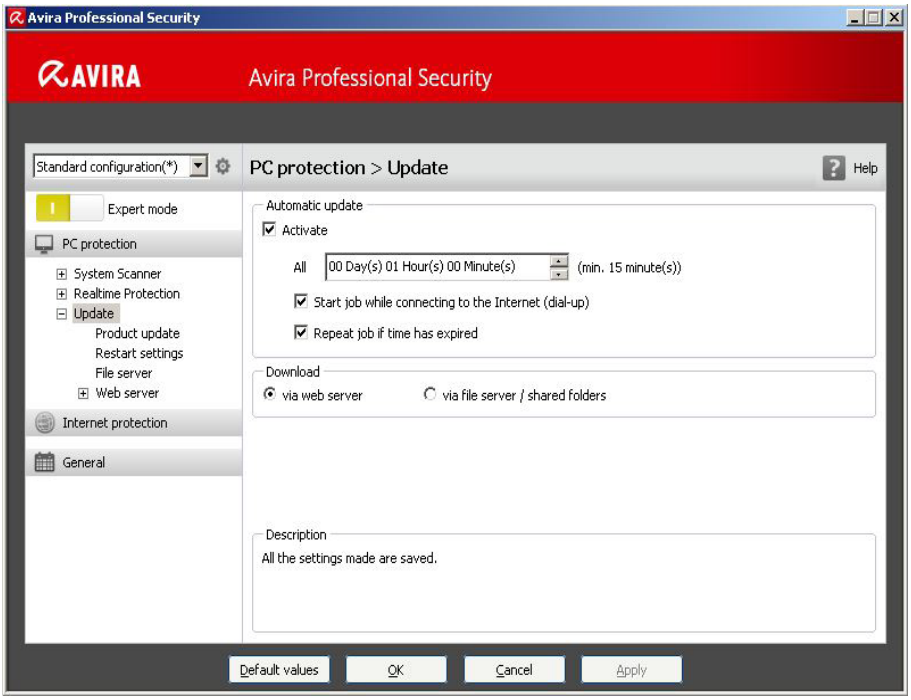
You should install this software on a server operating system. For detailed information about the installation and configuration of the Avira Update Manager, please read the corresponding manual that you can download from the link mentioned above.

After the installation and configuration, the Avira Update Manager downloads the new virus definition files of the Avira Professional Security according to the scheduled intervals and saves them into its root directory.

As the Avira Update Manager also provides an integrated web server with the port 7080, all workstations in the local network can get a connection to this directory and load their updates.

In order to configure the updates of the Avira Professional Security, please proceed as follows:

- Open the configuration of the Avira Professional Security
- Activate the “Expert mode”
- Go to “General” and “Update”
- Choose the option “via web server”



Afterwards, please go to the menu item “Web server”. Here you can find two options, “Priority server” and “Default server”.

Avira Professional Security initially tries to contact the priority server. In case there is no connection to the priority server available, Avira tries to get a connection to the default server.

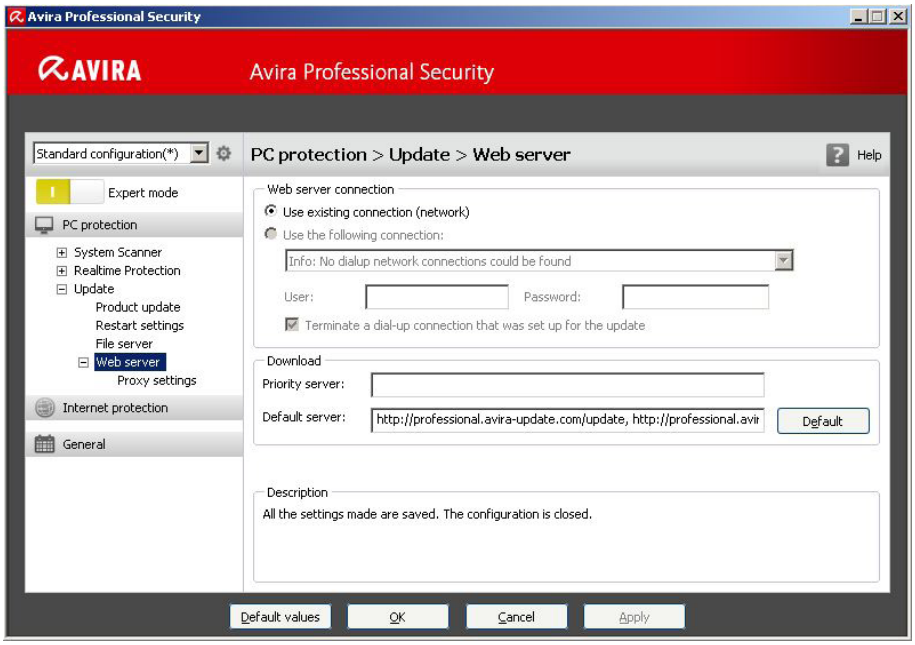
Therefore, the function “Priority server” should be used for the updates via the Avira Update Manager (AUM). This is very useful for notebooks that are part of the enterprise network, but have to be updated as they are outside the network.

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

The entry you should make in this field looks as follows:

http://[IP-address of the 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: local host) > settings > Networks.*
Here you can change the port of the server from 7080 to the required port.

Accordingly, the settings for the update configuration of the Avira Professional Security have to be changed.

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

2.3 Configuration of Product Updates

You can find the menu item “product updates” in the configuration settings of the update of the Avira Professional Security. Avira provides all customers with software updates in order to offer new features or to resolve problems. The setting “Download and install product updates automatically” can cause a reboot. The reboot is activated automatically by Avira Professional Security in order to avoid vulnerabilities.

You can prevent a forced reboot by choosing “Notify user if product updates are available”. You can configure this via the configuration of Avira Professional Security by clicking on *General* > *Update*.

After that you can plan when the product update should be installed, e.g. at a moment when the PC can be rebooted without causing any inconvenience.

2.4 Setting exceptions

Avira Professional Security is connected directly to the operating system. Especially the Avira 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.

For example, all programs which operate with a database in the background are concerned like accounting programs or financial software.

Furthermore, special backup programs which require a data backup of your systems are concerned. 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.

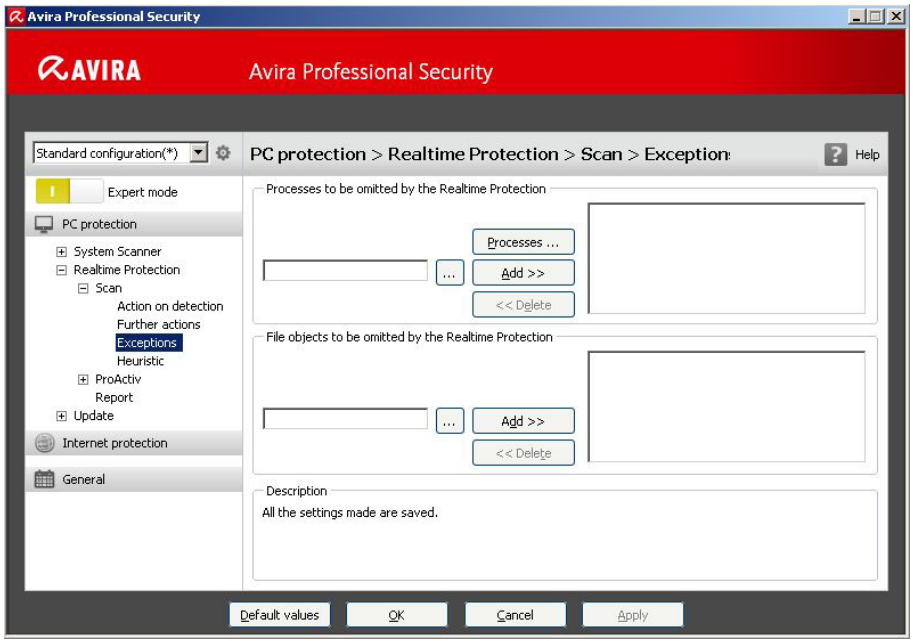
Please proceed as follows in order to prevent a slowing down of your system and exclude the respective programs from the scan:

- Start the configuration of the Avira Professional Security
- Change to the “Expert mode”
- Open the point “Real-Time Protection” and “Scan”
- Choose the point “Exceptions”

In the fields “Processes to be omitted by the Real-Time Protection” you have to enter the paths of the program folder where the concerned software is installed. It is important that a “\” is entered at the end of the path information so that Avira recognizes the path as a directory and not as a file.

An example for the path information:

C:\Programs\Backup_programXY



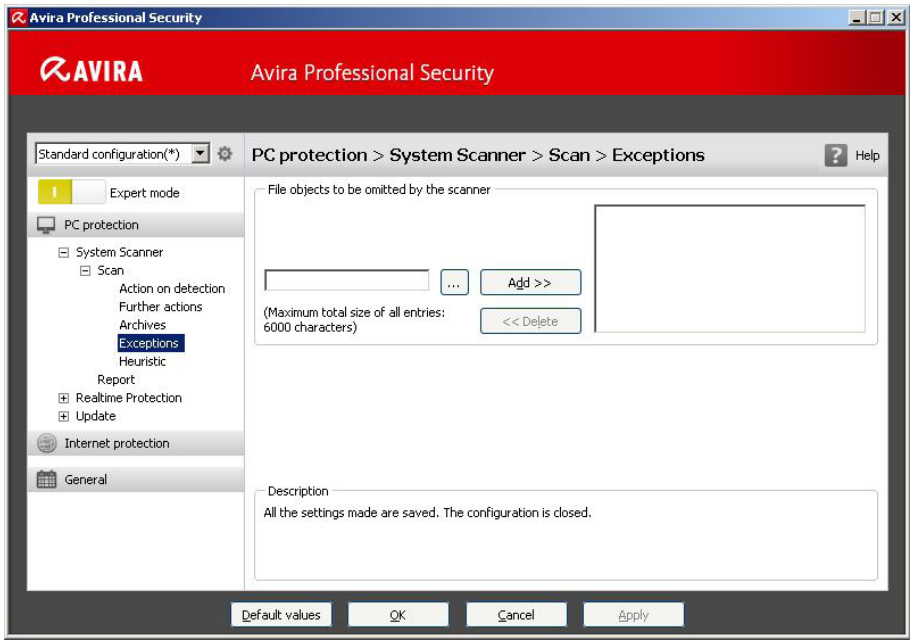
Additionally, it is important to exclude the processes of the affected software also from the scan as well.

These running processes like e.g. backup software initialize file access. 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”.

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*.



2.5. Configuration Profiles

Avira Professional Security offers the possibility to enter different configuration profiles. A configuration profile is a set of configuration settings which can be activated by a mouse click or automatically.

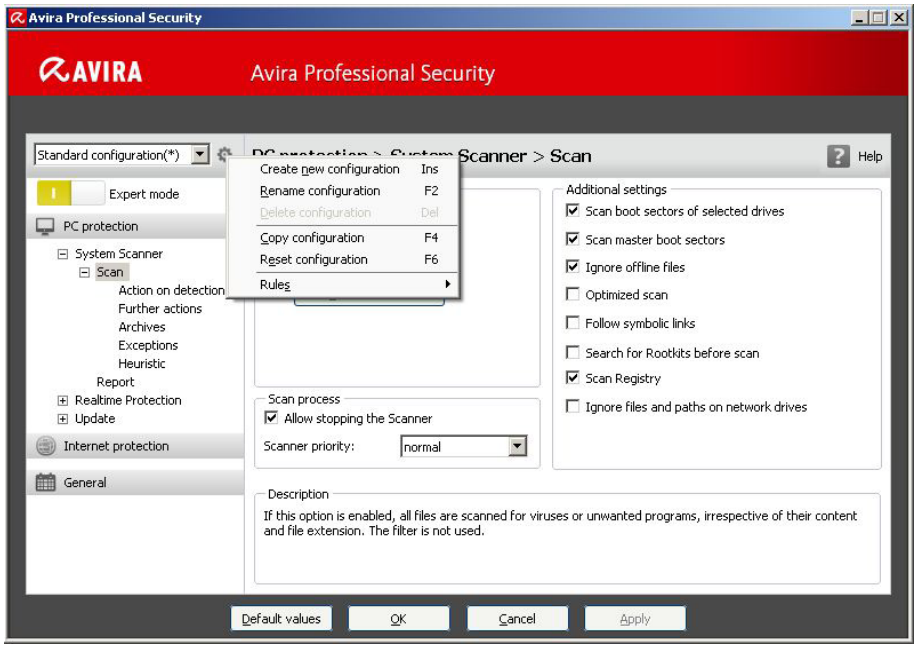
Configuration profiles are especially useful in enterprise networks where notebooks are used. So far, the updates for mobile devices could only be planned by default or priority server. But now you can enter two completely individual configurations.

One profile can be used in the enterprise network and another one can be active as soon as the notebook is used outside of the enterprise e.g. in the home office.

In case a proxy is used in the enterprise to load the updates or in case the Web Protection / Mail Protection is not needed, you can enter the corresponding settings into a special profile. The options are changed with the profile as the notebook leaves the enterprise network.

In order to create and to configure a new configuration profile, please proceed as follows:

- Open the configuration of the Avira Professional Security
- Click on the button in the top left-hand corner for “Create new configuration” (view screenshot)
- Define a name for the profile and configure it using the expert mode



For changing the profiles, you have several possibilities or so-called rules you can set. You can change the profiles manually or automatically depending on the network.

The manual change between the configuration profiles can be made via the context menu in the system tray (with a right mouse click on the symbol). There, you will find the item “Change profile” to select another profile.

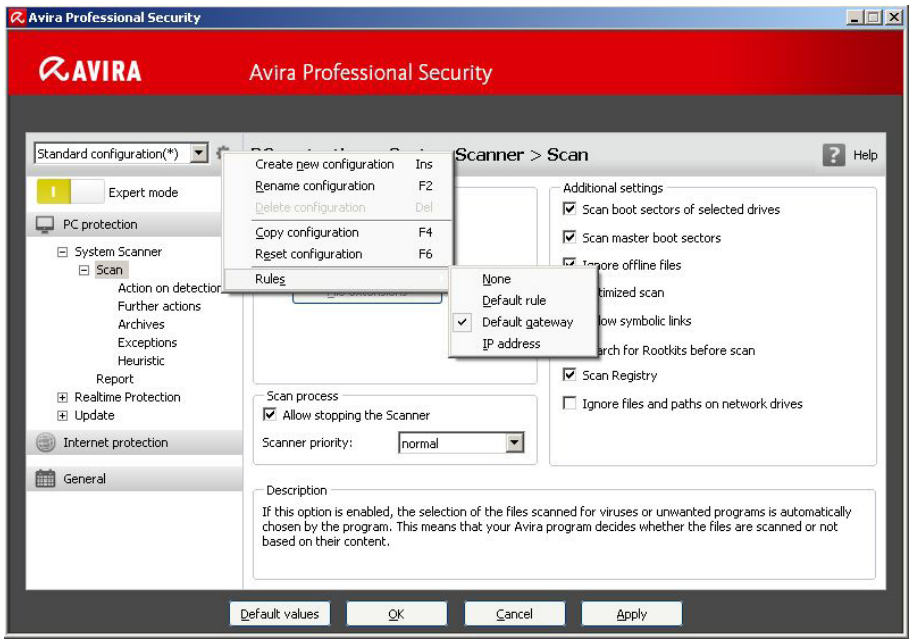
If you want to use the automatic change, you have to define a rule in the configuration of Avira Professional Security. This rule defines when a special profile is activated.

In order to set the rule, click on the corresponding profile in the configuration with the right mouse button and choose the menu item “rule”. Here you have the following options: “None”, “Default rule” and “Default gateway”.

These rules refer to the IP address of the default gateway. They are supervised by the service of the Avira Scheduler that changes automatically to the corresponding profile as soon as a defined rule is fulfilled.

The rule “default gateway” should always refer to the profile which is used in the in-house enterprise network. As soon as the computer is taken out of the network, the gateway changes and Avira Professional Security changes to the profile that has been defined by the rule “Default gateway”.

In case a notebook is used in three different subsidiaries with different network configurations, you can create three different configuration profiles and assign the profiles to the corresponding networks via a specific “Default gateway” rule.



3. Creating jobs in the scheduler

The Avira Professional Security offers an integrated scheduler in order to plan one-time or regular jobs like e.g. updates and scans.
You should enter the settings for the scheduler after the installation in order to make updates and scans automatically.

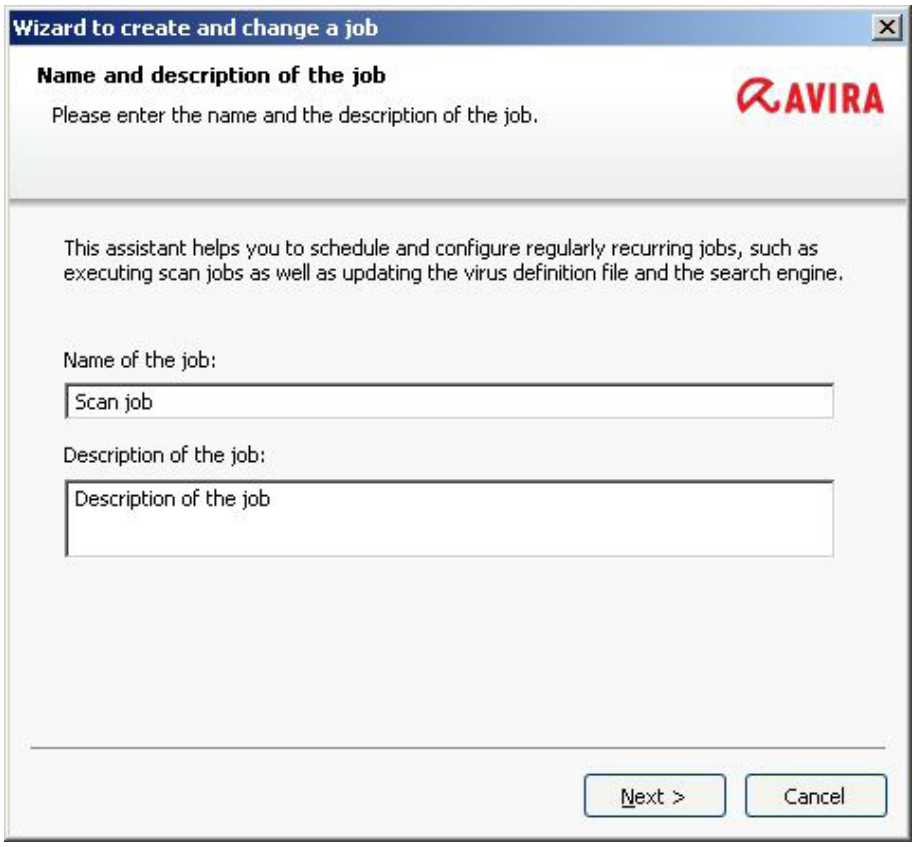
Start the Avira Control Center and select the button *Administration* > *Scheduler*. Choose “Insert new jobs” in the toolbar. Then, define a name (e.g. Internet update or weekly scan) and a short description of the job. Enter the kind of job (in case of an update, select “update job” and in case of a scan, choose “scan job”).

For scan jobs you can define which profile should be used for the scan afterwards. You can find further information about scan profiles in chapter 4 of this document.

Then configure the time frame when the job should be executed (e.g. immediately / daily / weekly / interval / single). Afterwards you define the display mode to be used for the job. In the display mode “invisible” the whole process runs in the background.

The mode “minimized” creates a small control window on the desktop which informs you about the progress of the job. The mode “maximized” creates a larger window with additional details about the running job.

Please check if the job is displayed as “enabled” in the overview. A checkmark has to be set in the corresponding check box.



We recommend an hourly update and a weekly scan job.

We produce updates of the virus definition/engine about 5 times a day. Using hourly updates you can make sure that your protection is really up-to-date. Furthermore, the weekly system scan provides you with a maximum of security.

Frequent scans several times a day can increase your system performance. Large time periods without scans might increase the risk of viruses on the PC that could be detected after the scan.

If you make an update after a gap of several weeks or months, you could detect a virus which might have already been active for a certain time on the computer in case the Real-Time Protection has not already found it.

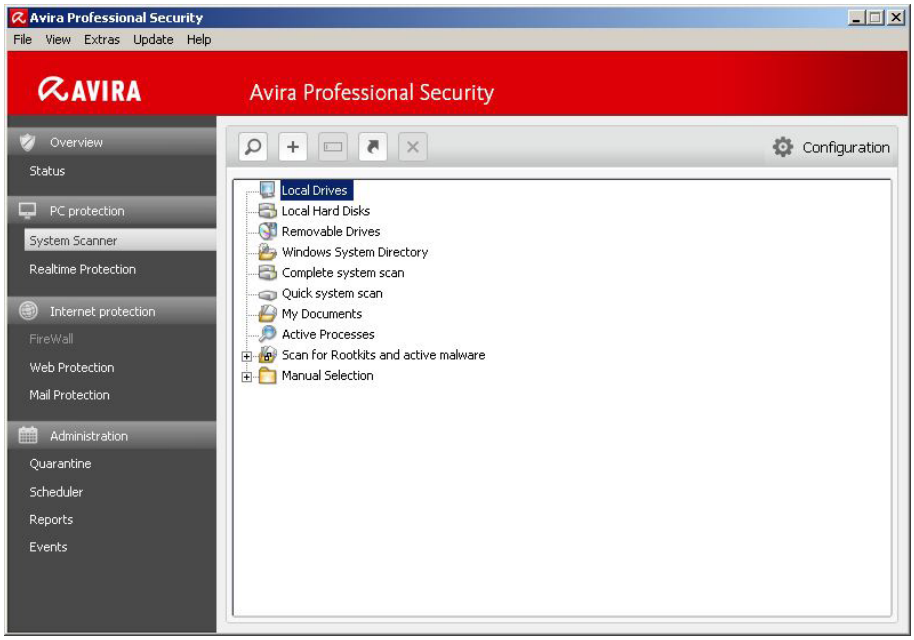
Therefore, a weekly system scan is a good balance between low system load and an optimum of security of the system.

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 “Local protection” beneath “Scanner” in the control center of Avira Professional Security.



Which scan profile is the best depends on which data have 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, which are connected to 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
Rootkit search	Checks the system for active rootkits. (Software which cannot be found with the usual methods of malware detections)	This profile should be used in case of suspicion.

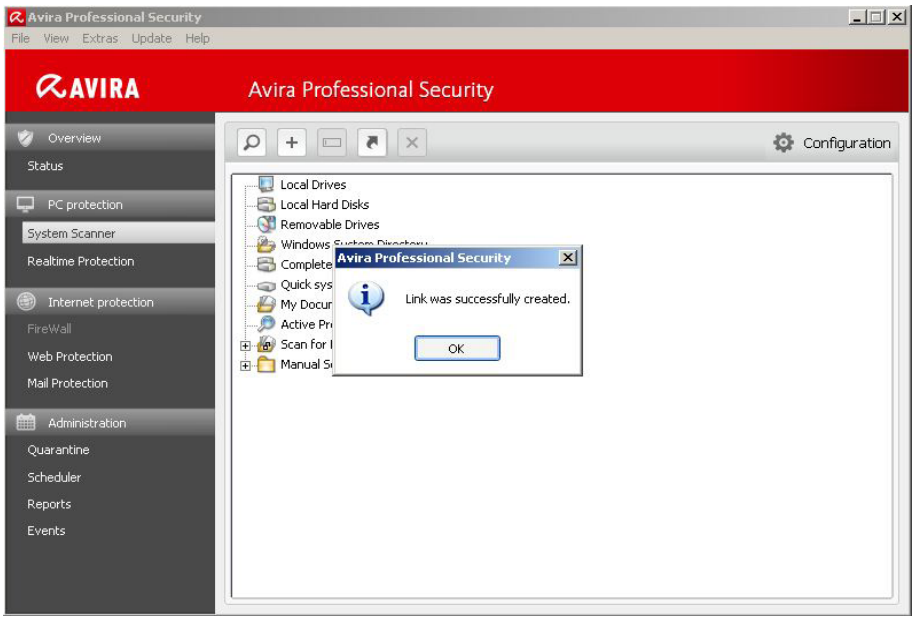
In order to adjust the scan for special drives and directories you can use the default profile "Manual Selection" or you can create individual scan profiles.

The manual selection or your own profiles offer you the possibility to exclude special file types from the scan or to check special file types.

Click on the corresponding scan profile with the right mouse button and choose the option "File filter". Now you can add or delete file endings via the item "User-defined".

You can create a desktop link for a special scan profile which allows you to start your individual scan with a click from the desktop.

You can use your created profiles in the scheduler in order to scan the directories you have defined before; e.g. a special local drive where external data is added frequently and a network drive which is connected to your PC and has to be checked.



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 any more.

This directory is located by default in case of Windows 2000 / XP at:

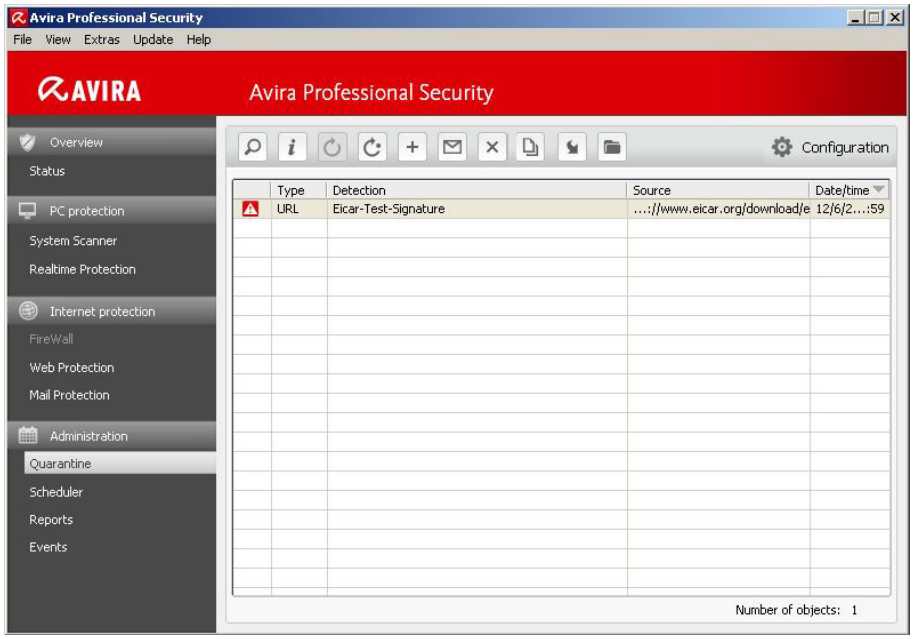
C:\Documents and Settings\All Users\Application Data\Avira\AntiVir Desktop\INFECTED

For Windows Vista, Windows 7 the directory can be found in:

C:\ProgramData\Avira\AntiVir Desktop\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 by starting the Avira ControlCenter and by choosing *Administration* > *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. In the Windows dialog of the virus detection or in the report file, an analysis of the file by the Avira Malware Center has been recommended.

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 advanced continuously.

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.

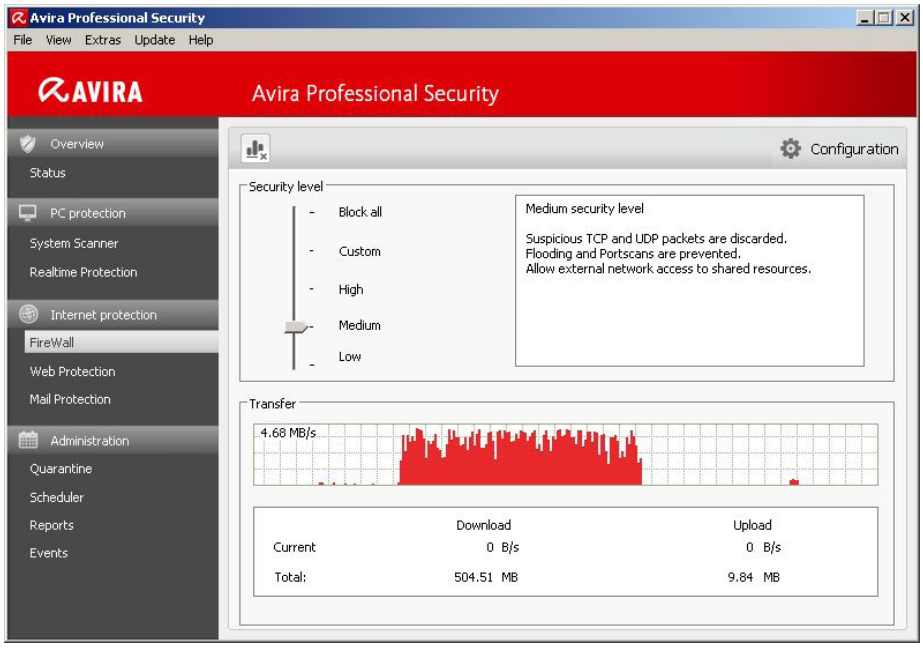
False positive
You are quite sure that a detection is a false positive: Avira Professional Security detects a file which is very unlikely to be malware.

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. Avira FireWall

A desktop firewall has been integrated since Avira Antivir Professional 10. This component allows you to control the incoming and outgoing data traffic. On the one hand you have a scroll bar to define a security level. The security level is set on “Medium” by default. That way the computer will be visible in the network. File share and printer share will work, too.



On the other hand, you are provided with predefined adapter and application rules that can be individually configured and extended.

In case you want to add the browser firefox, you need to proceed as follows.

Open the configuration and go to *FireWall > Application Rules > Add application*.

Now a window opens and lists all applications that have been used recently.
In case the application you are looking for is not shown, you can look for it by selecting “Look for further applications”:

Afterwards, the application is added as a new rule and you can define how it is treated by the Avira FireWall. There are different modes or actions:

Mode:

- *Privileged:* Applications are used independently from the adapter rules or from the security level. That means the application rules are used before the adapter rules.

- *Filtered:* First the adapter rules are used and after that the application rules. In case a port should be blocked according to the adapter rules (e.g. port 80), applications can’t use this port for communication (e.g. web browser).

Action:

- *Permit:* Application is allowed to communicate with the Internet

- *Deny:* Application is not allowed to communicate with the Internet.

- *Ask:* The user can select an action.

7. Quick Tips

7.1 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 the safe mode is reasonable.
You get to the safe mode by rebooting your system and by pressing F8 during the reboot. Then, you choose the item “reboot in the safe mode”.

In the safe mode the Avira scanner receives all the necessary write accesses to all system and program files and can possibly repair files if a repair routine for the virus concerned is available.

Please make sure that the system restore of Windows is deactivated. You can deactivate it clicking on *Start* > *Programs* > *Accessories* > *System Tools* > *System Restore*.

7.2 Web-Filter of the Web Protection

The Web Protection blocks websites by default, which contain spam, malware or phishing. Furthermore, fraud websites, so-called “subscription traps”, are blocked as well as websites which offer a link to these sites.

Here, services are offered which have a low value or no value at all, but cost a lot of money. The costs are usually hidden somewhere in the terms and conditions. Therefore, the claims are not recognized according to the consumer protection.

Blocking a website can be lifted by setting exceptions or by the deactivation of special web filter groups. Go to the configuration of Avira Professional Security, activate the expert mode and click on *Web Protection* > *Scan* > *Locked requests*.
Here you see the item “Activate web filter” and the particular categories which you can choose or exclude.

7.3 Reset LSP in case of problems with the Web- and Mail Protection

Occurring problems with the Web Protection or the Mail Protection, e.g. the modules do not start during the system boot, are often caused by errors in the LSP (Layered Service Provides, a program which is in the TCP/IP socket).

It might help to uninstall the modules completely and to reset the LSP to the default values. In Windows click on *Start* and enter „cmd“ to start the console. Here you should enter `netsh winsock reset`. Afterwards, the computer needs to be restarted and the Mail Protection and/or Web Protection can be installed again.

Note
The registry protection has to be switched off on the computer. In case other programs should have made entries in the LSP, these entries are deleted. That means that these programs don't work properly after a LSP reset.

An example is AVM FritzProtect, which creates an entry in the LSP with the name "Sarah LSP". Without this entry, the program doesn't work.
In order to see which entries are made in the LSP, you can execute our Support Collector on your system, which creates an image of the LSP stack.

7.4 Protocols which are checked by the Mail Protection

The Mail Protection offers a permanent control of your emails and checks them for viruses and malware; including the email attachments.

POP3 incoming emails are checked by default if the Mail Protection is installed.

You can activate the SMTP check (outgoing emails) in the configuration of the Avira Professional Security at *Configuration* > *Mail Protection*.
The scan using the IMAP protocol is also possible. You can activate it in the configuration of Avira Professional Security by clicking *Configuration* > *Mail Protection* > *Monitor IMAP accounts*. In contrast to the POP3 protocol, the emails remain on the server and are managed there.

7.5 Manual insertion of the license file

If you have renewed your license and cannot load it via the button "Load license file" in the main window of the Avira Professional Security, you have the possibility to copy the file (hbedv.key) directly into the main directory of Avira.
(*C:\Program Files\Avira\AntiVir Desktop*).
The result is the same as loading the file in the program using the button "Help" and "Load license file".

7.6 Keeping the configuration for several installations

You can install the Avira Professional Security on several PCs and use a defined configuration on all the PCs by means of the "avwin.ini". You can find it in the following path:

Windows XP
C:\Documents und Settings\All Users\Application Data\Avira\AntiVir Desktop\CONFIG\avwin.ini

Windows 7
C:\Programm Data\Avira\AntiVir Desktop\CONFIG\avwin.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 „avwin.ini“ using the command line during the installation, e.g. in case of a logon script. The „avwin.ini“ is imported during the installation.

In case of an automatic installation of Avira Professional Security, the setup program works with the control file „setup.inf“. The setup program (presetup.exe) is included in the installation package of Avira Professional Security.

The setup file of Avira Professional Security is a self unpacking WinRAR archive which you can open and unpack with WinRAR. This archive also includes the files “presetup.exe” and “setup.inf”, which are necessary for the installation in the network.

The installation is started with a script or a batch file and receives all the necessary information from the control file. The commands in the script replace the manual entries during the installation.
The Avira Professional Security can be easily allocated in the network with a login script of the server or via AMC.

The following steps are necessary in order to install Avira Professional Security automatically in the network:

- Administrator rights are necessary (also in the batch mode)
- Configure the parameter of the file setup.inf and save the file
- Start the installation of Avira Professional Security with the parameter /inf
- Or include the parameter into the login script of the server -
  Example: `presetup.exe /inf="c:\temp\setup.inf"`
- The installation is processed automatically
- All entries for paths or files have to be set in “…”

7.7 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 does not 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 does not 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, which have been compressed using unusual run-time compression, can be regarded as suspicious.

Double-extension files
Executable files which 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.

Issued Q4-2011

AVIRA

live free.™

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

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