Avira

Professional Security

User Manual

Trademarks and Copyright

Trademarks

Windows is a registered trademark of the Microsoft Corporation in the United States and other countries.
All other brand and product names are trademarks or registered trademarks of their respective owners.
Protected trademarks are not marked as such in this manual. This does not mean, however, that they may be used freely.

Copyright information

Code provided by third party providers was used for Avira Professional Security. We thank the copyright owners for making the code available to us.
For detailed information on copyright, please refer to "Third Party Licenses" in the program help of Avira Professional Security.

End User License Agreement - EULA

https://www.avira.com/en/license-agreement

Privacy Policy

https://www.avira.com/en/general-privacy

Table of Contents

1. Introduction

Your Avira product protects your computer against viruses, worms, Trojans, adware and spyware and other risks. In this manual these are referred to as viruses or malware (harmful software) and unwanted programs.

The manual describes the program installation and operation.

For further options and information, please visit our website:
http://www.avira.com

The Avira website lets you:

- access information on other Avira desktop programs
- download the latest Avira desktop programs
- download the latest product manuals in PDF format
- download free support and repair tools
- access our comprehensive knowledge database and FAQs for troubleshooting
- access country-specific support addresses.

Your Avira Team

1.1 Icons and emphases

The following icons are used:

Icon / designation	Explanation
✓	Placed before a condition which must be fulfilled prior to execution of an action.
▸	Placed before an action step that you perform.
Warning	Placed before a warning when critical data loss might occur.
Note	Placed before a link to particularly important information or a tip which makes your Avira Professional Security easier to use.

The following emphases are used:

Emphasis	Explanation
Italics	File name or path data.
	Displayed software interface elements (e.g. window section or error message).
Bold	Clickable software interface elements (e.g. menu item, navigation area, option box or button).

2. Product information

This chapter contains all information relevant to the purchase and use of your Avira product:

- see Chapter: Delivery scope
- see Chapter: System requirements
- see Chapter: Licensing and Upgrade
- see Chapter: License Manager

Avira products are comprehensive and flexible tools you can rely on to protect your computer from viruses, malware, unwanted programs and other dangers.

▶ Please note the following information:

Warning
Loss of valuable data usually has dramatic consequences. Even the best virus protection program cannot provide one hundred percent protection from data loss. Make regular copies (Backups) of your data for security purposes.

Note
A program can only provide reliable and effective protection from viruses, malware, unwanted programs and other dangers if it is up-to-date. Make sure your Avira product is up-to-date with automatic updates. Configure the program accordingly.

2.1 Delivery scope

Your Avira product has the following functions:

- Control Center for monitoring, managing and controlling the entire program
- Central configuration with user-friendly standard and advanced options and context-sensitive help
- System Scanner (on-demand scan) with profile-controlled and configurable scan for all known types of virus and malware
- Integration into the Windows User Account Control allows you to carry out tasks requiring administrator rights.
- Real-Time Protection (on-access scan) for continuous monitoring of all file access attempts

- ProActiv component for the permanent monitoring of program actions (for 32-bit systems only)
- Mail Protection (POP3 Scanner, IMAP Scanner and SMTP Scanner) for the permanent checking of emails for viruses and malware, including the checking of email attachments
- Web Protection for monitoring data and files transferred from the Internet using the HTTP protocol (monitoring of ports 80, 8080, 3128)
- Integrated quarantine management to isolate and process suspicious files
- Rootkits protection for detecting hidden malware installed in your computer system (rootkits)
  (Not available under Windows XP 64 bit)
- Direct access to detailed information on the detected viruses and malware via the Internet
- Simple and quick updates to the program, virus definitions, and search engine through Single File Update and incremental VDF updates via a web server on the Internet or an intranet
- User-friendly licensing in License Manager
- Integrated Scheduler for planning one-off or recurring jobs such as updates or scans
- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method
- Detection of all conventional archive types including detection of nested archives and smart extension detection
- High-performance multithreading function (simultaneous high-speed scanning of multiple files)
- FireWall for protecting your computer from unauthorized access from the Internet or another network and from unauthorized access to the Internet/network by unauthorized users

2.2 System requirements

2.2.1 System requirements Avira Professional Security

Avira Professional Security has the following requirements for successful use of the system:

Operating system

- Windows 8, newest SP (32 or 64 bit) or
- Windows 7, newest SP (32 or 64 bit) or
- Windows XP, newest SP (32 or 64 bit)

Hardware

- Computer with Pentium processor or later, at least 1 GHz
- At least 150 MB of free hard disk memory space (more if using quarantine for temporary storage)
- At least 1024 MB RAM under Windows 8, Windows 7
- At least 512 MB RAM under Windows XP

Other requirements

- For the program installation: Administrator rights
- For all installations: Windows Internet Explorer 6.0 or higher
- Internet connection where appropriate (see Preparing for installation)

2.2.2 Administrator rights (since Windows Vista)

On Windows XP, many users work with administrator rights. However, this is not desirable from the point of view of security because it is then easy for viruses and unwanted programs to infiltrate computers.

For this reason, Microsoft introduced the "User Account Control" (UAC). The User Account Control is part of the following operating systems:

- Windows Vista
- Windows 7
- Windows 8

The User Account Control offers more protection for users who are logged in as administrators. Thus an administrator only has the privileges of a normal user at first. Actions for which administrator rights are required are clearly marked by the operating system with an information icon. In addition, the user must explicitly confirm the required action. Privileges will only then be increased and the administrative task will be performed by the operating system after this permission has been obtained.

The Avira Professional Security requires administrator rights for some actions. These actions are marked with the following symbol: 🛡. If this symbol also appears on a button, administrator rights are required to carry out this action. If your current user account does not have administrator rights, the Windows dialog of the User Account Control asks you to enter the administrator password. If you do not have an administrator password, you cannot carry out this action.

2.2.3 Incompatibility with other programs

Avira Professional Security

Avira Professional Security cannot currently be used with the following products:

- PGP Desktop Home

- PGP Desktop Professional 9.0
- CyberPatrol

An error in the aforesaid products may cause the Avira Mail Protection (POP3 scanner) in Avira Professional Security not to function or the system to become unstable. Avira is working with PGP and CyberPatrol to resolve the problem. Until a solution is found, we strongly recommend that you uninstall the aforesaid products before installing Avira Professional Security.

Avira Web Protection

Avira Web Protection is not compatible with the following products:

- Bigfoot Networks Killer Ethernet Controller
- Teleport Pro from Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording from SCM Microsystems
- MSN Messenger from Microsoft

Any data sent or requested by these products will therefore be ignored by Avira Web Protection.

> **Note**
> Avira Mail Protection will not function if a mail server (e.g. AVM KEN, Exchange) is already installed on the computer.

2.3 Licensing and Upgrade

2.3.1 Licensing

In order to be able to use your Avira product, you require a license. You thereby accept the license terms.

The license is issued via a digital license in the form of a *.KEY* file. This digital license file is the key to your personal license. It contains exact details of which programs are licensed to you and for what period of time. A digital license file can therefore also contain the license for more than one product.

If you purchased your Avira product on the Internet, or via a program CD/DVD, the digital license file is sent to you by email. You can load the license key during installation of the program or install it later in License Manager.

2.3.2 Extending a license

When your license is about to expire, Avira will send a slide-up reminding you to extend your license. To do so, you only have to click a link and you will be forwarded to the Avira online shop.

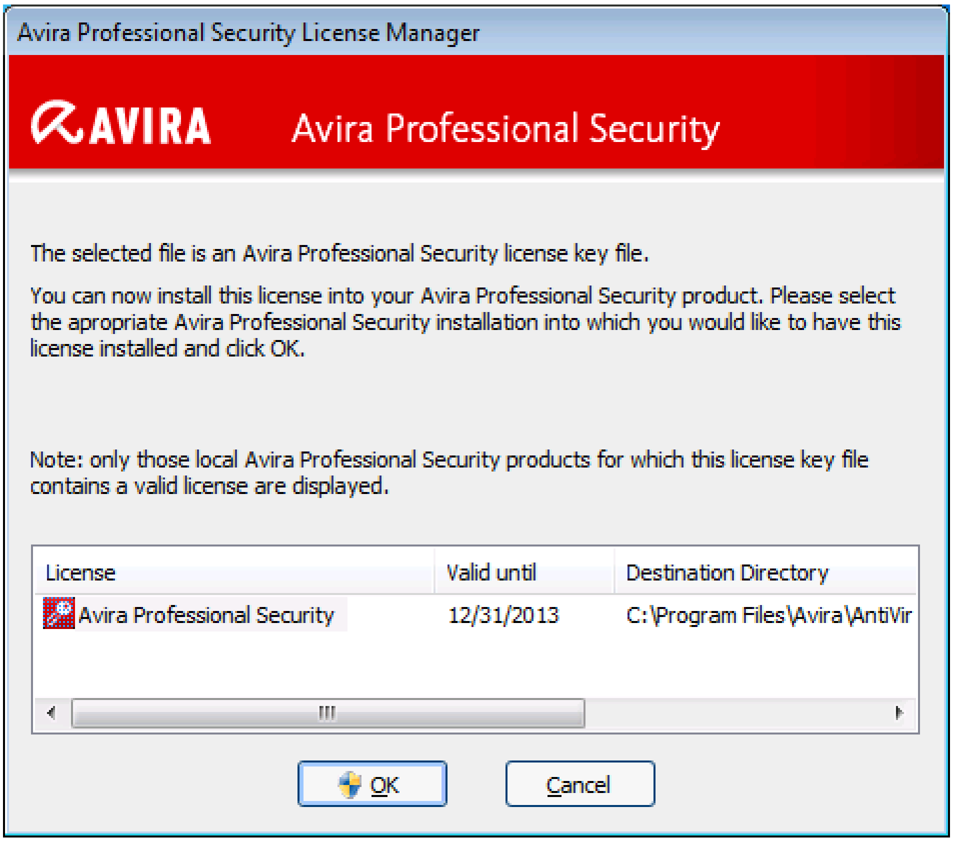
If you have registered in the licensing portal of Avira, you can additionally extend your license directly online via the **License Overview** or select the automatic renewal of your license.

> **Note**
> If your Avira product is managed under AMC, your administrator will execute the upgrade. You will be asked to save your data and reboot your computer, otherwise you are not protected.

2.3.3 License manager

The Avira Professional Security License Manager enables very simple installation of the Avira Professional Security license.

Avira Professional Security License Manager



Avira Professional Security License Manager

AVIRA Avira Professional Security

The selected file is an Avira Professional Security license key file.

You can now install this license into your Avira Professional Security product. Please select the apropriate Avira Professional Security installation into which you would like to have this license installed and click OK.

Note: only those local Avira Professional Security products for which this license key file contains a valid license are displayed.

License	Valid until	Destination Directory
Avira Professional Security	12/31/2013	C:\Program Files\Avira\AntiVir

You can install the license by selecting the license file in your file manager or in the activation email with a double click and following the relevant instructions on the screen.

Note
The Avira Professional Security License Manager automatically copies the corresponding license in the relevant product folder. If a license already exists, a note appears as to whether the existing license file is to be replaced. In this case the existing file is overwritten by the new license file.

3. Installation and uninstallation

This chapter contains information relating to the installation of Avira Professional Security.

- Preparing for installation
- Installing from CD when online
- Installing from CD when offline
- Installing downloaded software
- Removing incompatible software
- Choosing an installation type
- Installing Avira Professional Security
- Changing the installation
- Uninstalling Avira Professional Security

3.1 Preparing for installation

✓ Before installation, check whether your computer fulfills all the minimum System Requirements.

✓ Close all running applications.

✓ Make sure that no other virus protection solutions are installed. The automatic protection functions of various security solutions may interfere with each other (for the automatic options see Removing incompatible software).

✓ If necessary, please uninstall any previously installed search toolbars before you install the Avira SearchFree Toolbar. Otherwise you will not be able to install the Avira SearchFree Toolbar.

✓ Establish an Internet connection.

- The connection is necessary for performing the following installation steps:
  - Downloading the current program file and scan engine as well as the latest virus definition files via the installation program (for Internet-based installation)
  - Activating the program
  - Registering as a user
  - Where appropriate, carrying out an update after completed installation

✓ Keep the activation code or license file for your Avira Professional Security handy for the time when you want to activate the program.

✓ For product activation or registration, your Avira Professional Security uses the HTTP protocol and Port 80 (web communication), as well as encryption protocol SSL and port 443, to communicate with the Avira servers. If you are using a firewall, please ensure that the required connections and/or incoming or outgoing data are not blocked by the firewall.

3.2 Installing from CD when online

- Insert the Avira Professional Security CD.

If autostart is enabled, click **Open folder** to view files.
OR

Navigate to your CD drive, right-click on AVIRA and select **Open folder** to view files.

Double-click the file *autorun.exe*.

In the CD menu choose the online version to install.

The program scans for incompatible software (more information here: Removing incompatible software).

Click **Next** in the *Welcome* screen.

Select the language and click **Next**. All files necessary for installation are downloaded from the Avira web servers.

Continue with Choosing an installation type.

3.3 Installing from CD when offline

- Insert the Avira Professional Security CD.

If autostart is enabled, click **Open folder** to view files.
OR

Navigate to your CD drive, right-click on AVIRA and select **Open folder** to view files.

Double-click the file *autorun.exe*.

In the CD menu choose the offline version to install.

The program scans for incompatible software (more information here: Removing incompatible software).

The installation file is extracted. The installation routine is started.

Continue with Choosing an installation type.

3.4 Installing software downloaded from the Avira website

- Go to www.avira.com/download.

Select the product and click **Download**.

Save the downloaded file on your system.

Double-click the installation file avira_professional_security_en.exe.

If the User Account Control window appears, click **Yes**.

The program scans for incompatible software (more information here: Removing incompatible software).

The installation file is extracted. The installation routine is started.

Continue with Selecting an installation type.

> **Note**
> You can cancel the installation and resume it later, if needed. A shortcut will be created on your desktop. To resume the installation you just have to double-click the *Resume installation* shortcut with the Avira logo on it.

3.5 Removing incompatible software

The Avira Professional Security will search for any possible incompatible software on your computer. If potentially incompatible software is detected Avira Professional Security generates a list of these programs. It is recommended to remove these software programs in order not to endanger the stability of your computer.

- Select from the list the check boxes of all those programs that should be removed automatically from your computer and click **Next**.

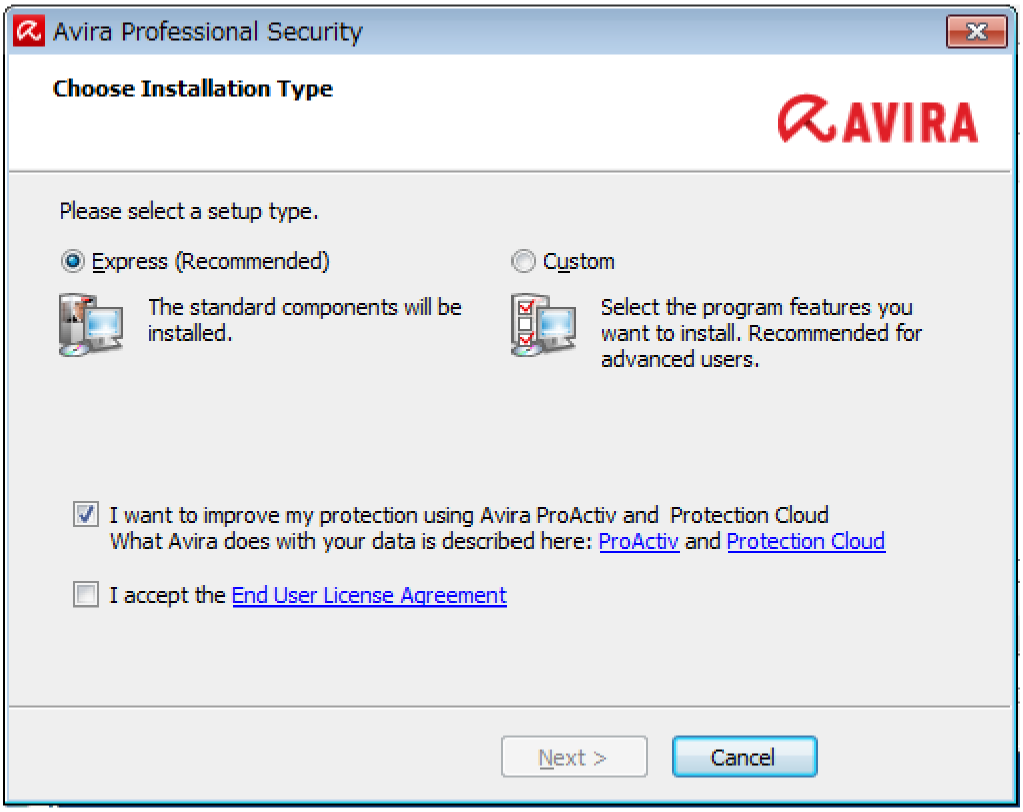
  For some products the uninstallation has to be confirmed manually.

  Select those programs and click **Next**.

  The uninstallation of one or more of the selected programs may require a restart of your computer. After rebooting the installation will begin.

3.6 Choosing an installation type

During installation you can select a setup type in the installation wizard. The installation wizard is designed to smoothly guide you through the installation.



Avira Professional Security

Choose Installation Type

Please select a setup type.

● Express (Recommended)

The standard components will be installed.

○ Custom

Select the program features you want to install. Recommended for advanced users.

☑ I want to improve my protection using Avira ProActiv and Protection Cloud
What Avira does with your data is described here: ProActiv and Protection Cloud

□ I accept the End User License Agreement

Related Topics:

- see Performing an Express Installation
- see Performing a Custom Installation

3.6.1 Performing an Express Installation

The *Express installation* is the recommended setup routine.

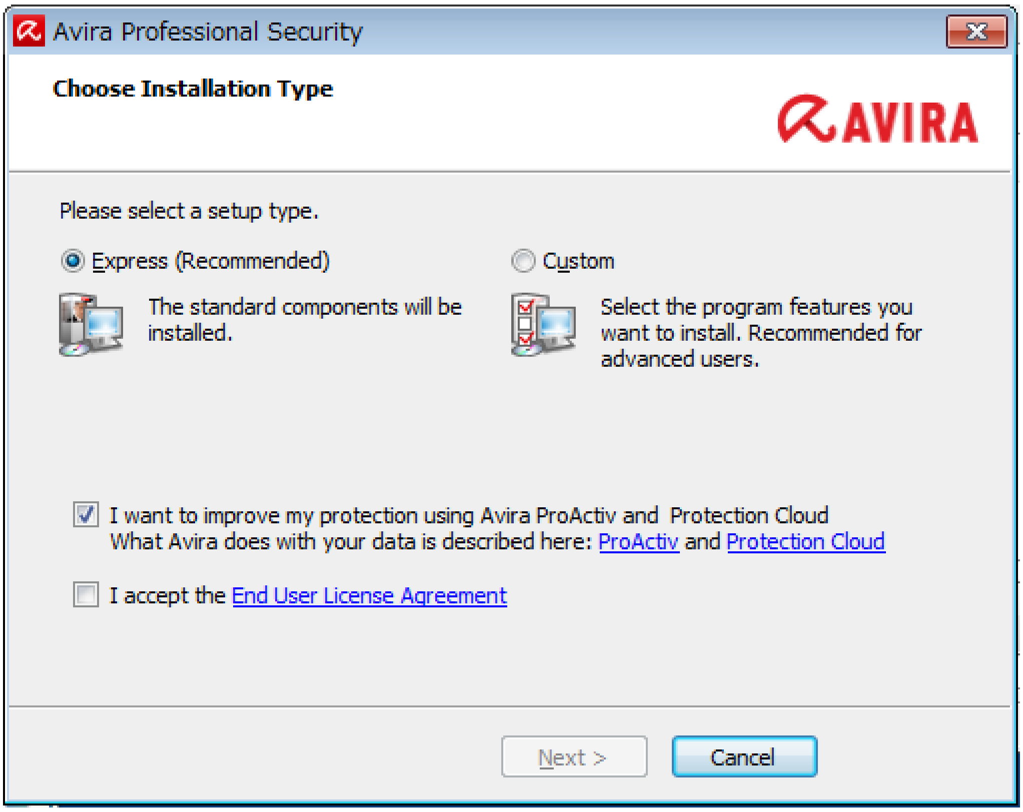
- It installs all the standard components of Avira Professional Security. The Avira recommended security level settings are used.
- As default one of the following installation paths is chosen:
  - *C:\Program Files\Avira* (for Windows 32bit versions) or
  - *C:\Program Files (x86)\Avira* (for Windows 64bit versions)
- Here you can find all files related to Avira Professional Security.
- If you choose this installation type, you can perform an installation by simply clicking **Next** until completion.
- This installation type is designed especially for those users who do not feel comfortable with configuring software tools.

3.6.2 Performing a Custom Installation

The *Custom installation* enables you to configure your installation. This is only recommended for advanced users who are well acquainted with matters of hard- and software as well as security issues.

- You can choose to install individual program components.
- A target folder can be selected for the program files to be installed.
- You can disable **Create a desktop icon and program group in the Start menu**.
- Using the configuration wizard, you can define custom settings for your Avira Professional Security. Also you can choose the security level that you feel comfortable with.
- After installation you can initiate a short system scan that is performed automatically after installation.

3.7 Installing Avira Professional Security



Avira Professional Security

Choose Installation Type

Please select a setup type.

● Express (Recommended)

The standard components will be installed.

○ Custom

Select the program features you want to install. Recommended for advanced users.

☑ I want to improve my protection using Avira ProActiv and Protection Cloud
What Avira does with your data is described here: ProActiv and Protection Cloud

□ I accept the End User License Agreement

- If you do not wish to participate in the Avira Community, unmark the **I want to improve my protection using Avira ProActiv and Protection Cloud** check box, preset by default.

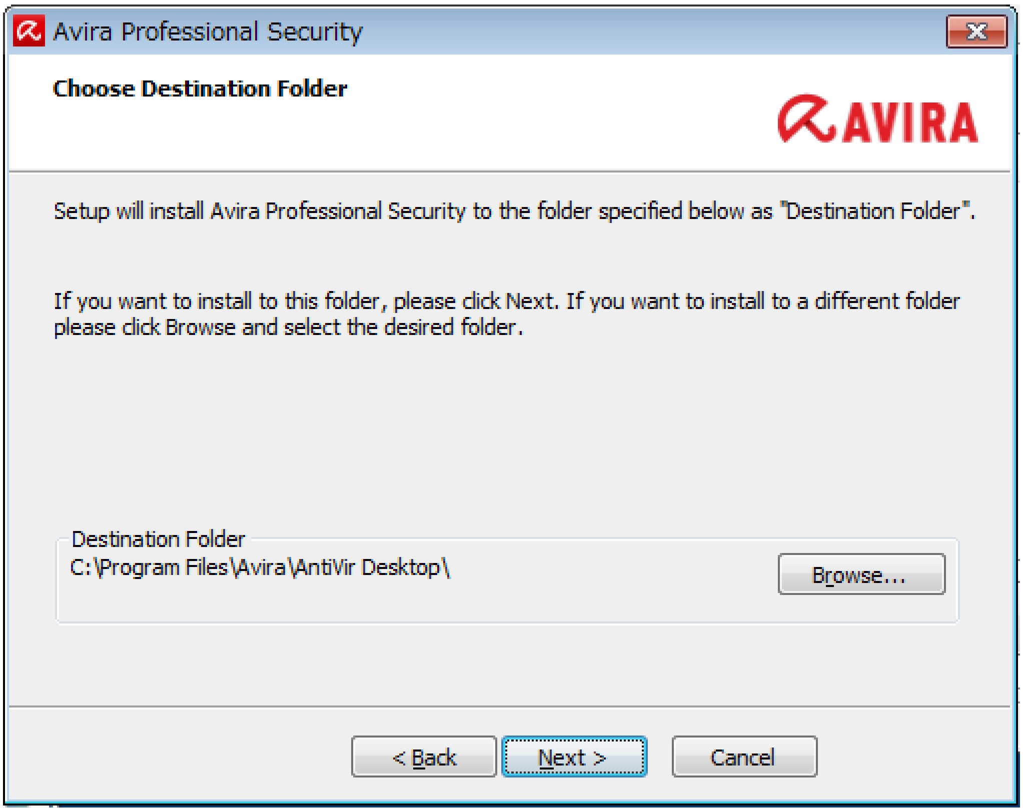
  If you confirm your participation in the Avira Community, Avira Professional Security sends data on detected suspicious programs to the Avira Malware Research Center. The data is used only for an advanced online scan and to expand and refine detection technology.

You can click the links **ProActiv** and **Protection Cloud** to obtain more details on the expanded online and cloud scan.

Confirm that you accept the **End User License Agreement**. For reading the detailed text of the **End User License Agreement**, click the link.

3.7.1 Choosing a destination folder

The custom installation allows you to choose the folder where you want to install Avira Professional Security.



Avira Professional Security

Choose Destination Folder

Setup will install Avira Professional Security to the folder specified below as "Destination Folder".

If you want to install to this folder, please click Next. If you want to install to a different folder please click Browse and select the desired folder.

Destination Folder
C:\Program Files\Avira\AntiVir Desktop\

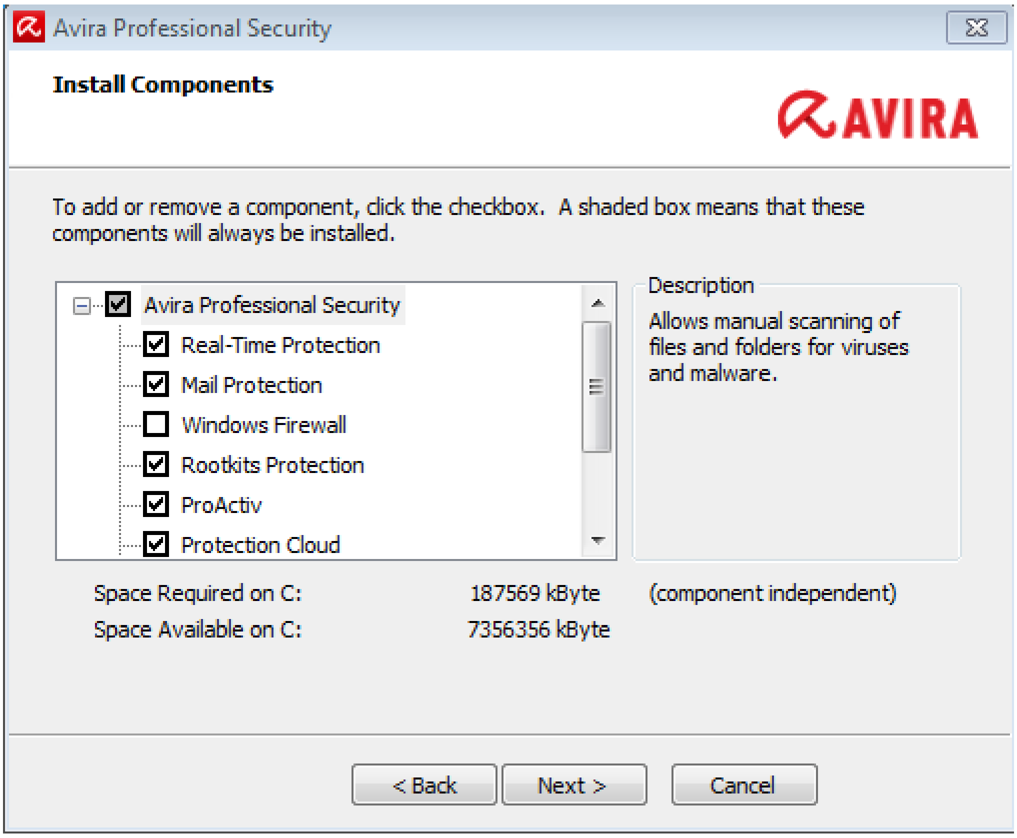
- Click **Browse** and navigate to the location where you want to install Avira Professional Security.

Select the folder where you want to install Avira Professional Security in the **Choose Destination Folder** window.

Click **Next**.

3.7.2 Choosing installation components

In a custom installation or a change installation, the following installation components can be selected, added or removed.



Avira Professional Security

Install Components

To add or remove a component, click the checkbox. A shaded box means that these components will always be installed.

- ☑ Avira Professional Security
  - ☑ Real-Time Protection
  - ☑ Mail Protection
  - □ Windows Firewall
  - ☑ Rootkits Protection
  - ☑ ProActiv
  - ☑ Protection Cloud

Description

Allows manual scanning of files and folders for viruses and malware.

Space Required on C: 187569 kByte (component independent)

Space Available on C: 7356356 kByte

Select or deselect components from the list in the Install components dialog.

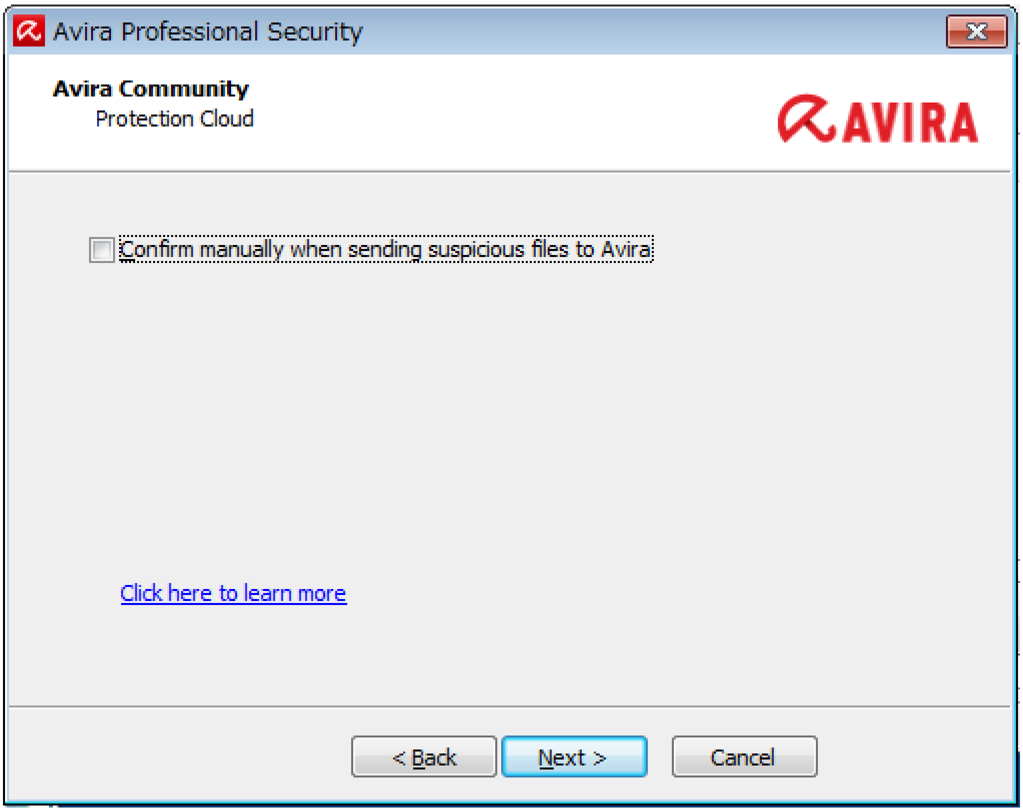
- **Avira Professional Security**
  This contains all components required for successful installation of Avira Professional Security.
  - **Real-Time Protection**
    The Avira Real-Time Protection runs in the background. It monitors and repairs, if possible, files during operations such as open, write and copy in "on-access mode". On access mode means that, whenever a user carries out a file operation (e.g. load document, execute, copy), Avira Professional Security automatically scans the file. Renaming a file, however, does not trigger a scan by Avira Real-Time Protection.
  - **Mail Protection**
    Mail Protection is the interface between your computer and the email server from which your email program (email client) downloads emails. Mail Protection is connected as a so-called proxy between the email program and the email server. All incoming emails are routed through this proxy, scanned for viruses and unwanted programs and forwarded to your email program. Depending on the configuration, the program processes the affected emails automatically or asks you for a certain action.
  - **Avira FireWall** (up to Windows XP)
    Avira FireWall controls communication to and from your computer. It permits or denies communications based on security policies.
  - **Windows Firewall** (starting from Windows Vista)
    This component manages the Windows Firewall from Avira Professional Security.
  - **Rootkits Protection**
    Avira Rootkits Protection checks whether software is already installed on your

computer that can no longer be detected with conventional methods of malware protection after penetrating the computer system.

- **ProActiv**
  The ProActiv component monitors application actions and alerts users to suspicious application behavior. This behavior-based recognition enables you to protect yourself against unknown malware. The ProActiv component is integrated into Avira Real-Time Protection.
- **Protection Cloud**
  The Protection Cloud component is a module for dynamic online detection of still unknown malware. This means that the files are uploaded to a remote location and compared to known files as well as other files that are being uploaded and analyzed in real-time (unscheduled and without delay). This way the database is constantly updated, therefore an even higher level of security can be provided.
  If you have chosen to install the Protection Cloud component, but you want to confirm manually, which files should be sent to the Cloud for analysis, you can enable the option **Confirm manually when sending suspicious files to Avira**.
- **Web Protection**
  When surfing the Internet, you are using your web browser to request data from a web server. The data transferred from the web server (HTML files, script and image files, Flash files, video and music streams, etc.) will normally be moved directly into the browser cache for display in the web browser, meaning that an on-access scan as performed by Avira Real-Time Protection is not possible. This could allow viruses and unwanted programs to access your computer system. Web Protection is what is known as an HTTP proxy which monitors the ports used for data transfer (80, 8080, 3128) and scans the transferred data for viruses and unwanted programs. Depending on the configuration, the program may process the affected files automatically or prompt the user for a specific action.
- **Shell Extension**
  The Shell Extension generates an entry **Scan selected files with Avira** in the context menu of the Windows Explorer (right-hand mouse button). With this entry you can directly scan files or directories.

Related Topics:
Changing an installation

If you have decided to take part in the Avira Community, you can choose to manually confirm the upload each time a file is to be sent to the Avira Malware Research Center.



Avira Professional Security

Avira Community
Protection Cloud

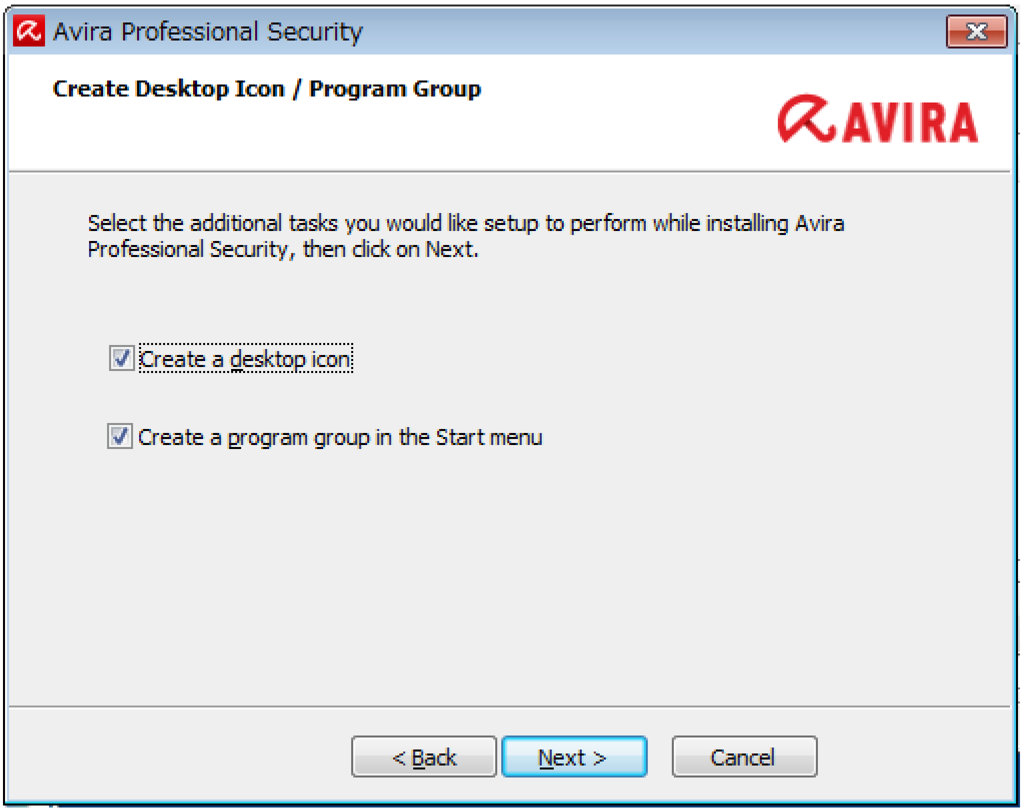
□ Confirm manually when sending suspicious files to Avira

Click here to learn more

- For Avira Professional Security to ask for confirmation each time, enable the option **Confirm manually when sending suspicious files to Avira**.

3.7.3 Creating shortcuts for Avira Professional Security

A desktop icon and/or a program group in the Start menu help you to access Avira Professional Security more quickly and easily.



Avira Professional Security

Create Desktop Icon / Program Group

Select the additional tasks you would like setup to perform while installing Avira Professional Security, then click on Next.

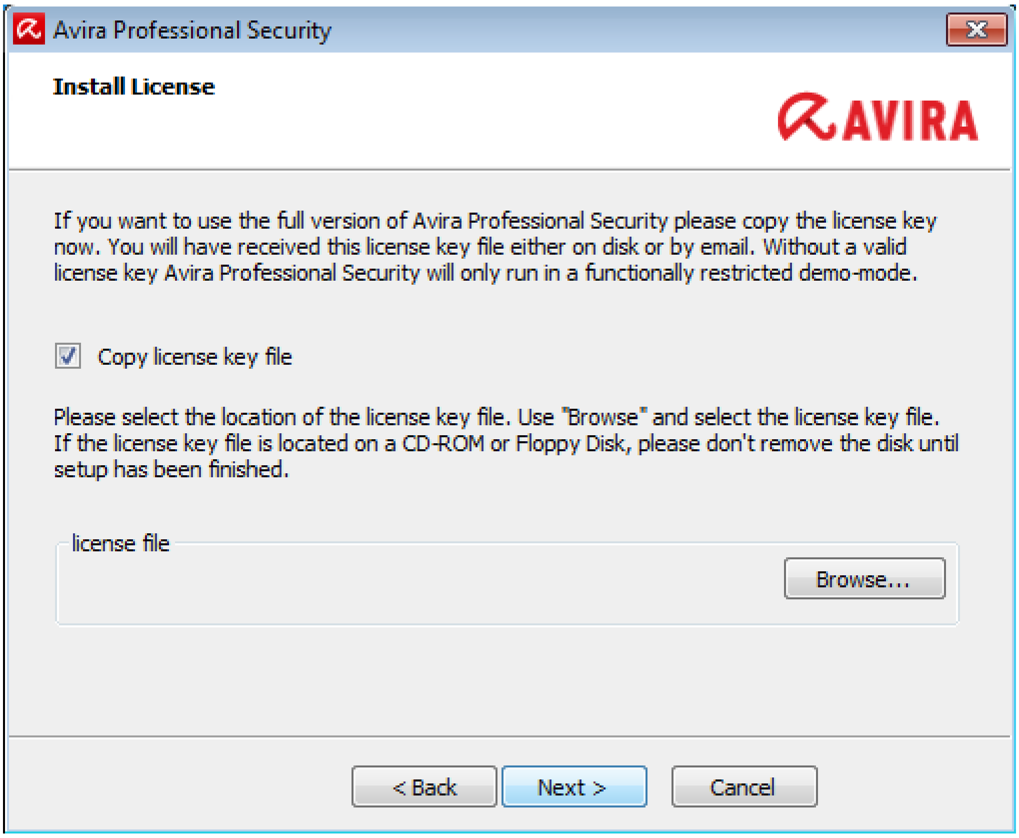
☑ Create a desktop icon

☑ Create a program group in the Start menu

- To create a desktop shortcut for Avira Professional Security and/or a program group in the **Start menu** leave the option(s) activated.

3.7.4 Activating Avira Professional Security

There are several ways to activate your Avira Professional Security.



Install License

If you want to use the full version of Avira Professional Security please copy the license key now. You will have received this license key file either on disk or by email. Without a valid license key Avira Professional Security will only run in a functionally restricted demo-mode.

☑ Copy license key file

Please select the location of the license key file. Use "Browse" and select the license key file. If the license key file is located on a CD-ROM or Floppy Disk, please don't remove the disk until setup has been finished.

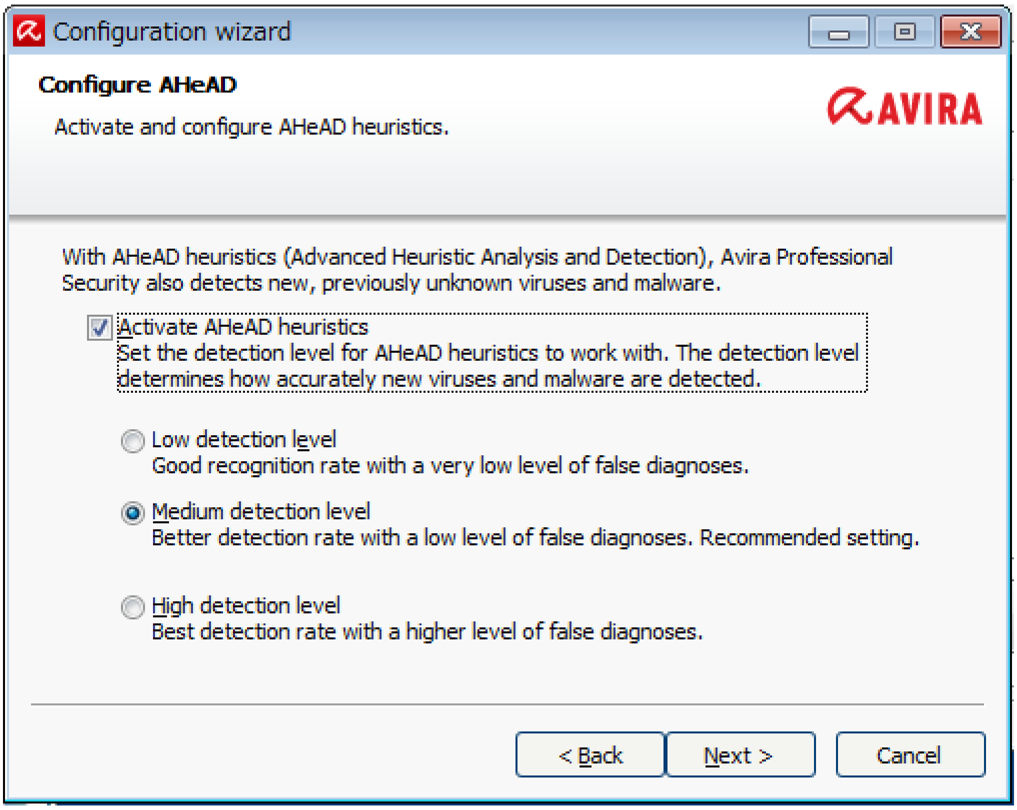
license file

- To copy the license key file for Avira Professional Security make sure the **Copy license key file** check box is activated.
- Click the **Browse...** button.

  A browser window opens and you can navigate to the *hbedv.key* file on your system.
- If you only want to test the product, click **Next**.

3.7.5 Configuring the heuristic detection level (AHeAD)

Avira Professional Security contains a very powerful tool in form of Avira AHeAD (*Advanced Heuristic Analysis and Detection*) technology. This technology uses pattern recognition techniques, so it can detect unknown (new) malware from having analyzed other malware previously.



Configuration wizard

Configure AHeAD

Activate and configure AHeAD heuristics.

With AHeAD heuristics (Advanced Heuristic Analysis and Detection), Avira Professional Security also detects new, previously unknown viruses and malware.

☑ Activate AHeAD heuristics
Set the detection level for AHeAD heuristics to work with. The detection level determines how accurately new viruses and malware are detected.

○ Low detection level
Good recognition rate with a very low level of false diagnoses.

● Medium detection level
Better detection rate with a low level of false diagnoses. Recommended setting.

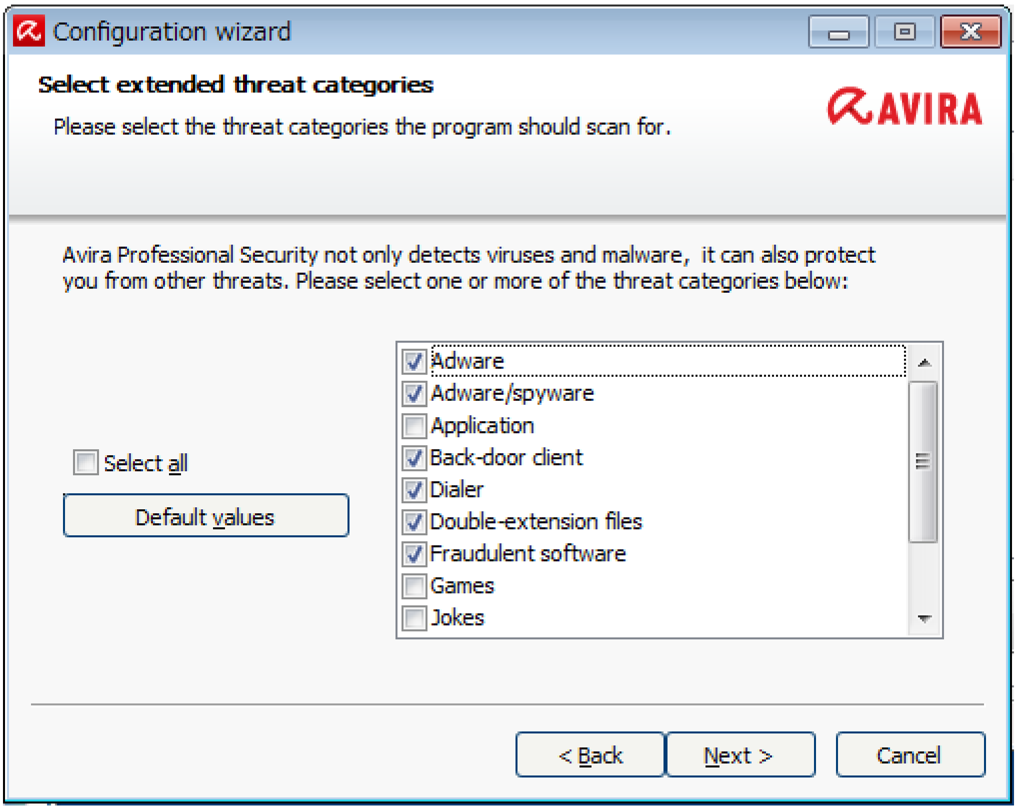
○ High detection level
Best detection rate with a higher level of false diagnoses.

- Select a detection level in the **Configure AHeAD** dialog box and click **Next**.

  The detection level selected is used for the System Scanner (On-demand scan) and Real-Time Protection (On-access scan) AHeAD technology settings.

3.7.6 Selecting extended threat categories

Virus and malware are not the only threats that pose a danger to your computer system. We have defined a whole list of risks and sorted those into extended threat categories for you.



Configuration wizard

Select extended threat categories

Please select the threat categories the program should scan for.

Avira Professional Security not only detects viruses and malware, it can also protect you from other threats. Please select one or more of the threat categories below:

☑ Adware
☑ Adware/spyware
☐ Application
☑ Back-door client
☑ Dialer
☑ Double-extension files
☑ Fraudulent software
☐ Games
☐ Jokes

☐ Select all

- A number of threat categories is already pre-selected by default.

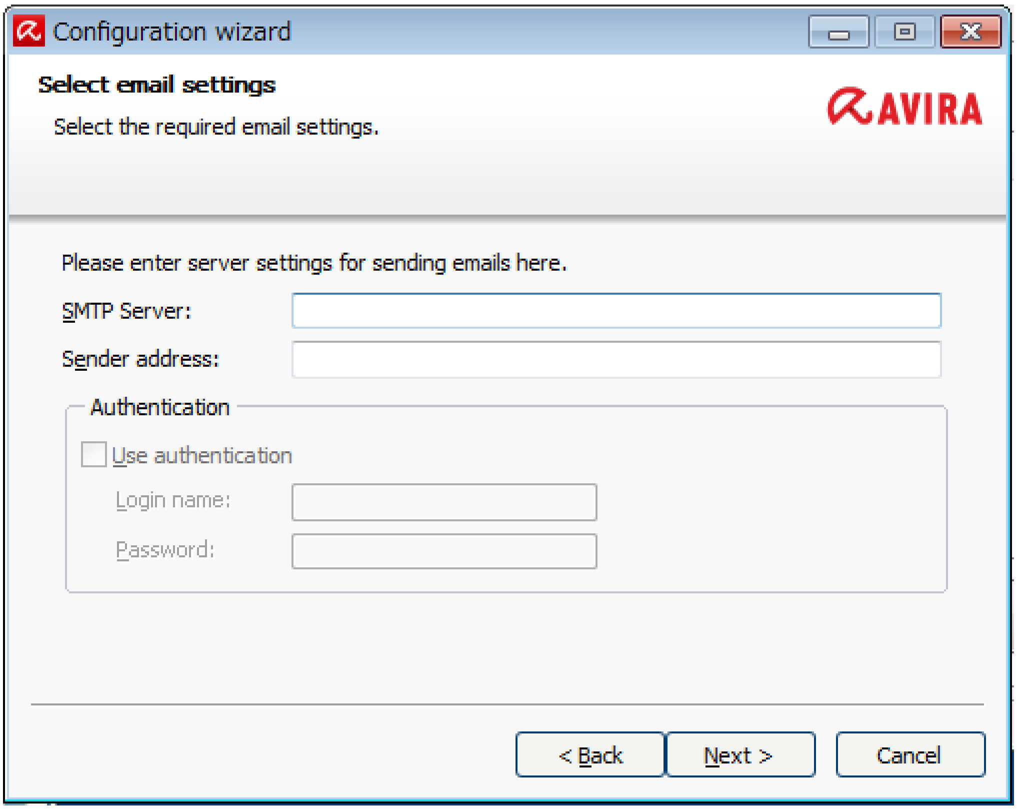
Where appropriate, activate further threat categories in the dialog box **Select extended threat categories**.

If you change your mind, you can revert to the recommended values by clicking the **Default values** button.

Continue the installation by clicking **Next**.

3.7.7 Selecting email settings

Avira Professional Security uses SMTP to send emails, forward suspicious objects from Quarantine to the Avira Malware Research Center, as well as send email alerts.



Configuration wizard

Select email settings

Select the required email settings.

Please enter server settings for sending emails here.

SMTP Server:

Sender address:

Authentication

□ Use authentication

Login name:

Password:

- If you want to be able to send these automatic emails via SMTP,define the server settings for sending emails in the **Select email settings** dialog box.

SMTP Server

Enter the computer name or IP address of the SMTP server you want to use.

Examples:

Address: smtp.company.com

Address: 192.168.1.100

Sender address

Enter the email address of the sender.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an email is sent. Alerts can be transmitted with authentication to an SMTP server via email.

Use authentication

If this option is enabled, a user name and a password can be entered in the relevant boxes for login (authentication).

Login name:

Enter your user name here.

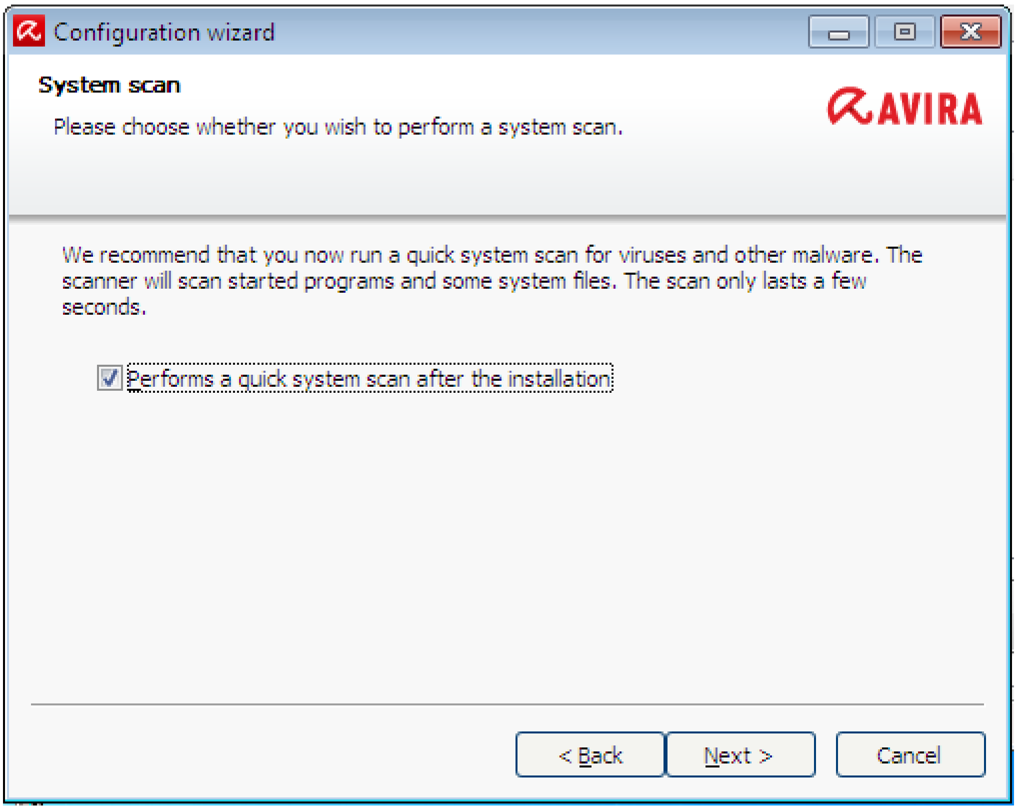
Password:

Enter the relevant password here. The password is saved in encrypted form. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

Click **Next**.

3.7.8 Starting a scan after installation

To check the current security state of the computer, a quick system scan can be performed after the configuration has been completed and before the computer is rebooted. The System Scanner scans running programs and the most important system files for viruses and malware.



Configuration wizard

System scan

Please choose whether you wish to perform a system scan.

We recommend that you now run a quick system scan for viruses and other malware. The scanner will scan started programs and some system files. The scan only lasts a few seconds.

☑ Performs a quick system scan after the installation

- If you want to perform a quick system scan, leave the **Quick system scan** option activated.

Click **Next**.

Complete the configuration by clicking **Finish**.

If you have not deactivated the **Quick system scan** option, the System Scanner performs a quick system scan.

3.7.9 Installation on the network

To simplify installation of Avira products on a network of multiple client computers for the system administrator, your Avira product has a special procedure for the initial installation and the change installation.

For automatic installation, the setup program works with the control file *setup.inf*. The setup program (*presetup.exe*) is contained in the program's installation package. Installation is started with a script or batch file and all necessary information is obtained from the control file. The script commands therefore replace the usual manual inputs during installation.

> **Note**
> Please note that a license file is obligatory for initial installation on the network.

> **Note**
> Please note that an installation package for the Avira product is required for installation via a network. An installation file for Internet-based installation cannot be used.

Avira products can be easily shared on the network with a server login script or via AMC.

For information on installation and uninstallation on the network:

- see Chapter: Command line parameters for the setup program
- see Chapter: Parameter of the file *setup.inf*
- see Chapter: Installation on the network
- see Chapter: Uninstallation on the network

> **Note**
> The Avira Management Console provides another easy option for the installation and uninstallation of Avira products on the network. The Avira Management Console enables the remote installation and maintenance of Avira products on the network. For further information, please refer to our website.
> http://www.avira.com

Installation on the network

The installation can be script-controlled in batch mode.

The setup is suitable for the following installations:

- Initial installation via the network (unattended setup)

- Installation on single-user computers
  - Change installation and update

> **Note**
> We recommend that you test automatic installation before the installation routine is implemented on the network.

> Note
> When installing on a server operating system, the Real-Time Protection and the files protection are not available.

To install Avira product on the network automatically:

✓ You must have administrator rights (also required in batch mode)

- Configure the parameter of the file *setup.inf* and save the file.
- Begin installation with the parameter /inf or integrate the parameter into the login script of the server.

  Example: `presetup.exe /inf="c:\temp\setup.inf"`

  ↳ The installation starts automatically.

Command line parameters for the setup program

> **Note**
> Parameters containing paths or file names must be placed in double quotes (Example: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

The following parameter is possible for installation:

- `/inf`

  The setup program starts with the script mentioned and retrieves all parameters required.
  Example: `presetup.exe /inf="c:\temp\setup.inf"`

The following parameters are possible for the uninstallation:

- `/remove`

  The setup program uninstalls the Avira product.
  Example: `presetup.exe /remove`

- `/remsilent`

  The setup program uninstalls the Avira product without displaying dialogs. The computer is restarted after uninstallation.

Example: `presetup.exe /remsilent`

- `/remsilentaskreboot`

  The setup program uninstalls the Avira product without displaying dialogs and requests a computer restart after uninstallation.
  Example: `presetup.exe /remsilentaskreboot`

The following parameter is available as an option for the uninstallation log:

- `/unsetuplog`

  All actions during uninstallation are logged.
  Example: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

Parameters of the file *setup.inf*

In the control file *setup.inf*, you can set the following parameters in the [DATA] field for the automatic installation of the Avira product. The sequence of the parameters is unimportant. If a parameter setting is missing or wrong, the setup routine is aborted and an error message is displayed.

> **Note**
> Parameters containing paths or file names must be placed in double quotes (Example: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

- `DestinationPath`

  Destination path in which the program is installed. It has to be included to the script. Please note that the setup includes company name and product name automatically. Environment variables can be used.
  Example: `DestinationPath=%PROGRAMFILES%`
  produces the installation path `C:\Program Files\Avira\AntiVir Desktop`

- `ProgramGroup`

  Creates a program group for all users of the computer in the Windows Start menu.
  `1`: Create program group
  `0`: Do not create program group
  Example: `ProgramGroup=1`

- `DesktopIcon`

  Creates a shortcut desktop icon for all users of the computer on the desktop.
  `1`: Create desktop icon
  `0`: Do not create desktop icon
  Example: `DesktopIcon=1`

- `ShellExtension`

Registers the shell extension in the registry. With the shell extension, files or directories can be scanned for viruses and malware via the context menu of the right-hand mouse button.
`1`: Register shell extension
`0`: Do not register shell extension
Example: `ShellExtension=1`

- `Guard`

  Installs the Avira Real-Time Protection (on-access Scanner).
  `1`: Install Avira Real-Time Protection
  `0`: Do not install Avira Real-Time Protection
  Example: `Guard=1`

- `MailScanner`

  Installs the Avira Mail Protection.
  `1`: Install Avira Mail Protection
  `0`: Do not install Avira Mail Protection
  Example: `MailScanner=1`

- `KeyFile`

  Specifies the path for the license file that is copied during installation. For initial installation: obligatory. The file name must be specified completely (fully qualified). (For a change installation: optional.)
  Example: `KeyFile=D:\inst\license\hbedv.key`

- `ShowReadMe`

  Displays the *readme.txt* file after installation.
  `1`: Display file
  `0`: Do not display file
  Example: `ShowReadMe=1`

- `RestartWindows`

  Restarts the computer after installation. This entry has a higher priority than `ShowRestartMessage`.
  `1`: Restart computer
  `0`: Do not restart computer
  Example: `RestartWindows=1`

- `ShowRestartMessage`

  Displays information during the setup before carrying out an automatic restart.
  `0`: Do not display information
  `1`: Display information
  Example: `ShowRestartMessage=1`

- `SetupMode`

  Not required for initial installation. The setup program knows if an initial installation has been performed. Specifies the type of installation. If an installation is available already, it has to be indicated in the `SetupMode` whether this installation is an update only or a change installation (reconfiguration) or an uninstallation.

Update: Updates an existing installation. In this case configuration parameters, for example Guard, are ignored.
Modify: Modifies (reconfigures) an existing installation. In the process no files are copied into the destination path.
Remove: Uninstalls your Avira product from the system.
Example: SetupMode=Update

- AVWinIni (optional)

  Specifies the destination path for the configuration file that may be copied during installation. The file name must be specified completely (fully qualified).
  Example: AVWinIni=d:\inst\config\avwin.ini

- Password

  This option assigns the password that was set for the (modification) installation and uninstallation to the setup routine. The entry is only scanned by the setup routine when a password has been set. If a password has been set and the password parameter is missing or wrong, the setup routine is aborted.
  Example: Password=Password123

- WebGuard

  Installs the Avira Web Protection.
  1: Install Avira Web Protection
  0: Do not install Avira Web Protection
  Example: WebGuard=1

- RootKit

  Installs the Avira Rootkits Protection module. Without Avira Rootkits Protection the System Scanner will not be able to scan for rootkits on the system!
  1: Install Avira Rootkits Protection
  0: Do not install Avira Rootkits Protection
  Example: RootKit=1

- ProActiv

  Installs the Avira ProActiv component. Avira ProActiv is a pattern-based detection technology that enables as yet unknown malware to be detected.
  1: Install ProActiv
  0: Do not install ProActiv
  Example: ProActiv=1

- MgtFirewall

  Installs the Windows Firewall management component. As of Windows Vista, Windows Firewall is managed through the Avira product.
  1: Install the Windows Firewall management component
  0: Do not install the Windows Firewall management component
  Example: MgtFirewall=1

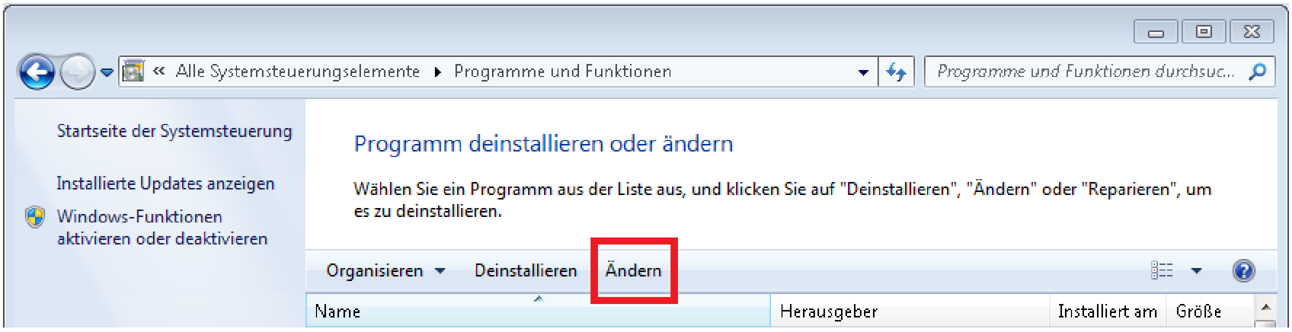
3.8 Changing the installation

If you wish to add or remove modules of the current installation, you can do this without having to uninstall Avira Professional Security. Here is how:

- Changing an installation under Windows 8
- Changing an installation under Windows 7
- Changing an installation under Windows XP

3.8.1 Changing an installation under Windows 8

You have the option of adding or removing individual program components of the Avira Professional Security installation (see Choosing installation components).


« Alle Systemsteuerungselemente ▸ Programme und Funktionen
Programme und Funktionen durchsuc...
Startseite der Systemsteuerung
Installierte Updates anzeigen
Windows-Funktionen aktivieren oder deaktivieren
Organisieren
Deinstallieren
Ändern
Name
Herausgeber
Installiert am
Größe

Programm deinstallieren oder ändern

Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "Deinstallieren", "Ändern" oder "Reparieren", um es zu deinstallieren.

If you wish to add or remove modules of the current installation, you can use the option **Uninstall Programs** in the **Windows control panel** to **Change/Uninstall** programs.

- Right-click on the screen.

  The **All apps** symbol appears.

  Click on the symbol and look in the *Apps - Windows System* section for **Control Panel**.

  Double-click the **Control Panel** symbol.

  Click **Programs - Uninstall a program**.

  Click **Programs and Features - Uninstall a program**.

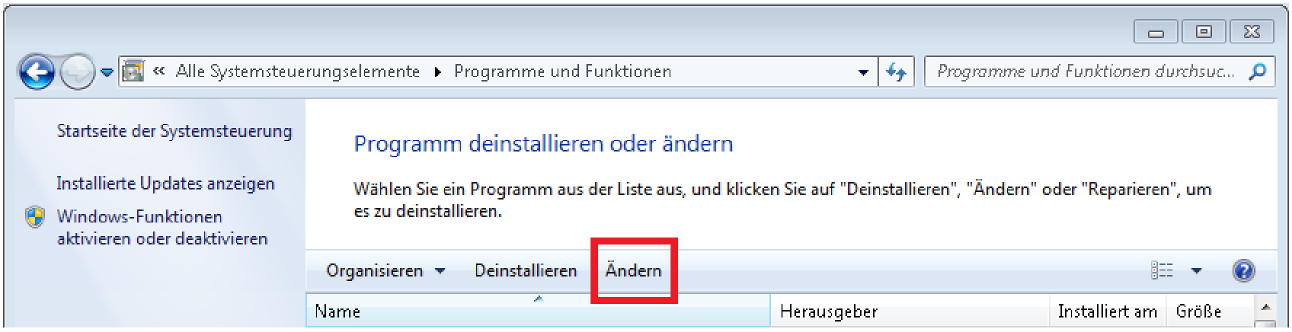
  Select Avira Professional Security and click **Change**.

  In the **Welcome** dialog of the program, select the option **Modify**. You will be guided through the installation changes.

Related Topics:
Choosing installation components

3.8.2 Changing an installation under Windows 7

You have the option of adding or removing individual program components of the Avira Professional Security installation (see Choosing installation components).


Alle Systemsteuerungselemente
Programme und Funktionen
Programme und Funktionen durchsuc...
Startseite der Systemsteuerung
Installierte Updates anzeigen
Windows-Funktionen aktivieren oder deaktivieren
Organisieren
Deinstallieren
Ändern
Name
Herausgeber
Installiert am
Größe

Programm deinstallieren oder ändern

Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "Deinstallieren", "Ändern" oder "Reparieren", um es zu deinstallieren.

If you wish to add or remove modules of the current installation, you can use the option **Add or Remove Programs** in the **Windows control panel** to **Change/Remove** programs.

- Open the **Control Panel** via the Windows **Start** menu.

  Double click on **Programs and Features**.

  Select Avira Professional Security and click **Change**.

  In the **Welcome** dialog of the program, select the option **Modify**. You will be guided through the installation changes.

Related Topics:
Choosing installation components

3.8.3 Changing an installation under Windows XP

You have the option of adding or removing individual program components of the Avira Professional Security installation (see Choosing installation modules).

If you wish to add or remove modules of the current installation, you can use the option **Add or Remove Programs** in the **Windows control panel** to **Change/Remove** programs.

- Open the **Control Panel** via the Windows **Start > Settings** menu.

  Double click on **Add or Remove Programs**.

  Select Avira Professional Security and click **Change**.

  In the **Welcome** dialog of the program, select the option **Modify**. You will be guided through the installation changes.

Related Topics:
Choosing installation components

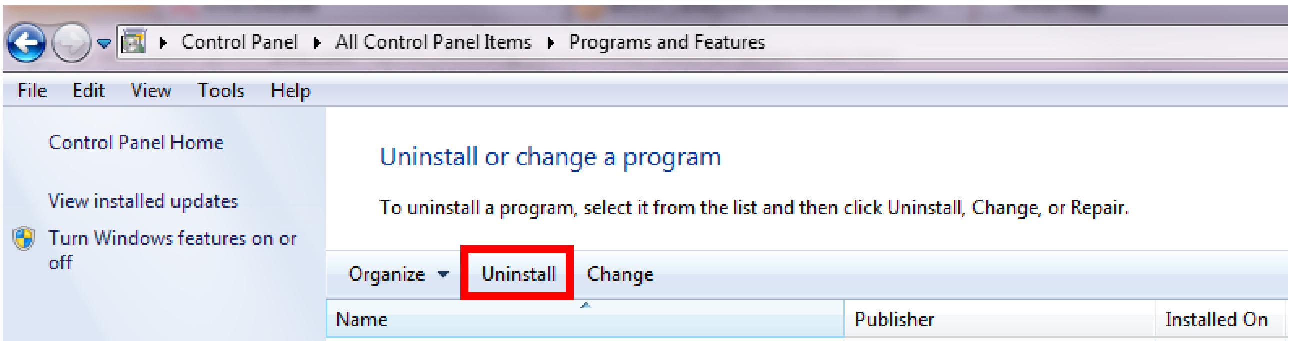
3.9 Uninstalling Avira Professional Security

Should you ever feel the need to uninstall Avira Professional Security, here is how:

- Uninstalling Avira Professional Security under Windows 8
- Uninstalling Avira Professional Security under Windows 7
- Uninstalling Avira Professional Security under Windows XP

3.9.1 Uninstalling Avira Professional Security under Windows 8

To uninstall Avira Professional Security from your computer use the option **Programs and Features** in the Windows Control Panel.


Control Panel ▸ All Control Panel Items ▸ Programs and Features
File Edit View Tools Help
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall
Change
Name
Publisher
Installed On

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

- Right-click on the screen.

The **All apps** symbol appears.

Click on the symbol and look in the *Apps - Windows System* section for **Control Panel**.

Double-click the **Control Panel** symbol.

Click on **Programs - Uninstall a program**.

Click on **Programs and Features - Uninstall a program**.

Select Avira Professional Security in the list and click **Uninstall**.

When asked if you really want to remove the application and all its components, click **Yes** to confirm.

When asked if you want to activate Windows Firewall (the Avira FireWall will be uninstalled), click **Yes** to confirm to keep at least some protection for your system.

All components of the program will be removed.

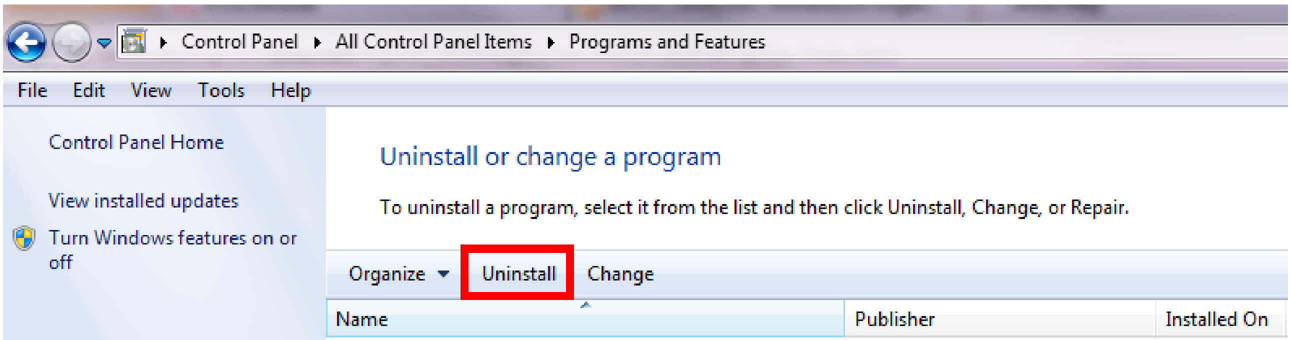
Click **Finish** to complete uninstallation.

If a dialog box appears recommending that your computer be restarted, click **Yes** to confirm.

Avira Professional Security is now uninstalled and all directories, files and registry entries for the program are deleted when your computer is restarted.

3.9.2 Uninstalling Avira Professional Security under Windows 7

To uninstall Avira Professional Security from your computer use the option **Programs and Features** in the Windows Control Panel.


Control Panel ▸ All Control Panel Items ▸ Programs and Features
File
Edit
View
Tools
Help
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
Organize
Uninstall
Change
Name
Publisher
Installed On

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

- Open the **Control Panel** via the Windows **Start** menu.

  Click **Programs and Features**.

  Select Avira Professional Security in the list and click **Uninstall**.

  When asked if you really want to remove the application and all its components, click **Yes** to confirm.

  When asked if you want to activate Windows Firewall (the Avira FireWall will be uninstalled), click **Yes** to confirm to keep at least some protection for your system.

  All components of the program will be removed.

  Click **Finish** to complete uninstallation.

  If a dialog box appears recommending that your computer be restarted, click **Yes** to confirm.

  Avira Professional Security is now uninstalled and all directories, files and registry entries for the program are deleted when your computer is restarted.

3.9.3 Uninstalling Avira Professional Security under Windows XP

To uninstall Avira Professional Security from your computer use the option **Change or Remove Programs** in the Windows Control Panel.

- Open the **Control Panel** via the Windows **Start > Settings** menu.

  Double click on **Add or Remove Programs**.

  Select Avira Professional Security in the list and click **Remove**.

  When asked if you really want to remove the application and all its components, click **Yes** to confirm.

  All components of the program will be removed.

  Click **Finish** to complete uninstallation.

If a dialog box appears recommending that your computer be restarted, click **Yes** to confirm.

Avira Professional Security is now uninstalled and all directories, files and registry entries for the program are deleted when your computer is restarted.

3.9.4 Uninstallation on the network

To uninstall Avira products on the network automatically:

✓ You must have administrator rights (also required in batch mode)

▸ Start the uninstallation with the parameter `/remsilent` or `/remsilentaskreboot` or integrate the parameter into the login script of the server.

You can also specify the parameter for the uninstallation log.

Example: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

↳ The uninstallation starts automatically.

Note
The setup program for the uninstallation should be started on the PC on which the Avira product is to be uninstalled; do not start the setup program from a network drive.

4. Overview of Avira Professional Security

This chapter contains an overview of the functionality and operation of your Avira product.

- see Chapter User interface and operation
- see Chapter How to...?

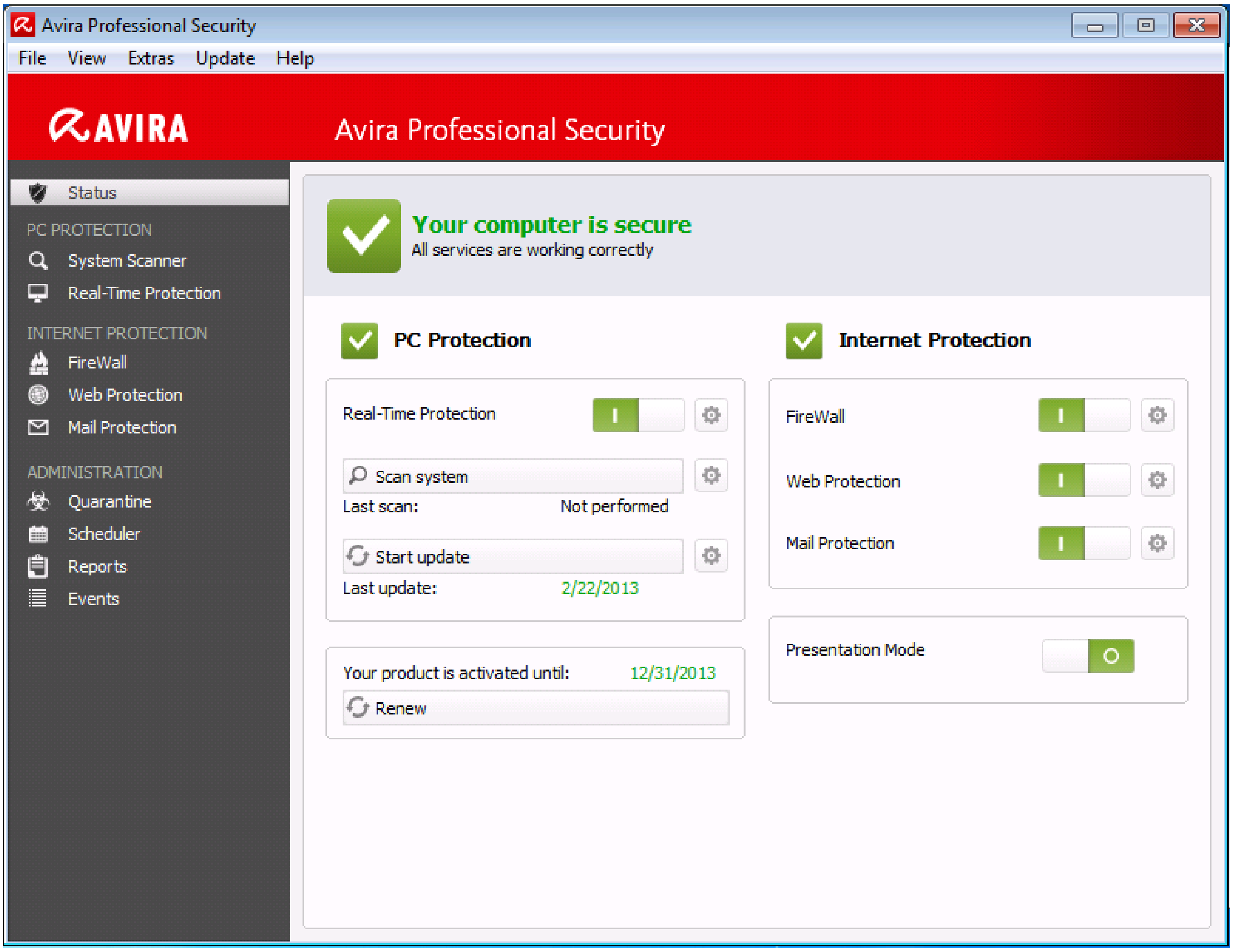
4.1 User interface and operation

You operate your Avira product via three program interface elements:

- Control Center: monitoring and controlling the Avira product
- Configuration: Configuring the Avira product
- Tray Icon in the system tray of the taskbar: Opening the Control Center and other functions

4.1.1 Control Center

The Control Center is designed to monitor the protection status of your computer systems and control and operate the protection components and functions of your Avira product.



The Control Center window is divided into three areas: The **Menu bar**, the **Navigation area** and the detail window **Status**:

- **Menu bar:** In the Control Center menu bar, you can access general program functions and information on the program.
- **Navigation area:** In the navigation area, you can easily swap between the individual sections of the Control Center. The individual sections contain information and functions of the program components and are arranged in the navigation bar according to activity. Example: Activity *PC PROTECTION* - Section **Real-Time Protection**.
- **Status:** The Control Center opens with the **Status** view, where you can see at a glance, if your computer is safe, and you have an overview of the active modulesand the date of the last system scan. The **Status** view also contains buttons for starting features or actions, such as starting or stopping the **Real-Time Protection**.

Starting and closing of Control Center

To start the Control Center the following options are available:

- Double-click the program icon on your desktop
- Via the program entry in the **Start > Programs** menu.
- Via the Tray Icon of your Avira product.

Close the Control Center via the menu command **Close** in the menu **File** or by clicking on the close tab in the Control Center.

Operate Control Center

To navigate in the Control Center

- Select an activity in the navigation bar.
  - ↳ The activity opens and other sections appear. The first section of the activity is selected and displayed in the view.
- If necessary, click another section to display this in the detail window.

> **Note**
> You can activate the keyboard navigation in the menu bar with the help of the [**Alt**] key. If navigation is activated, you can move within the menu with the **arrow** keys. With the **Return** key you activate the active menu item.
> To open or close menus in the Control Center, or to navigate within the menus, you can also use the following key combinations: [**Alt**] + underlined letter in the menu or menu command. Hold down the [**Alt**] key if you want to access a menu, a menu command or a submenu.

To process data or objects displayed in the detail window:

- Highlight the data or object you wish to edit.

  To highlight multiple elements (elements in columns), hold down the **control** key or the **shift** key while selecting the elements.
- Click the appropriate button in the upper bar of the detail window to edit the object.

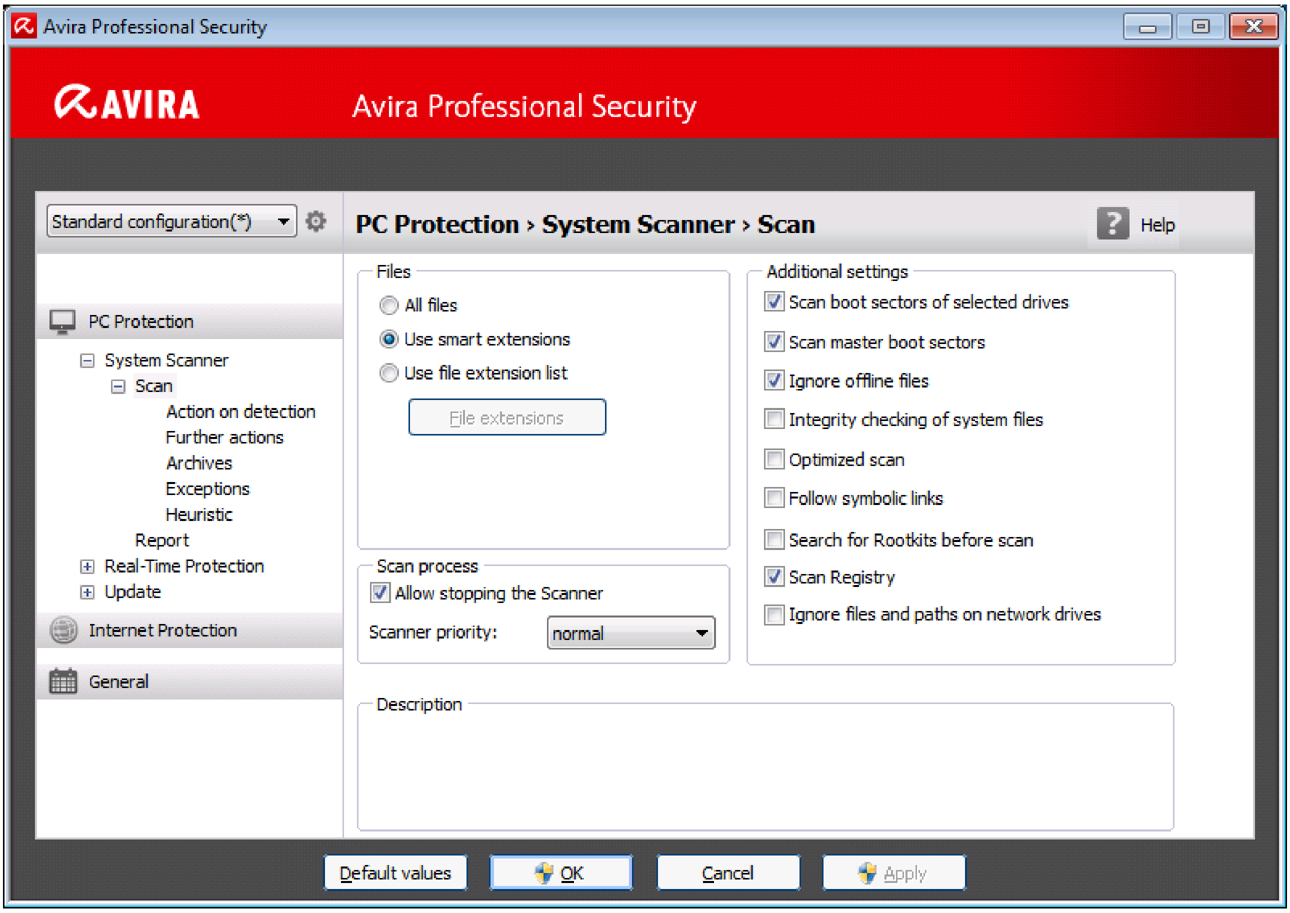
Control Center overview

- **Status**: Clicking on the **Status** bar gives you an overview of the product's functionality and performance (see Status).
  - The **Status** section lets you see at a glance which modules are active and provides information on the last update performed.
- *PC PROTECTION*: In this section you will find the components for checking the files on your computer system for viruses and malware.
  - The System Scanner section enables you to easily configure and start an on-demand scan. Predefined profiles enable a scan with already adapted default options. In the same way it is possible to adapt the scan for viruses and unwanted programs to your personal requirements with the help of manual selection (will be saved) or by creating user-defined profiles.
  - The Real-Time Protection section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".

- *INTERNET PROTECTION*: In this section you will find the components to protect your computer system against viruses and malware from the Internet, and against unauthorized network access.
  - The FireWall section enables you to configure the basic settings for the FireWall. In addition, the current data transfer rate and all active applications using a network connection are displayed.
  - The Web Protection section displays information on scanned URLs and detected viruses, as well as other statistical data, which can be reset at any time and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
  - The Mail Protection section shows you all the emails scanned by Mail Protection, their properties and other statistical data. You can alsoexclude email addresses from future scanning for malware. Emails can also be deleted from the Mail Protection buffer.
- *ADMINISTRATION*: In this section you will find tools for isolating and managing suspicious or infected files, and for planning recurring tasks.
  - The Quarantine section contains the so-called quarantine manager. This is the central point for files already placed in quarantine or for suspect files that you would like to place in quarantine. It is also possible to send a selected file to the Avira Malware Research Center by email.
  - The Scheduler section enables you to configure scheduled scanning and update jobs as well as backup jobs and to adapt or delete existing jobs.
  - The Reports section enables you to view the results of actions performed.
  - The Events section enables you to view events generated by certain program modules.

4.1.2 Configuration

You can define settings for your Avira product in the Configuration. After installation, your Avira product is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for your Avira product may mean you need to adapt the protective components of the program.



Files
- ○ All files
- ● Use smart extensions
- ○ Use file extension list

Additional settings
- ☑ Scan boot sectors of selected drives
- ☑ Scan master boot sectors
- ☑ Ignore offline files
- □ Integrity checking of system files
- □ Optimized scan
- □ Follow symbolic links
- □ Search for Rootkits before scan
- ☑ Scan Registry
- □ Ignore files and paths on network drives

Scan process
- ☑ Allow stopping the Scanner
- Scanner priority: normal

The Configuration opens a dialog box: You can save your configuration settings via the **OK** or **Apply** buttons, delete your settings by clicking the Cancel button or restore your default configuration settings using the **Default values** button. You can select individual configuration sections in the left-hand navigation bar.

Accessing the Configuration

You have several options for accessing the configuration:

- via the Windows control panel.
- via the Windows Security Center - from Windows XP Service Pack 2.
- via the Tray Icon of your Avira product.
- in the Control Center via the menu item Extras > Configuration.
- in the Control Center via the Configuration button.

> **Note**
> If you are accessing configuration via the **Configuration** button in the Control Center, go to the Configuration register of the section which is active in the Control Center.

Configuration operation

Navigate in the configuration window as you would in Windows Explorer:

- Click an entry in the tree structure to display this configuration section in the detail window.
- Click the plus symbol in front of an entry to expand the configuration section and display configuration subsections in the tree structure.
- To hide configuration subsections, click on the minus symbol in front of the expanded configuration section.

> **Note**
> To enable or disable Configuration options and use the buttons, you can also use the following key combinations: [**Alt**] + underlined letter in the option name or button description.

If you want to confirm your Configuration settings:

- Click **OK**.
  - ↳ The configuration window is closed and the settings are accepted.

  - OR -
- Click **Apply**.
  - ↳ The settings are applied. The configuration window remains open.

If you want to finish configuration without confirming your settings:

- Click **Cancel**.
  - ↳ The configuration window is closed and the settings are discarded.

If you want to restore all configuration settings to default values:

- Click **Default values**.
  - ↳ All settings of the configuration are restored to default values. All amendments and custom entries are lost when default settings are restored.

Configuration profiles

You have the option of saving your configuration settings as configuration profiles. In the configuration profile, i.e. of a configuration, all configuration options are saved in a group. The configuration is displayed in the navigation bar as a node. You can add other configurations to the default configuration. You also have the option of defining rules for switching to a specific configuration:
When switching configuration using a rule-based procedure, the configuration can be linked to the use of a LAN or Internet connection (identification via default gateway). In this way, configuration profiles can be created for different laptop usage scenarios:

- Use on company networks: Update via intranet server, Web Protection disabled
- Use at home: Update via default Avira web server, Web Protection enabled

If no switching rules have been defined, you can switch to a configuration manually in the context menu of the tray icon. You can add, rename, delete, copy or restore configurations and define rules for switching configurations using the buttons in the navigation bar, or using commands from the context menu in the configuration section.

> **Note**
> The User Account Control (UAC) will ask for your permission to enable or disable the Real-Time Protection, FireWall, Web Protection and Mail Protection services in operating systems as of Windows Vista.

Overview of configuration options

The following configuration options are available:

- **System Scanner**: Configuration of on-demand scan
  - Scan options
  - Action on detection
  - Further actions
  - Archive scan options
  - System scan exceptions
  - System scan heuristics
  - Report function setting
- **Real-Time Protection**: Configuration of on-access scan
  - Scan options
  - Action on detection
  - Further actions
  - On-access scan exceptions
  - On-access scan heuristics
  - Report function setting
- **Update**: Configuration of the update settings, download via Web server or fileserver
  - Download via fileserver
  - Download via web server
  - Proxy settings
- **Web Protection**: Configuration of Web Protection
  - Scan options, enabling and disabling the Web Protection
  - Action on detection

  - Blocked access: Unwanted file types and MIME types, Web filter for known unwanted URLS (malware, phishing, etc.)
  - Web Protection scan exceptions: URLs, file types, MIME types
  - Web Protection heuristics
  - Report function setting

- **Mail Protection**: Configuration of Mail Protection
  - Scan options: Enable the monitoring of POP3 accounts, IMAP accounts, outgoing emails (SMTP)
  - Actions on detection
  - Further actions
  - Mail Protection scan heuristics
  - AntiBot function: Permitted SMTP servers, permitted email senders
  - Mail Protection scan exceptions
  - Configuration of cache, empty cache
  - Configuration of a footer in sent emails
  - Report function setting
- **General**:
  - Configuration of email using SMTP
  - Threat categories for System Scanner and Real-Time Protection
  - Advanced protection: Options to enable the ProActiv and Protection Cloud features.
  - Application filter: Block or allow applications
  - Password protection for access to the Control Center and the Configuration
  - Security: block autostart function, product protection, protect Windows hosts file
  - WMI: Enable WMI support
  - Event log configuration
  - Configuration of report functions
  - Setting of directories used
  - Alerts:

    Configuration of network alerts for component(s):

    - System Scanner
    - Real-Time Protection

    Configuration of email alerts for component(s):

    - System Scanner
    - Real-Time Protection
    - Updater
  - Configuration of acoustic alerts when malware is detected

4.1.3 Tray icon

After installation, you will see the tray icon of your Avira product in the system tray of the taskbar:

Icon	Description
	Avira Real-Time Protection is enabled and the FireWall is enabled
	Avira Real-Time Protection is disabled or the FireWall is disabled

The tray icon displays the status of the Real-Time Protection and the FireWall service.

Central functions of your Avira product can be quickly accessed via the context menu of the **tray icon**. To open the context menu, click the **tray icon** with the right-hand mouse button.

Entries in the context menu

- **Enable Real-Time Protection**: Enables or disables the Avira Real-Time Protection.
- **Enable Mail Protection**: Enables or disables the Avira Mail Protection.
- **Enable Web Protection**: Enables or disables the Avira Web Protection.
- **FireWall**:
  - **Enable FireWall**: Enables or disables the Avira FireWall
  - **Enable Windows Firewall**: Enables or disables the Windows Firewall (this feature is available starting from Windows 8).
  - **Block all traffic**: Enabled. Blocks all data transfers except transfers to the host computer system (Local Host/IP 127.0.0.1).
- **Start Avira Professional Security**: Opens the Control Center.
- **Configure Avira Professional Security**: Opens the Configuration.
- **Start update:** Starts an update.
- **Select configuration**: Opens a submenu with the available configuration profiles. Click on a configuration to activate this configuration. The menu command is disabled if you have already defined rules for automatic switching to a configuration.
- **Help**: opens the Online Help.
- **About Avira Professional Security:** Opens a dialog box with information on your Avira product: Product information, Version information, License information.
- **Avira on the Internet**: Opens the Avira web portal on the Internet. The condition for this is that you have an active connection to the Internet.

> **Note**
> The User Account Control (UAC) will ask for your permission to enable or disable the Real-Time Protection, FireWall, Web Protection and Mail Protection services in operating systems as of Windows Vista.

4.2 How to...?

The chapters "How to...?" offer short instructions about license and product activation as well as information on the most important functions of your Avira product. The selected short articles serve as an overview about the functionality of your Avira product. They do not substitute the detailed information of each section of this help center.

4.2.1 Activate license

To activate your Avira product's license:

Activate your license for your Avira product with the *.KEY* license file. You can obtain the license file by email from Avira. The license file contains the license for all products that you have ordered in one order process.

If you have not yet installed your Avira product:

- Save the license file to a local directory on your computer.
- Install your Avira product.
- During installation, enter the save location of the license file.

If you have already installed your Avira product:

- Double-click the license file in File Manager or in the activation email and follow the on-screen instructions when License Manager opens.

  - OR -

  In your Avira product's Control Center, select the menu item **Help > Load license file…**

> **Note**
> As of Windows Vista the User Account Control dialog box appears. Log in as administrator if appropriate. Click **Continue**.

- Highlight the license file and click **Open**.

  ↳ A message appears.
- Click **OK** to confirm.

  ↳ The license is activated.

- If necessary, restart your system.

4.2.2 Perform automatic updates

To create a job with the Avira Scheduler to update your Avira product automatically:

- In the Control Center, select the section *ADMINISTRATION* **> Scheduler**.
- Click the + **Insert new job** icon.

  ↳ The dialog box **Name and description of the job** appears.
- Give the job a name and, where appropriate, a description.
- Click **Next**.

  ↳ The dialog box **Type of job** is displayed.
- Select **Update job** from the list.
- Click **Next**.

  ↳ The dialog box **Time of job** appears.
- Select a time for the update:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**
- **Login**

> **Note**
> We recommend regular automatic updates. The recommended update interval is: 60 minutes.

- Where appropriate, specify a date according to the selection.
- Where appropriate, select additional options (availability depends on type of job):

- **Repeat job if time has expired**
  Past jobs are performed that could not be performed at the required time, for example because the computer was switched off.
- **Start job while connecting to the Internet (dial-up)**
  In addition to the defined frequency, the job is performed when an Internet connection is set up.

- Click **Next**.

  ↳ The dialog box **Select display mode** appears.
- Select the display mode of the job window:

- **Invisible**: No job window
- **Minimize**: progress bar only
- **Maximize**: Entire job window

▶ Click **Finish**.

↳ Your newly created job appears on the start page of the *ADMINISTRATION* **> Scheduler** section with the status enabled (check mark).

▶ Where appropriate, deactivate jobs that are not to be performed.

Use the following icons to further define your jobs:

ℹ	View properties of a job
✎	Edit job
✕	Delete job
▶	Start job
■	Stop job

4.2.3 Start a manual update

You have various options for starting an update manually: When an update is started manually, the virus definition file and scan engine are always updated.

To start an update of your Avira product manually:

▶ With the right-hand mouse button, click the Avira tray icon in the taskbar.

↳ A context menu appears.

▶ Select **Start update**.

↳ The **Updater** dialog box appears.

- OR -

▶ In the Control Center, select **Status**.

▶ In the **Last update** field, click on the **Start update** link.

↳ The Updater dialog box appears.

- OR -

▶ In the Control Center, in the **Update** menu, select the menu command **Start update**.

↳ The Updater dialog box appears.

> **Note**
> We recommend regular automatic updates. The recommended update interval is: 60 minutes.

> **Note**
> You can also carry out a manual update directly via the Windows security center.

4.2.4 Using a scan profile to scan for viruses and malware

A scan profile is a set of drives and directories to be scanned.

The following options are available for scanning via a scan profile:

Use predefined scan profile

If the predefined scan profile corresponds to your requirements.

Customize and apply scan profile (manual selection)

If you want to scan with a customized scan profile.

Create and apply new scan profile

If you want to create your own scan profile.

Depending on the operating system, various icons are available for starting a scan profile:

- In Windows XP:

  🔍 This icon starts the scan via a scan profile.

- As of Windows Vista:

  As of Microsoft Windows Vista, the Control Center only has limited rights at the moment, e.g. for access to directories and files. Certain actions and file accesses can only be performed in the Control Center with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

  - 🔍This icon starts a limited scan via a scan profile. Only directories and files that the operating system has granted access rights to are scanned.
  - 🔍This icon starts the scan with extended administrator rights. After confirmation, all directories and files in the selected scan profile are scanned.

To scan for viruses and malware with a scan profile:

- Go to Control Center and select the section *PC PROTECTION* **> System Scanner**.

↳ Predefined scan profiles appear.

- Select one of the predefined scan profiles.

  -OR-

  Adapt the scan profile **Manual selection**.

  -OR-

  Create a new scan profile

- Click the icon (Windows XP: 🔍 or as of Windows Vista: 🔍).
- The **Luke Filewalker** window appears and a system scan is started.

  ↳ When the scan is completed, the results are displayed.

If you want to adapt a scan profile:

- In the scan profile **Manual Selection**, expand the file tree so that all the drives and directories you want to scan are open.
- Click the **+** icon: The next directory level is displayed.
- Click the **-** icon: The next directory level is hidden.
- Highlight the nodes and directories you want to scan by clicking on the relevant box of the appropriate directory level:

  The following options are available for selecting directories:

- Directory, including sub-directories (black check mark)
- Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
- No directory (no check mark)

If you want to create a new scan profile:

- Click the icon + **Create new profile**.

  ↳ The profile **New profile** appears below the profiles previously created.

- Where appropriate, rename the scan profile by clicking on the icon ▭.
- Highlight the nodes and directories to be saved by clicking the check box of the respective directory level.

  The following options are available for selecting directories:

- Directory, including sub-directories (black check mark)
- Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
- No directory (no check mark)

4.2.5 Scan for viruses and malware using drag & drop

To scan for viruses and malware systematically using drag & drop:

✓ The Control Center of your Avira product has been opened.

- Highlight the file or directory you want to scan.
- Use the left-hand mouse button to drag the highlighted file or directory into the **Control Center**.
  - ↳ The **Luke Filewalker** window appears and a system scan is started.
  - ↳ When the scan is completed, the results are displayed.

4.2.6 Scan for viruses and malware via the context menu

To scan for viruses and malware systematically via the context menu:

- Click with the right-hand mouse button (e.g. in Windows Explorer, on the desktop or in an open Windows directory) on the file or directory you want to scan.
  - ↳ The Windows Explorer context menu appears.
- Select **Scan selected files with Avira** in the context menu.
  - ↳ The **Luke Filewalker** window appears and a system scan is started.
  - ↳ When the scan is completed, the results are displayed.

4.2.7 Automatically scan for viruses and malware

> **Note**
> After installation, the scan job **Full system scan** is created in the Scheduler: A complete system scan is automatically performed at a recommended interval.

To create a job to automatically scan for viruses and malware:

- In the Control Center, select the section *ADMINISTRATION* **> Scheduler**.
- Click the icon ⊞.
  - ↳ The dialog box **Name and description of job** appears.
- Give the job a name and, where appropriate, a description.
- Click **Next**.
  - ↳ The dialog box **Type of job** appears.
- Select **Scan job**.
- Click **Next**.
  - ↳ The dialog box **Selection of the profile** appears.

- Select the profile to be scanned.
- Click **Next**.
  - ↳ The dialog box **Time of the job** appears.
- Select a time for the scan:

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Single**
- **Login**

- Where appropriate, specify a date according to the selection.
- Where appropriate, select the following additional options (availability depends on job type):

Repeat job if the time has already expired

Past jobs are performed that could not be performed at the required time, for example because the computer was switched off.

- Click **Next**.
  - ↳ The dialog box **Selection of the display mode** appears.
- Select the display mode of the job window:

- **Invisible**: No job window
- **Minimized**: progress bar only
- **Maximized**: Entire job window

- Select the **Shut down computer if job is done** option if you want the computer to shut down automatically when the scan is finished. This option is only available if the display mode is set to minimized or maximized.
- Click **Finish**.
  - ↳ Your newly created job appears on the start page of the *ADMINISTRATION* **> Scheduler** section with the status enabled (check mark).
- Where appropriate, deactivate jobs that are not to be performed.

Use the following icons to further define your jobs:

ℹ View properties of a job

✎ Edit job

✕ Delete job

▶ Start job

■ Stop job

4.2.8 Targeted scan for Rootkits and active malware

To scan for active rootkits, use the predefined scan profile **Scan for Rootkits and active malware**.

To scan for active rootkits systematically:

- Go to Control Center and select the section *PC PROTECTION* **> System Scanner**.
  - ↪ Predefined scan profiles appear.
- Select the predefined scan profile **Scan for Rootkits and active malware**.
- Where appropriate, highlight other nodes and directories to be scanned by clicking the check box of the directory level.
- Click the icon (Windows XP: 🔍 or as of Windows Vista: 🔍).
  - ↪ The **Luke Filewalker** window appears and a system scan is started.
  - ↪ When the scan is completed, the results are displayed.

4.2.9 React to detected viruses and malware

For the individual protection components of your Avira product, you can define how your Avira product reacts to a detected virus or unwanted program in the **Configuration** under the section **Action on detection**.

No configurable action options are available for the ProActiv component of the Real-Time Protection: Notification of a detection is always given in the **Real-Time Protection: Suspicious application behavior** window.

Action options for the System Scanner:

Interactive

In interactive action mode, the results of the System Scanner scan are displayed in a dialog box. This option is enabled as the default setting.

In the case of **System Scanner scan**, you will receive an alert with a list of the affected files when the scan is complete. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the System Scanner.

Automatic

In automatic action mode, when a virus or unwanted program is detected the action you selected in this area is executed automatically. If you enable the option **Display detection alerts**, you will receive an alert whenever a virus is detected, indicating the action performed.

Action options for the Real-Time Protection:

Interactive

In interactive action mode, data access is denied and a desktop notification is displayed. In the desktop notification you can remove the malware detected or transfer the malware to the System Scanner component using the **Details** button for further virus management. The System Scanner opens a window containing notification of the detection, which gives you various options for managing the affected file via a context menu (see Detection > System Scanner):

Automatic

In automatic action mode, when a virus or unwanted program is detected, the action you selected in this area is executed automatically. If you enable the option **Display detection alerts**, you will receive a desktop notification whenever a virus is detected.

Action options for Mail Protection, Web Protection:

Interactive

In interactive action mode, if a virus or unwanted program is detected, a dialog box appears in which you can select what to do with the infected object. This option is enabled as the default setting.

Automatic

In automatic action mode, when a virus or unwanted program is detected the action you selected in this area is executed automatically. If you enable the **Show progress bar** option, you will receive an alert when a virus is detected. The alert will allow you to confirm the action to be performed.

In interactive action mode, you can react to detected viruses and unwanted programs by selecting an action for the infected object in the alert and executing the selected action by clicking **Confirm**.

The following actions for handling infected objects are available for selection:

> **Note**
> Which actions are available for selection depends on the operating system, the protection components (Avira Real-Time Protection, Avira System Scanner, Avira Mail Protection, Avira Web Protection) reporting the detection, and the type of malware detected.

Actions of the System Scanner and the Real-Time Protection (not ProActiv detections):

Repair

The file is repaired.

This option is only available if the infected file can be repaired.

Rename

The file is renamed with a **.vir* extension. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can be repaired and given their original name at a later time.

Quarantine

The file is packaged into a special format (**.qua*) and moved to the Quarantine directory *INFECTED* on your hard disk, so that direct access is no longer possible. Files in this directory can be repaired in Quarantine at a later data or, if necessary, sent to Avira.

Delete

The file will be deleted. This process is much quicker than **Overwrite and delete**. If a boot sector virus is detected, this can be deleted by deleting the boot sector. A new boot sector is written.

Ignore

No further action is taken. The infected file remains active on your computer.

> **Warning**
> This could result in loss of data and damage to the operating system! Only select the **Ignore** option in exceptional cases.

Overwrite and delete

The file is overwritten with a default template and then deleted. It cannot be restored.

Always ignore

Action option for Real-Time Protection detections: No further action is taken by Real-Time Protection. Access to the file is permitted. All further access to this file is permitted and no further notifications will be provided until the computer is restarted or the virus definition file is updated.

> **Warning**
> This could result in loss of data and damage to the operating system! Only select the **Always ignore** option in exceptional cases.

Copy to quarantine

Action option for a rootkits detection: The detection is copied to quarantine.

Repair boot sector | Download repair tool

Action options when infected boot sectors are detected: A number of options are available for repairing infected diskette drives. If your Avira product is unable to perform the repair, you can download a special tool for detecting and removing boot sector viruses.

> **Note**
> If you carry out actions on running processes, the processes in question are terminated before the actions are performed.

Actions of the Real-Time Protection for detections made by the ProActiv component (notification of suspicious actions of an application):

Trusted program

The application continues to run. The program is added to the list of permitted applications and is excluded from monitoring by the ProActiv component. When adding to the list of permitted applications, the monitoring type is set to *Content*. This means that the application is only excluded from monitoring by the ProActiv component if the content remains unchanged (see Application filter: Applications to be skipped).

Block program once

The application is blocked, i.e. the application is terminated. The actions of the application continue to be monitored by the ProActiv component.

Always block this program

The application is blocked, i.e. the application is terminated. The program is added to list of blocked applications and can no longer be run (see Application filter: Applications to be blocked).

Ignore

The application continues to run. The actions of the application continue to be monitored by the ProActiv component.

Mail Protection actions: Incoming emails

Move to quarantine

The email including all attachments is moved to quarantine. The affected email is deleted. The body of the text and any attachments of the email are replaced by a default text.

Delete mail

The affected email is deleted. The body of the text and any attachments of the email are replaced by a default text.

Delete attachment

The infected attachment is replaced by a default text. If the body of the email is affected, it is deleted and also replaced by a default text. The email itself is delivered.

Move attachment to quarantine

The infected attachment is placed in quarantine and then deleted (replaced by a default text). The body of the email is delivered. The affected attachment can later be delivered via the quarantine manager.

Ignore

The affected email is delivered.

> **Warning**
> This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases. Disable the preview in your mail client, never open any attachments with a double click!

Mail Protection actions: Outgoing emails

Move mail to quarantine (do not send)

The email, together with all attachments, is copied to Quarantine and is not sent. The email remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

Block sending of mails (do not send)

The email is not sent and remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

Ignore

The affected email is sent.

> **Warning**
> Viruses and unwanted programs can penetrate the computer system of the email recipient in this way.

Web Protection actions:

Deny access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser.

Move to quarantine

The website requested from the web server and/or any data or files transferred are moved to quarantine. The affected file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center.

Ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by Web Protection to your web browser.

Warning
This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases.

Note
We recommend that you move any suspicious file that cannot be repaired to quarantine.

Note
You can also send files reported by the heuristic to us for analysis.
For example, you can upload these files to our website:
http://www.avira.com/sample-upload
You can identify files reported by the heuristic from the designation *HEUR/* or *HEURISTIC/* that prefixes the file name, e.g.: *HEUR/testfile.**.

4.2.10 Handling quarantined files (*.qua)

To handle quarantined files:

- In the Control Center, select the section *ADMINISTRATION* **> Quarantine** section.
- Check which files are involved, so that, if necessary, you can reload the original back onto your computer from another location.

If you want to see more information on a file:

- Highlight the file and click on 𝑖 .
  - ↳ The dialog box **Properties** appears with more information on the file.

If you want to rescan a file:

Scanning a file is recommended if the virus definition file of your Avira product has been updated and a false positive report is suspected. This enables you to confirm a false positive with a rescan and restore the file.

- Highlight the file and click on 🔍 .
  - ↳ The file is scanned for viruses and malware using the system scan settings.
  - ↳ After the scan, the dialog **Rescan statistics** appears which displays statistics on the status of the file before and after the rescan.

To delete a file:

- Highlight the file and click on ✕ .
- You have to confirm your choice with **Yes**.

If you want to upload the file to a Avira Malware Research Center web server for analysis:

- Highlight the file you want to upload.
- Click on ✉ .
  - ↳ A dialog opens with a form for inputting your contact data.
- Enter all the required data.
- Select a type: **Suspicious file** or **Suspicion of false positive**.
- Select a response format: **HTML**, **Text**, **HTML & Text**.
- Click **OK.**
  - ↳ The file is uploaded to a Avira Malware Research Center web server in compressed form.

> **Note**
> In the following cases, analysis by the Avira Malware Research Center is recommended:
> **Heuristic hits (Suspicious file)**: During a scan, a file has been classified as suspicious by your Avira product and moved to quarantine: Analysis of the file by the Avira Malware Research Center has been recommended in the virus detection dialog box or in the report file generated by the scan.
> **Suspicious file**: You consider a file to be suspicious and have therefore moved this file to quarantine, but a scan of the file for viruses and malware is negative.
> **Suspicion of false positive**: You assume that a virus detection is a false

positive: Your Avira product reports a detection in a file, which is very unlikely to have been infected by malware.

Note
The size of the files you upload is limited to 20 MB uncompressed or 8 MB compressed.

If you want to copy a quarantined object from quarantine to another directory:

- Highlight the quarantined object and click on .
  - ↳ The dialog *Browse For Folder* opens from which you can select a directory.
- Select a directory where you want to save a copy of the quarantined object and confirm your selection.
  - ↳ The selected quarantined object is saved to the selected directory.

Note
The quarantined object is not identical to the restored file. The quarantined object is encrypted and cannot be executed or read in its original format.

If you want to export the properties of a quarantined object to a text file:

- Highlight the quarantined object and click on .
  - ↳ The text file *quarantaene - Notepad* opens containing the data from the selected quarantined object.
- Save the text file.

You can also restore the files in quarantine (see Chapter: Quarantine: Restore the files in quarantine).

4.2.11 Restore the files in quarantine

Different icons control the restore procedure, depending on the operating system:

- In Windows XP:
  - This icon restores the files to their original directory.
  - This icon restores the files to a directory of your choice.
- As of Windows Vista:

  As of Microsoft Windows Vista, the Control Center only has limited rights at the moment, e.g. for access to directories and files. Certain actions and file accesses can only be performed in the Control Center with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

- ↻ This icon restores the files to a directory of your choice.
- ↻ This icon restores the files to their original directory. If extended administrator rights are necessary to access this directory, a corresponding request appears.

To restore files in quarantine:

> **Warning**
> This could result in loss of data and damage to the operating system of the computer! Only use the function **Restore selected object** in exceptional cases. Only restore files that could be repaired by a new scan.

✓ File rescanned and repaired.

▶ In the Control Center, select the section *ADMINISTRATION* **> Quarantine** section.

> **Note**
>
> Emails and email attachments can only be restored using the option ↻ if the file extension is **.eml*.

To restore a file to its original location:

▶ Highlight the file and click the icon (Windows XP: ↻ , as of Windows Vista ↻).

This option is not available for emails.

> **Note**
>
> Emails and email attachments can only be restored using the option ↻ if the file extension is **.eml*.

↳ A message appears asking if you want to restore the file.

▶ Click **Yes**.

↳ The file is restored to the directory it was in before it was moved to quarantine.

To restore a file to a specified directory:

▶ Highlight the file and click on ↻ .

↳ A message appears asking if you want to restore the file.

- Click **Yes**.
    - ↳ The Windows default window *Save As* for selecting the directory appears.
- Select the directory to restore the file to and confirm.
    - ↳ The file is restored to the selected directory.

4.2.12 Move suspicious files to quarantine

To move a suspect file to quarantine manually:

- In the Control Center, select the section *ADMINISTRATION* **> Quarantine** section.
- Click on + .
    - ↳ The Windows default window for selecting a file appears.
- Select the file and confirm with **Open**.
    - ↳ The file is moved to quarantine.

You can scan files in quarantine with the Avira System Scanner (see Chapter: Quarantine: Handling quarantined files (*.qua)).

4.2.13 Amend or delete file type in a scan profile

To stipulate additional file types to be scanned or exclude specific file types from the scan in a scan profile (only possible for manual selection and customized scan profiles):

- ✓ In the Control Center, go to the *PC PROTECTION* **> System Scanner** section.
- With the right-hand mouse button, click on the scan profile you want to edit.
    - ↳ A context menu appears.
- Select **File filter**.
- Expand the context menu further by clicking on the small triangle on the right-hand side of the context menu.
    - ↳ The entries **Default**, **Scan all files** and **User-defined** appear.
- Select **User-defined**.
    - ↳ The **File extensions** dialog box appears with a list of all file types to be scanned with the scan profile.

If you want to exclude a file type from the scan:

- Highlight the file type and click **Delete**.

If you want to add a file type to the scan:

- Highlight a file type.
- Click **Insert** and enter the file extension of file type into the input box.

Use a maximum of 10 characters and do not enter the leading dot. Wildcards (`*` and `?`) are allowed.

4.2.14 Create desktop shortcut for scan profile

You can start a system scan directly from your desktop via a desktop shortcut to a scan profile without accessing your Avira product’s Control Center.

To create a desktop shortcut to the scan profile:

✓ In the Control Center, go to the *PC PROTECTION* **> System Scanner** section.

▶ Select the scan profile for which you want to create a shortcut.

▶ Click the icon ↖ .

↳ The desktop shortcut is created.

4.2.15 Filter events

Events that have been generated by program components of your Avira product are displayed in the Control Center under *ADMINISTRATION* **> Events** (analogous to the event display of your Windows operating system). The program components, in alphabetical order, are the following:

- FireWall
- Helper Service
- Mail Protection
- Real-Time Protection
- Scheduler
- System Scanner
- Updater
- Web Protection
- ProActiv

The following event types are displayed:

- *Information*
- *Warning*
- *Error*
- *Detection*

To filter displayed events:

▶ In the Control Center, select the section *ADMINISTRATION* **> Events**.

- Check the box of the program components to display the events of the activated components.

  - OR -

  Uncheck the box of the program components to hide the events of the deactivated components.
- Check the event type box to display these events.

  - OR -

  Uncheck the event type box to hide these events.

4.2.16 Exclude email addresses from scan

To define which email addresses (senders) are excluded from the Mail Protection scan (white listing):

- Go to Control Center and select the section *INTERNET PROTECTION* **> Mail Protection**.

  ↳ The list shows incoming emails.
- Highlight the email you want to exclude from the Mail Protection scan.
- Click the icon to exclude the email from the Mail Protection scan:
- The selected email address will no longer be scanned for viruses and unwanted programs.

  ↳ The email sender address is included in the exclusion list and no longer scanned for viruses, malware .

Warning
Only exclude email addresses from the Mail Protection scan if the senders are completely trustworthy.

Note
In the Configuration, under Mail Protection > General > Exceptions, you can add other email addresses to the exclusion list or remove email addresses from the exclusion list.

4.2.17 Select the security level for the FireWall

There are various security levels to choose from. Depending on which you choose, you have different adapter rule configuration options.

The following security levels are available:

Low

Flooding and port scan are detected.

Medium

Suspicious TCP and UDP packages are discarded.

Flooding and port scan are prevented.

High

Computer is not visible on the network.

New connections from outside are not allowed.

Flooding and port scan are prevented.

Custom

User-defined rules: If this security level is selected, the program automatically recognizes that the adapter rules have been modified.

Block all

All existing network connections will be closed.

> **Note**
> The default security level setting for all predefined rules of the Avira FireWall is **Medium**.

To define the security level for the FireWall:

- Go to the Control Center and select the section *INTERNET PROTECTION* **> FireWall**.
- Move the slider to the required security level.
  - ↳ The selected security level is applied immediately.

5. Detection

5.1 Overview

When a virus is detected, your Avira can automatically execute certain actions or respond interactively. In interactive action mode, a dialog opens when a virus is detected in which you can control or initiate the subsequent handling of the virus (delete, ignore, etc). There is an option in automatic mode for displaying an alert when a virus is detected. The action that was automatically executed is displayed in the message.

This chapter contains comprehensive information, arranged according to module, on detection messages.

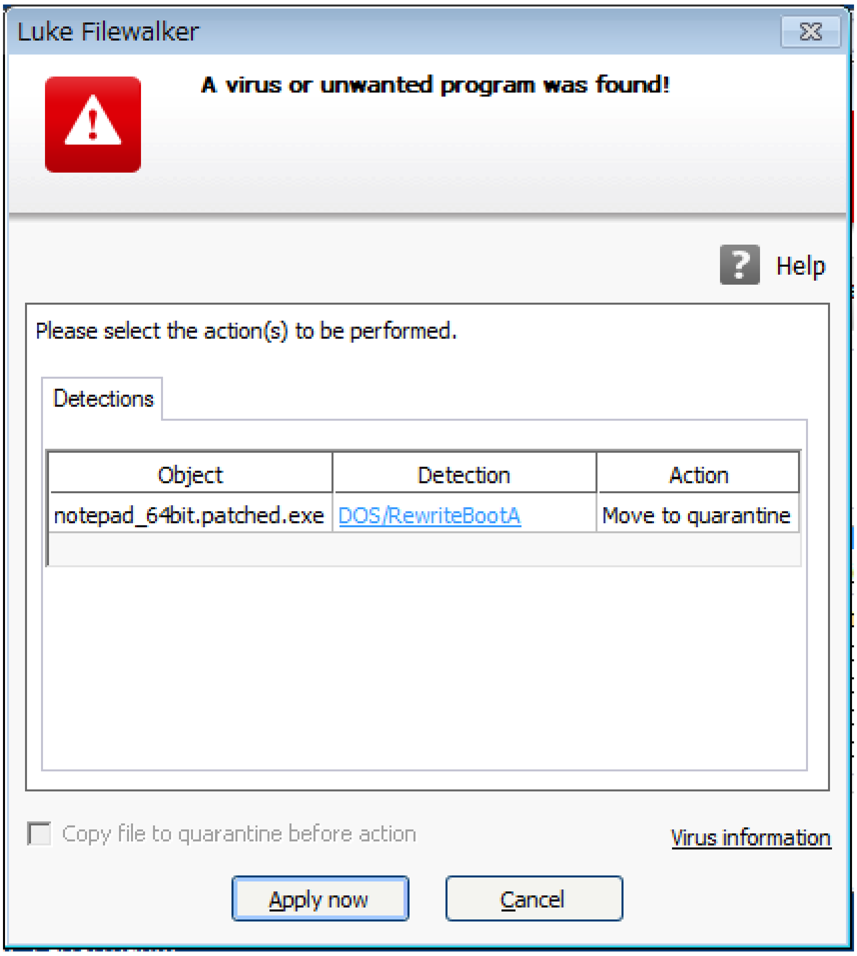
- see Chapter System Scanner: Interactive action mode
- see Chapter System Scanner: Automatic action mode
- see Chapter System Scanner: Sending files to Protection Cloud
- see Chapter Real-Time Protection
- see Chapter Real-Time Protection: Suspicious behavior
- see Chapter Mail Protection: Incoming emails
- see Chapter Mail Protection: Outgoing emails
- see Chapter Sending email: Server
- see Chapter Sending email: Sender
- see Chapter Web Protection

5.2 Interactive action mode

If you selected *Interactive* mode as the action mode when a virus is detected, you will receive an alert containing a list of the affected files when the scan is complete (see the configuration section System Scanner > Scan > Action on detection).
You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the System Scanner.

Note
If reporting is enabled, the System Scanner enters each detection in the Report file.

5.2.1 Alert



Luke Filewalker

A virus or unwanted program was found!

Please select the action(s) to be performed.

Object	Detection	Action
notepad_64bit.patched.exe	DOS/RewriteBootA	Move to quarantine

□ Copy file to quarantine before action

5.2.2 Detection, Errors, Warnings

Detailed information, action options for the detected viruses and messages will be displayed in the **Detection**, **Errors** and **Warnings** tabs:

- **Detection:**
  - *Object:* File name of the affected file
  - *Detection:* Name of the virus or unwanted program
  - *Action:* Selected action with which the affected file is to be handled
    You can choose other actions for dealing with the malware from the context menu associated with the displayed action.
- **Error:** Messages about errors that occurred during the scan
- **Alerts:** Alerts relating to the viruses that were detected

> **Note**
> The following information is displayed in the tooltip for the object: Name of the

affected file and full path, name of the virus and action that is executed with the **Apply Now** button.

Note
The default action of the System Scanner is displayed as the action to be executed. The default action of System Scanner for handling affected files can be set under the configuration section System Scanner > Scan > Action on detection in the *Permitted Actions* area.

5.2.3 Context menu actions

Note
If the detection is a heuristic hit (HEUR/), an unusual runtime packer (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), in interactive mode only the options Move to quarantine and Ignore are available. In automatic mode the detection is automatically moved to Quarantine.
This restriction prevents the detected files, which may be a false alarm, being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the Quarantine Manager.
Depending on the configuration, various options may not be available.

Repair

If this option is enabled, the Scanner repairs the affected file.

Note
The option **Repair** can only be enabled if a repair of the detected file is possible.

Quarantine

If this option is enabled, the Scanner moves the file to quarantine. The file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center. Depending on the file, further selection options may be available in the Quarantine Manager.

Delete

If this option is enabled, the file is deleted. This process is much quicker than "overwrite and delete".

Overwrite and delete

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Always ignore

Action option for Real-Time Protection detections: No further action is taken by Real-Time Protection. Access to the file is permitted. All further access to this file is permitted and no further notifications will be provided until the computer is restarted or the virus definition file is updated.

> **Warning**
> If you select the option **Ignore** or **Always ignore**, the affected files remain active on your computer! It may cause serious damage on your workstation!

5.2.4 Special features when infected boot sectors, rootkits and active malware are detected

Action options are available for repairing infected boot sectors when they are detected:

Repair 722 KB | 1.44 MB | 2.88 MB | 360 KB | 1.2 MB boot sector

These options are available for diskette drives.

Download rescue CD

This option will take you to the Avira website, from where you can download a special tool for detecting and removing boot sector viruses.

If you carry out actions on running processes, the processes in question are terminated before the actions are carried out.

5.2.5 Buttons and links

Button / link	Beschreibung
Apply Now	The selected actions are executed to handle all affected files.
Cancel	The Scanner is closed without further action. The affected files are left unchanged on your computer system.
	This page of the online help is opened via this button or link.

> **Warning**
> Only execute the *Cancel* action in exceptional cases. The affected files remain active on your workstation after you cancel! It may cause serious damage on your workstation!

5.2.6 Special features when malware is detected while Web Protection is inactive

If you have disabled the Web Protection, the System Scanner reports active malware it has detected via a slide-up while scanning the system. Prior to repairing your system you can create a restore point.

✓ First you have to enable System Restore on your Windows system.

▶ Click **Details** in the slide up.

↳ The window *System is being scanned* is displayed.

▶ Enable **Create system restore point before repair**.

▶ Click **Apply**.

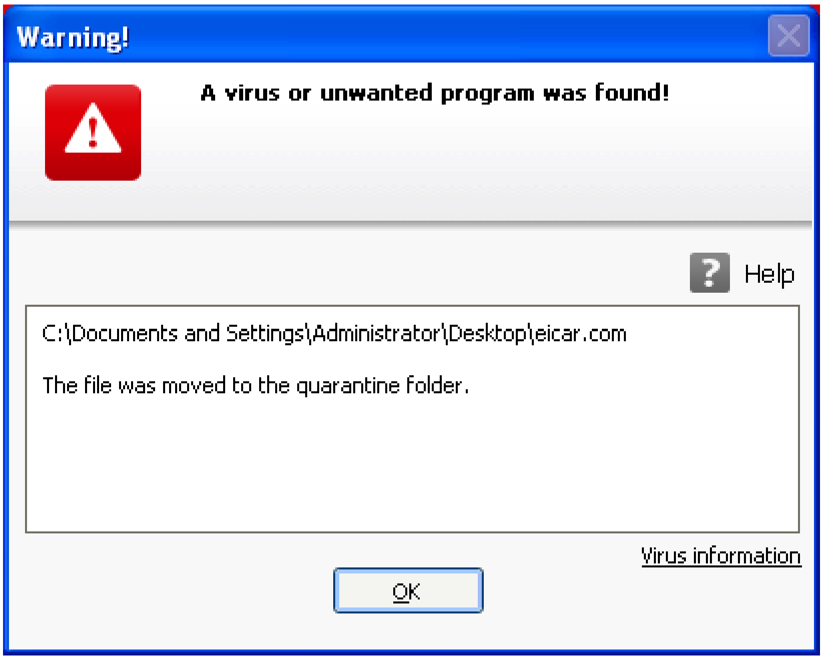
↳ A system restore point has been created. Now you can perform a system restore using the Windows Control Panel if necessary.

5.3 Automatic action mode

If you selected *Automatic* mode and the option *Display alert* as the action mode when a virus is detected, you will receive an alert each time the System Scanner detects a virus in the file (see the configuration section System Scanner > Scan > Action on detection).
There is no selection option for handling the detected virus in automatic mode with alert. The action that was selected in the configuration for dealing with a virus is performed. The action that was automatically executed is displayed in the message.

Note
If reporting is enabled, the System Scanner enters each detection in the Report file.

5.3.1 Alert



Warning!

A virus or unwanted program was found!

C:\Documents and Settings\Administrator\Desktop\eicar.com

The file was moved to the quarantine folder.

5.3.2 Buttons and links

Button / link	Description
? Help	This page of the online help is opened via this button or link.

5.4 Sending files to Protection Cloud

A list of file locations frequently targeted by malware is generated when the **Quick system scan** job runs. The list includes running processes, programs that run at start-up and services. Unknown program files are uploaded to the Avira Protection Cloud for analysis.

If you enabled the option **Confirm manually when sending suspicious files to Avira** during the custom installation or later in the **Advanced Protection** configuration, you see a list of the suspicious files that should be sent to the Protection Cloud, and you can choose which files you want to send. By default, all suspicious files are marked to be sent to Avira Protection Cloud, for further analysis.

Note
If you enabled the **Extended** reporting mode, the System Scanner logs each detection in the Report file and adds the *(Cloud)* suffix to the detections made by the Protection Cloud.

5.4.1 Displayed information

The list of suspicious files to be sent to Avira Protection Cloud.

- *Send:* You can select which files will be sent to Avira Protection Cloud.
- *File:* The name of the suspicious file.
- *Path:* The path to the suspicious file.

Always send files automatically

If this option is enabled, the suspicious files will be sent to the Protection Cloud for analysis directly after each **Quick system scan**, without asking for manual confirmation.

5.4.2 Buttons and links

Button / link	Description
Send	The selected files are sent to Avira Protection Cloud.
Cancel	The System Scanner is closed without further action. The suspicious files are left unchanged on your computer system.
Help	This page of the online help is opened.
About Protection Cloud	The Avira Protection Cloud web page is opened.

Related topics:

- Advanced Protection configuration
- Custom installation
- Report configuration
- Reports view

5.5 Real-Time Protection

If viruses are detected by Real-Time Protection, file access is denied and a desktop notification is displayed, if you have selected *interactive* mode as the action mode for virus detections, or the *automatic* mode with the **Display alert** option (see the Configuration section Real-Time Protection > Scan > Action on detection).

Notification

The following information is displayed in the notification:

- Date and time of the detection
- Path and name of the affected file
- Name of the malware

> **Note**
> When the default start mode for Real-Time Protection (Normal start) has been chosen and the logon process upon startup is carried out fast, programs configured to start automatically upon startup might not be scanned because they might be up and running before the Real-Time Protection has been started completely.

In interactive mode you have the following options:

Remove

The affected file is transferred to the System Scanner component and deleted by the System Scanner. No further message appears.

Details

The affected file is transferred to the System Scanner component. The System Scanner opens a window containing notification of the detection and various options for managing the affected file.

> **Note**
> Please note the information on virus management under Detection > System Scanner.

> **Note**
> For virus management, the action which you selected as the default action in the Configuration under Real-Time Protection > Scan > Action on detection is displayed. Further actions can be selected via the context menu.

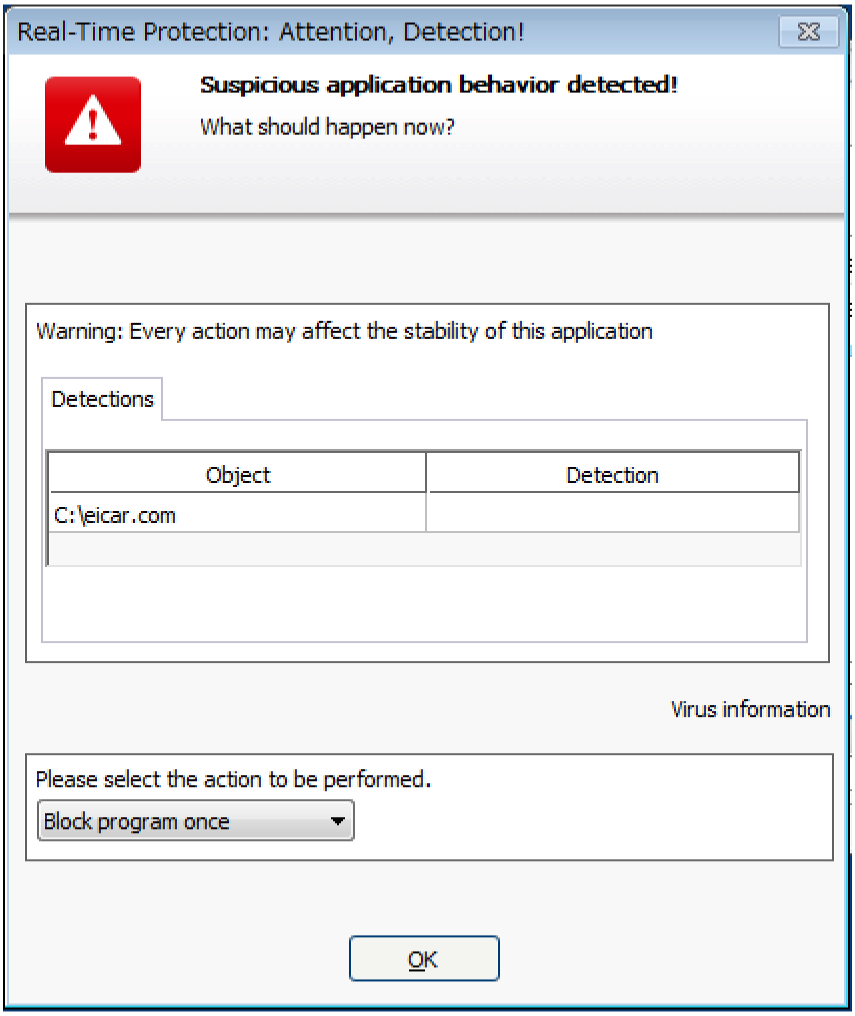
Close

The message is closed. Virus management is terminated.

5.6 Suspicious behavior

If you enable the ProActiv component of Real-Time Protection, application actions are monitored and scanned for suspicious behavior typical of malware. You will receive an alert if suspicious behavior is detected in an application. You have various options for how to handle the detection.

5.6.1 Alert of Real-Time Protection: Suspicious application behavior detected


Real-Time Protection: Attention, Detection!

Suspicious application behavior detected!

What should happen now?

Warning: Every action may affect the stability of this application

Detections

Object	Detection
C:\eicar.com	

Virus information

Please select the action to be performed.

Block program once

5.6.2 Name and path of the currently detected suspicious program

The name and path of the application executing suspicious actions are displayed in the middle window of the message.

5.6.3 Options

Trusted program

If this option is enabled, the application continues to run. The program is added to the list of permitted applications and is excluded from monitoring by the ProActiv component. When adding to the list of permitted applications, the monitoring type is set to *Content*. This means that the application is only excluded from monitoring by the ProActiv component if the content remains unchanged (see Configuration > General > Advanced protection > Application filter: Allowed applications).

Block program once

If this option is enabled, the application is blocked, i.e. the application is terminated. The actions of the application continue to be monitored by the ProActiv component.

Always block this program

If this option is enabled, the application is blocked, i.e. the application is terminated. The program is added to list of blocked applications and can no longer be run (see Configuration > General > Advanced protection > Application filter: Applications to be blocked).

Ignore

If this option is enabled, the application continues to run. The actions of the application continue to be monitored by the ProActiv component.

5.6.4 Buttons and links

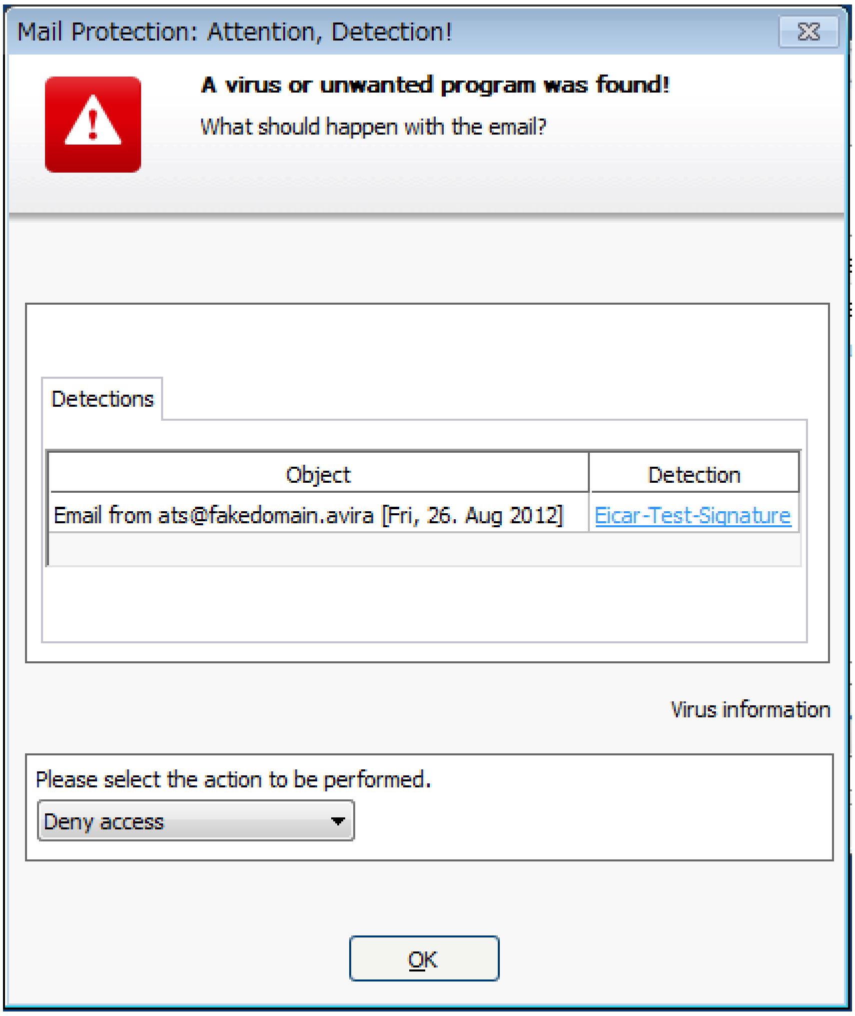
Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

5.7 Incoming emails

If the Mail Protection detects a virus, you will receive an alert if you selected *interactive* mode as the action mode when a virus is detected (see configuration section Mail Protection > Scan > Action on detection). In interactive mode you can choose what to do with the email or attachment in the dialog box.

You will receive the alert shown below if a virus is detected in an incoming email.

5.7.1 Alert



A virus or unwanted program was found!

What should happen with the email?

Object	Detection
Email from ats@fakedomain.avira [Fri, 26. Aug 2012]	Eicar-Test-Signature

Please select the action to be performed.

Deny access

5.7.2 Detections, Errors, Warnings

Messages and more detailed information about the emails in question will be displayed in the **Detections**, **Errors** and **Warnings** tabs:

- **Detections:** Object: Email in question, showing the name of the sender and the time the email was sent

  Detection: Name of the detected virus or unwanted program
- **Error:** Messages concerning errors that occurred during the Mail Protection scan
- **Alerts:** Alerts relating to the affected objects

5.7.3 Options

Note
If a detection is a heuristic hit (HEUR/), an unusual runtime packer (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), in interactive mode only the options Move to quarantine and Ignore are available. In automatic mode the detection is automatically moved to Quarantine.
This restriction prevents the detected files, which may be a false alarm, being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the quarantine manager.

Move to quarantine

If this option is enabled, the email including all attachments is moved to quarantine. It can later be delivered via the quarantine manager. The affected email is deleted. The body of the text and any attachments of the email are replaced by a default text.

Delete email

If this option is enabled, the affected email is deleted when a virus or unwanted program is detected. The body of the text and any attachments of the email are replaced by a default text.

Delete attachment

If this option is enabled, the affected attachment is replaced by a default text. If the body of the email is affected, it is deleted and also replaced by a default text. The email itself is delivered.

Move attachment to quarantine

If this option is enabled, the affected attachment is moved to quarantine and then deleted (replaced by a default text). The body of the email is delivered. The affected attachment can later be delivered via the quarantine manager.

Ignore

If this option is enabled, an affected email is delivered despite detection of a virus or unwanted program.

Warning
This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases. Disable the preview in your mail client, never open any attachments with a double click!

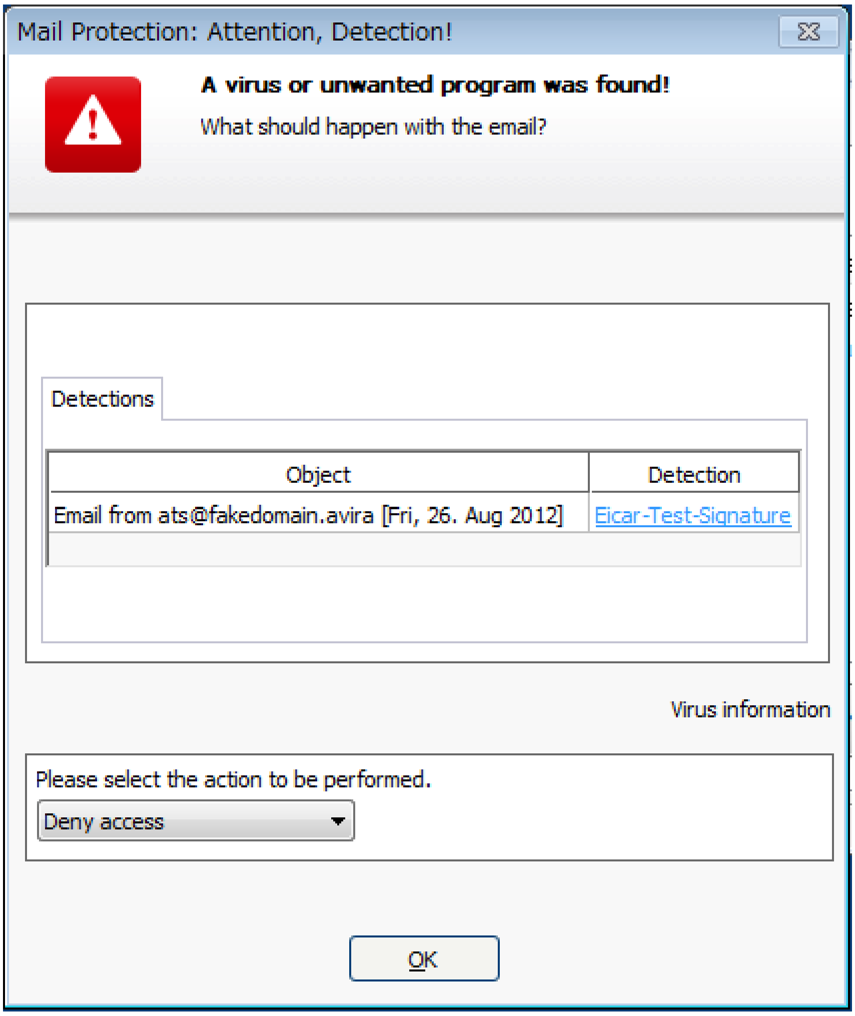
5.7.4 Buttons and links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

5.8 Outgoing emails

If the Mail Protection detects a virus, you will receive an alert if you selected *interactive* mode as the action mode when a virus is detected (see configuration section Mail Protection > Scan > Action on detection). In interactive mode you can choose what to do with the email or attachment in the dialog box.

5.8.1 Alert



Mail Protection: Attention, Detection!

A virus or unwanted program was found!

What should happen with the email?

Detections

Object	Detection
Email from ats@fakedomain.avira [Fri, 26. Aug 2012]	Eicar-Test-Signature

Virus information

Please select the action to be performed.

Deny access

5.8.2 Detections, Errors, Warnings

Messages and more detailed information about the emails in question will be displayed in the **Detections**, **Errors** and **Warnings** tabs:

- **Detections:** Object: Email in question, showing the name of the sender and the time the email was sent

  Detection: Name of the detected virus or unwanted program
- **Error:** Messages concerning errors that occurred during the Mail Protection scan
- **Alerts:** Alerts relating to the affected objects

5.8.3 Options

Move mail to quarantine (do not send)

If this option is enabled, the email, together with all attachments is copied to Quarantine and is not sent. The email remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

Block sending of mails (do not send)

The email is not sent and remains in the outbox of your email client. You receive an error message in your email program. All other emails sent from your email account will be scanned for malware.

Ignore

If this option is enabled, the infected email is sent despite detection of a virus or unwanted program.

> **Warning**
> Viruses and unwanted programs can penetrate the computer system of the email recipient in this way.

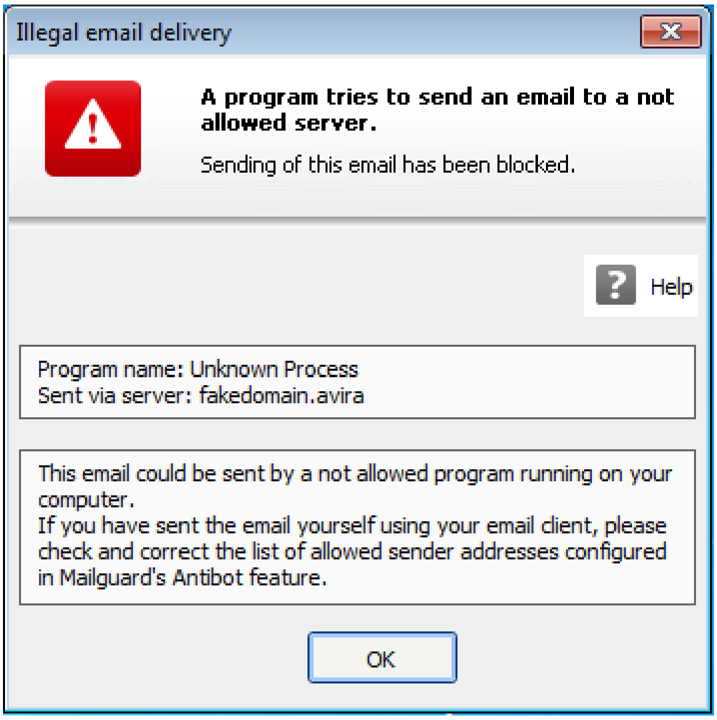
5.8.4 Buttons and links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

5.9 Sender

If you are using Mail Protection's AntiBot function, emails from unauthorized senders are blocked by Mail Protection. The sender is checked using the list of allowed senders that you created in the configuration under Mail Protection > Scan > AntiBot. The blocked email is displayed in a dialog box.

5.9.1 Alert



Illegal email delivery

A program tries to send an email to a not allowed server.

Sending of this email has been blocked.

Program name: Unknown Process
Sent via server: fakedomain.avira

This email could be sent by a not allowed program running on your computer.
If you have sent the email yourself using your email client, please check and correct the list of allowed sender addresses configured in Mailguard's Antibot feature.

5.9.2 Program used, SMTP server used and address of the sender of the email

The following information is displayed in the center window of the message:

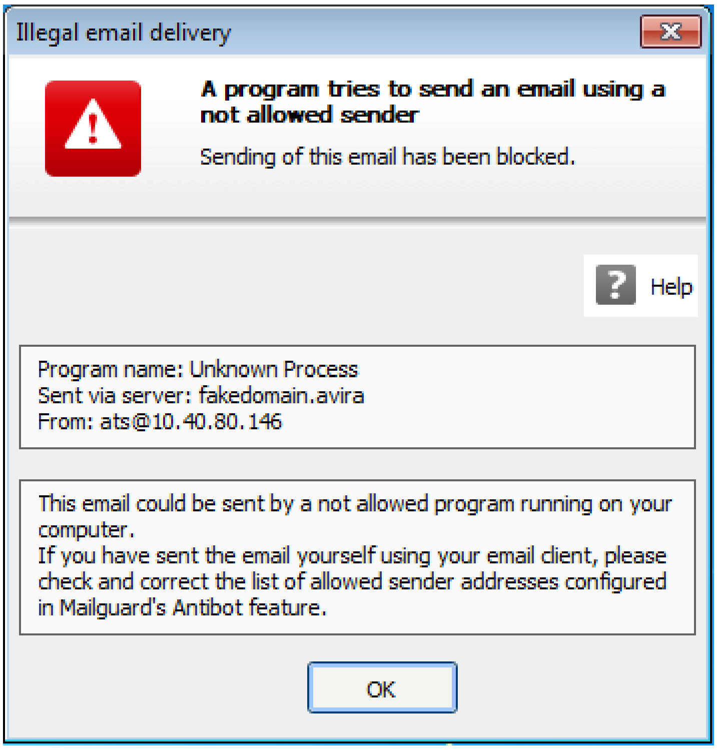
- Name of the program used to send the email
- Name of the SMTP server used to send the email
- Address of sender of email

If you sent the email in question using your email program, compare the list of permitted senders in the configuration under Mail Protection > Scan > AntiBot with the sender addresses that you use in the email accounts in your email client program. If the list of authorized senders in the configuration is incomplete, add the other sender addresses that you use to the list. You will find the blocked email in the outbox of your email client program. To send the blocked email, complete the configuration and then send the email again.

5.10 Server

If you are using Mail Protection's AntiBot function, emails sent by unauthorized SMTP servers are blocked by Mail Protection. Checking which SMTP server was used is performed using the list of permitted servers that you added to the configuration under Mail Protection > Scan > AntiBot. The blocked email is displayed in a dialog box.

5.10.1 Alert



Illegal email delivery

A program tries to send an email using a not allowed sender

Sending of this email has been blocked.

Program name: Unknown Process
Sent via server: fakedomain.avira
From: ats@10.40.80.146

This email could be sent by a not allowed program running on your computer.
If you have sent the email yourself using your email client, please check and correct the list of allowed sender addresses configured in Mailguard's Antibot feature.

5.10.2 Program used, SMTP server used

The following information is displayed in the center window of the message:

- Name of the program used to send the email
- Name of the SMTP server used to send the email

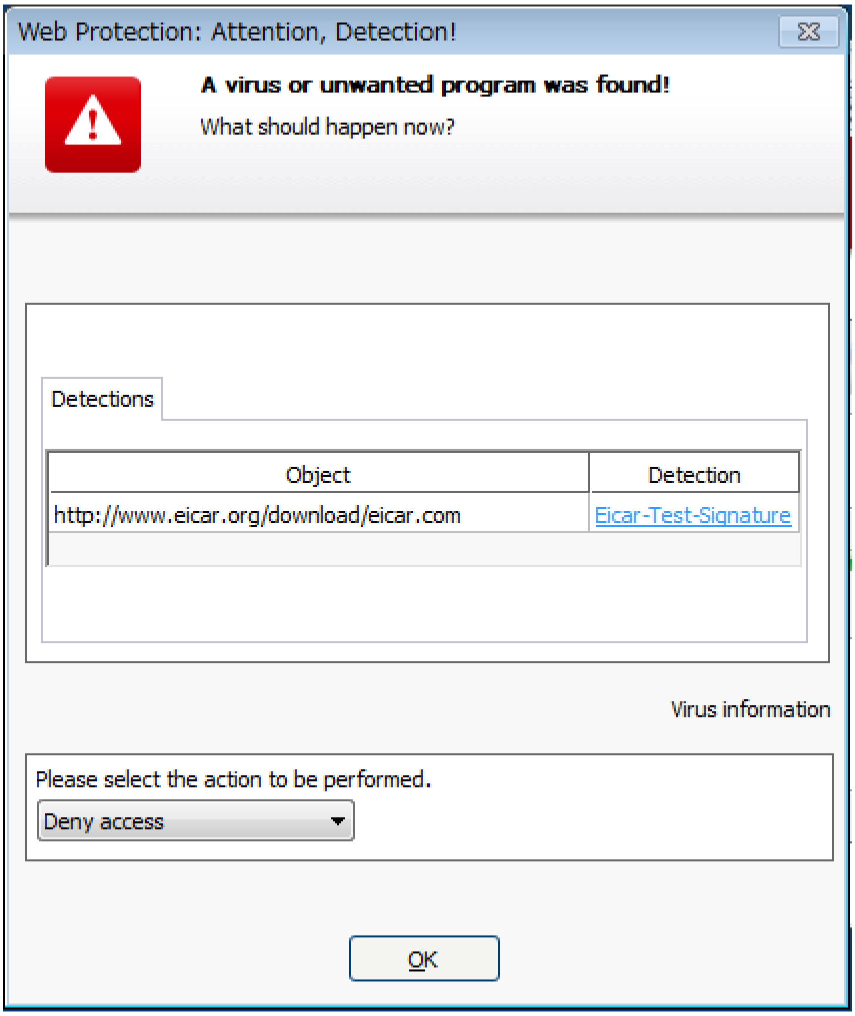
If you sent the email in question using your email program, compare the list of permitted servers in the configuration under Mail Protection > Scan > AntiBot with the SMTP servers you use to send emails. You can find the SMTP servers that are used in your email client program under the used email accounts. If the list of authorized servers in the configuration is incomplete, add the other SMTP servers that you use to the list. You will find the blocked email in the outbox of your email client program. To send the blocked email, complete the configuration and then send the email again.

5.11 Web Protection

If viruses are detected by Web Protection, you will receive an alert if you have selected *interactive* mode or *automatic* mode as the action mode for virus detection with the *Display detection alerts* option (see the configuration section Web Protection > Scan > Action on detection). In interactive mode you can choose what to do with the data sent by the web server in the dialog box. There is no selection option for handling the detected virus in automatic mode with alert. In the alert, you can either confirm the action that is to be performed automatically or cancel the Web Protection.

Note
The dialog shown below is a message about the detection of a virus in interactive mode.

Alert



Web Protection: Attention, Detection!

A virus or unwanted program was found!

What should happen now?

Detections

Object	Detection
http://www.eicar.org/download/eicar.com	Eicar-Test-Signature

Virus information

Please select the action to be performed.

Deny access

Detection, Errors, Warnings

Messages and detailed information relating to the viruses detected are displayed in the **Detection**, **Errors** and **Warnings** tabs:

- **Detection:** URL and the name of the detected virus or unwanted program
- **Error:** Messages about errors that occurred during the Web Protection scan
- **Alerts:** Warnings relating to the viruses that were detected

Possible actions

> **Note**
> If a detection is a heuristic hit (HEUR/), an unusual runtime packer (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), in interactive mode only the options Move to quarantine and Ignore are available. In automatic mode, the detection is automatically moved to Quarantine.
> This restriction prevents the detected files, which may be a false alarm, being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the quarantine manager.
> Depending on the configuration, various options may not be available.

Deny access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. Web Protection logs the detection to the report file if the report function is activated.

Move to quarantine

In the event of a virus or malware being detected, the website requested from the web server and/or the transferred data and files are moved into quarantine. The affected file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center.

Ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by Web Protection to your web browser.

> **Warning**
> This could allow viruses and unwanted programs to access your computer system. Only select the **Ignore** option in exceptional cases.

Buttons and links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

6. System Scanner

6.1 System Scanner

With the System Scanner component, you can carry out targeted scans (on-demand scans) for viruses and unwanted programs. The following options are available for scanning for infected files:

- **System scan via context menu**
  The system scan via the context menu (right-hand mouse button - entry **Scan selected files with Avira**) is recommended if, for example, you wish to scan individual files and directories. Another advantage is that it is not necessary to first start the Control Center for a system scan via the context menu.
- **System scan via drag & drop**
  When a file or directory is dragged into the program window of the Control Center, the System Scanner scans the file or directory and all sub-directories it contains. This procedure is recommended if you wish to scan individual files and directories that you have saved, for example, on your desktop.
- **System scan via profiles**
  This procedure is recommended if you wish to regularly scan certain directories and drives (e.g. your work directory or drives on which you regularly store new files). You do not then need to select these directories and drives again for every new scan, you simply select using the relevant profile.
- **System scan via the Scheduler**
  The Scheduler enables you to carry out time-controlled scans.

Special processes are required when scanning for rootkits, boot sector viruses, and when scanning active processes. The following options are available:

- Scan for rootkits via the scan profile **Scan for Rootkits and active malware**
- Scan active processes via the scan profile **Active processes**
- Scan for boot sector viruses via the menu command **Boot records scan...** in the menu **Extras**

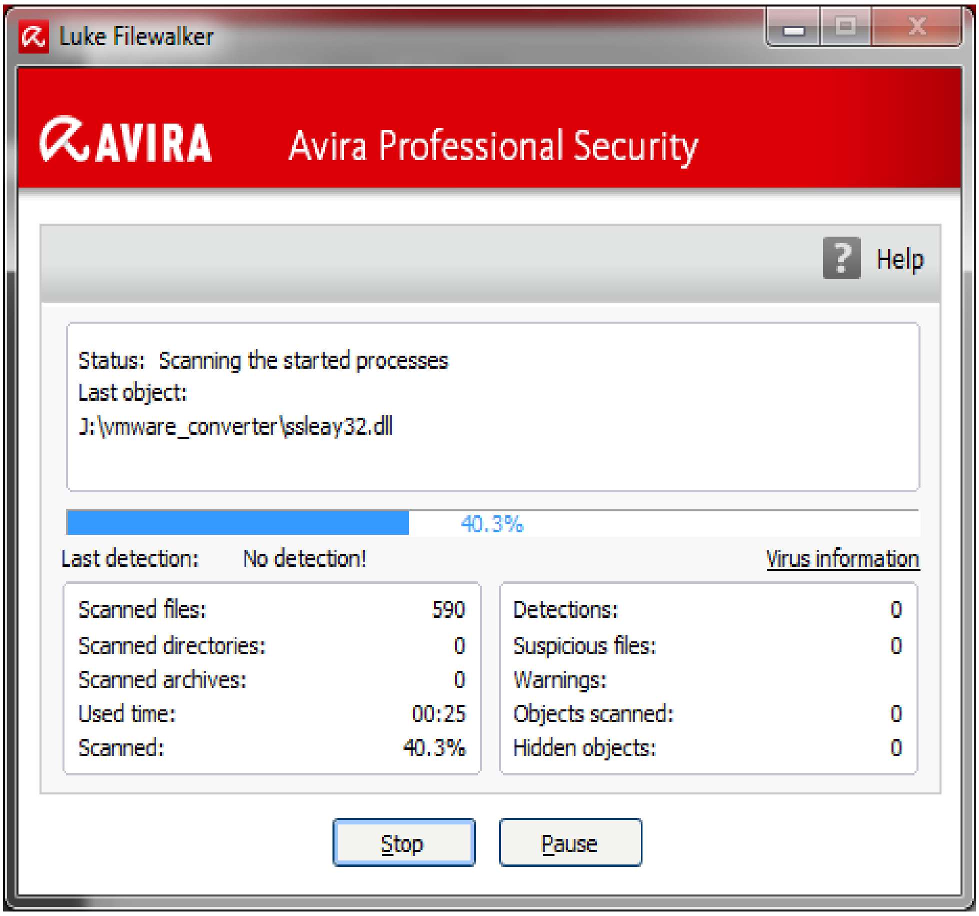
6.2 Luke Filewalker

During a system scan, the status window **Luke Filewalker** appears, which provides you with exact information on the status of the scan.

If the option **interactive** is selected in the configuration of the System Scanner in the group **Action on detection**, you are asked what is to be done with a detected virus or unwanted program. If the option **automatic** is selected, any detections are shown in the Scanner report.

When the scan is complete, its results (statistics), alerts and error messages are displayed in a new dialog box.

6.2.1 Luke Filewalker: Scan status window



Status: Scanning the started processes
Last object:
J:\vmware_converter\ssleay32.dll

40.3%

Last detection: No detection!

Scanned files:	590	Detections:	0
Scanned directories:	0	Suspicious files:	0
Scanned archives:	0	Warnings:	
Used time:	00:25	Objects scanned:	0
Scanned:	40.3%	Hidden objects:	0

Displayed information

Status: There are different status messages:

- *The program will be initialized*
- *Hidden objects search is running!*
- *Scanning the started processes*
- *Scanning file*
- *Initialize archive*
- *Free memory*
- *File is being unpacked*
- *Scanning boot sectors*
- *Scanning master boot sectors*
- *Scanning the registry*

- *The program will be ended!*
- *The scan has finished*

Last object: Name and path of the file that is currently being scanned or that was most recently scanned

Last detection: There are various messages for the last detection:

- *No detection!*
- Name of the most recently detected virus or unwanted program

Scanned files: Number of scanned files

Scanned directories: Number of scanned directories

Scanned archives: Number of scanned archives

Used time: Duration of the system scan

Scanned: Percentage of scan already completed

Detections: Number of viruses and unwanted programs detected

Suspicious files: Number of files reported by the heuristics

Warnings: Number of alerts about detected viruses

Objects scanned: Number of objects scanned during the rootkits scan

Hidden objects: Total number of hidden objects detected

Note

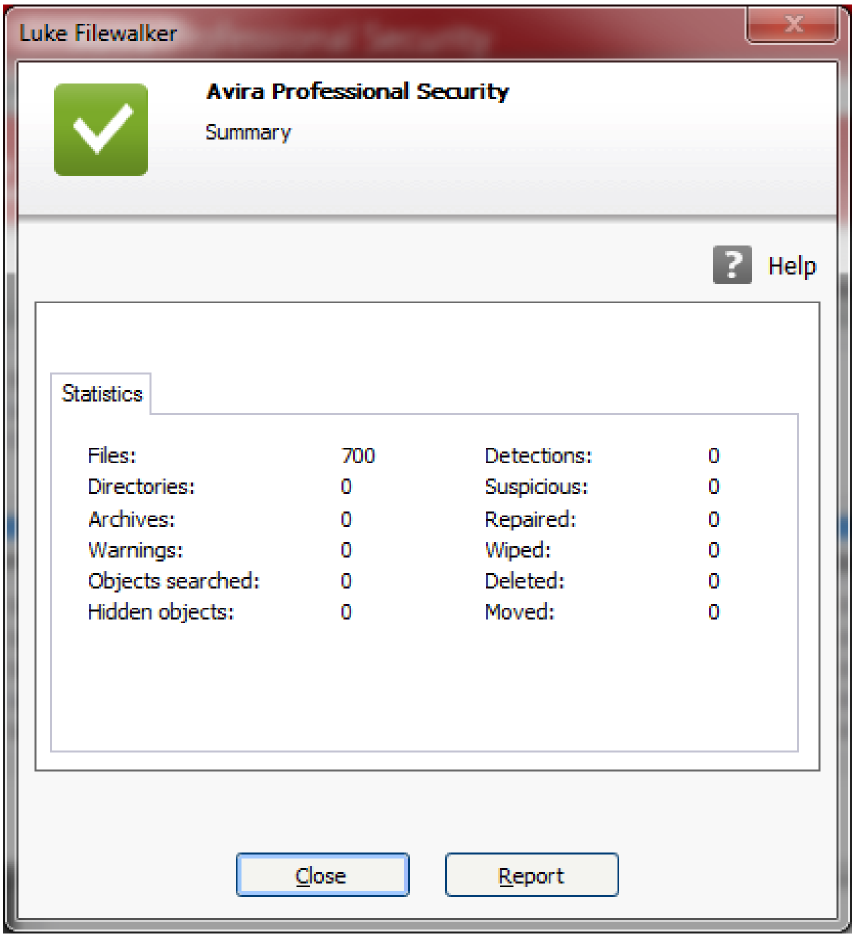
Rootkits have the ability to hide processes and objects, such as registry entries or files. However not every hidden object is necessarily proof of the existence of a rootkit. Hidden objects can also be harmless objects. If a scan detects hidden objects but does not issue a virus detection alert, you should use the report to determine which object is referred to and obtain more information about the detected object.

Buttons and links

Button / Link	Description
	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
	This page of the online help is opened via this button or link.
Stop	The scan process is stopped.
Pause	The scan will be interrupted and can be continued by clicking on the button **Resume**.
Resume	The interrupted scan will be continued.
End	The System Scanner is closed.

Report	The report file of the scan will be shown.

6.2.2 Luke Filewalker: Scan Statistics



Files:	700	Detections:	0
Directories:	0	Suspicious:	0
Archives:	0	Repaired:	0
Warnings:	0	Wiped:	0
Objects searched:	0	Deleted:	0
Hidden objects:	0	Moved:	0

Displayed information: Statistics

Files: Number of scanned files

Directories: Number of scanned directories

Archives: Number of scanned archives

Warnings: Number of alerts about detected viruses

Objects searched: Number of objects scanned during the rootkits scan

Hidden objects: Number of detected hidden objects (rootkits)

Detections: Number of viruses and unwanted programs detected

Suspicious: Number of files reported by the heuristics

Repaired: Number of repaired files

Wiped: Number of overwritten files

Deleted: Number of deleted files

Moved: Number of files that are moved to quarantine

Buttons and links

Button / Link	Description
	This page of the online help is opened via this button or link.
Close	The summary window is closed.
Report	The report file of the scan will be shown.

7. Control Center

7.1 Control Center Overview

The Control Center is an information, configuration and management center. In addition to the sections that can be selected individually, it offers a large number of options that can be accessed from the menu bar.

Menu bar

All functions of the Control Center are contained in the menu bar.

File

- Exit (Alt + F4)

View

- Status
- PC Protection
  - System Scanner
  - Real-Time Protection
- Internet Protection
  - FireWall
  - Web Protection
  - Mail Protection
- Administration
  - Quarantine
  - Scheduler
  - Reports
  - Events
- Refresh (F5)

Extras

- Boot records scan...
- Detection list...
- Download rescue CD
- Configuration (F8)

Update

- Start update...
- Manual update...

Help

- Topics
- Help me
- Download manual
- Load license file...
- Send feedback
- About Avira Professional Security

> **Note**
> You can activate the keyboard navigation in the menu bar with the help of the [ALT] key. If navigation is activated, you can move within the menu with the arrow keys. With the Return key you activate the active menu item.

Navigation sections

In the left-hand navigation bar you find the following sections:

- **Status**

PC PROTECTION

- System Scanner
- Real-Time Protection

INTERNET PROTECTION

- FireWall
- Web Protection
- Mail Protection

ADMINISTRATION

- Quarantine
- Scheduler
- Reports
- Events

Navigation description

- **Status**: Clicking on the **Status** bar gives you an overview of the product's functionality and performance (see Status).
    - The **Status** section lets you see at a glance which modules are active and provides information on the last update performed.
- *PC PROTECTION*: In this section you will find the components for checking the files on your computer system for viruses and malware.
    - The System Scanner section enables you to easily configure and start an on-demand scan. Predefined profiles enable a scan with already adapted default options. In the same way it is possible to adapt the scan for viruses and unwanted programs to your personal requirements with the help of manual selection (will be saved) or by creating user-defined profiles.
    - The Real-Time Protection section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
- *INTERNET PROTECTION*: In this section you will find the components to protect your computer system against viruses and malware from the Internet, and against unauthorized network access.
    - The FireWall section enables you to configure the basic settings for the FireWall. In addition, the current data transfer rate and all active applications using a network connection are displayed.
    - The Web Protection section displays information on scanned URLs and detected viruses, as well as other statistical data, which can be reset at any time and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
    - The Mail Protection section shows you all the emails scanned by Mail Protection, their properties and other statistical data. You can also exclude email addresses from future scanning for malware. Emails can also be deleted from the Mail Protection buffer.
- *ADMINISTRATION*: In this section you will find tools for isolating and managing suspicious or infected files, and for planning recurring tasks.
    - The Quarantine section contains the so-called quarantine manager. This is the central point for files already placed in quarantine or for suspect files that you would like to place in quarantine. It is also possible to send a selected file to the Avira Malware Research Center by email.
    - The Scheduler section enables you to configure scheduled scanning and update jobsand to adapt or delete existing jobs.
    - The Reports section enables you to view the results of actions performed.
    - The Events section enables you to view events generated by certain program modules.

Buttons and links

The following buttons and links may be available.

Button / link	Shortcut	Description
	F8	This button or link is used to access the corresponding configuration dialog for the section.
	F1	This button or link opens the corresponding online help topic for the section.

7.2 File

7.2.1 Exit

The menu item **Exit** in the **File** menu, closes the Control Center.

7.3 View

7.3.1 Status

The start screen of the Control Center, the **Status** section, enables you to see at a glance whether your computer system is protected and which Avira modules are active. The **Status** window also provides information about the last update performed. You can also see whether you own a valid license.

- PC Protection: Real-Time Protection, Last scan, Last update, Your Product is activated
- Internet Protection: Web Protection, Mail Protection, FireWall, Presentation Mode,

> **Note**
> The User Account Control (UAC) will ask for your permission to enable or disable the Real-Time Protection, FireWall, Web Protection and Mail Protection services in operating systems as of Windows Vista.

PC Protection

Information on the current status of the service and protective functions, locally protecting your computer against viruses and malware, is displayed in this section.

Real-Time Protection

Information on the current status of the Real-Time Protection is displayed in this field.

You may enable or disable the Real-Time Protection by clicking the **ON/OFF** button. Further options for the Real-Time Protection can be accessed by clicking **Real-Time Protection** in the navigation bar. At first you get information on the status of last found malware and infected files. Click **Configuration** to define further settings.

- **Configuration**: Go to the Configuration to define the settings for the Real-Time Protection components.

The following possibilities are available:

Icon	Status	Option	Description
✓	*Activated*	**Deactivate**	The Real-Time Protection service is active, i.e. your system is continually monitored for viruses and unwanted programs. **Note** You can disable the Real-Time Protection service. However, please note that if Real-Time Protection is disabled you are no longer protected from viruses and unwanted programs. All files can pass through the system unnoticed and possibly cause damage.
!	*Deactivated*	**Activate**	The Real-Time Protection service is disabled, i.e. the service is loaded but is not active. **Warning** No scan is performed for viruses and unwanted programs. All files can pass through the system unnoticed. You are not protected against viruses and unwanted programs. **Note** In order to be protected against viruses and unwanted programs again, please click the **ON/OFF** button next to **Real-Time Protection** in the *PC Protection* area.

☒	*Service stopped*	**Start service**	The Real-Time Protection service is stopped. **Warning** No scan is performed for viruses and unwanted programs. All files can pass through the system unnoticed. You are not protected against viruses and unwanted programs. **Note** In order to be protected against viruses and unwanted programs again, please click the **ON/OFF** button next to **Real-Time Protection** in the *PC Protection* area. The current status should be displayed in green color, meaning **Activated**.
	Unknown	**Help**	This status is displayed when an unknown error occurs. In this case, please get in touch with our Support.

Last scan

Information on the last system scan performed is displayed in this field. When a complete system check is performed, all the hard disks on your computer are thoroughly scanned. All scanning processes, with the exception of the integrity checking of system files, are employed: standard file scanning, checking the registry and boot sectors, scanning for rootkits, etc.

The following details are displayed:

- Date of last complete system scan

The following possibilities are available:

System scan	Option	Description
Not performed	**Scan system**	No complete system check has been executed since installation. **Warning** The status of the system is unchecked. There is the possibility that viruses or unwanted programs are to be found on your computer. **Note** To check your computer, please click on the **Scan system** link.
Date of last system scan, e.g. *09/18/2011*	**Scan system**	You performed a complete system scan on the specified date. **Note** We recommend that you use the default scan job *Complete system scan*. Use the Scheduler to enable the **Complete system scan** job.
Unknown	**Help**	This status is displayed when an unknown error occurs. In this case, please get in touch with our Support.

Last update

Information on the current status of the last update performed is displayed here.

The following details are displayed:

- Date of the last update

▸ Click the button **Open Configuration** to define further settings for automatic updates.

The following possibilities are available:

Icon	Status	Option	Description
✓	*Date of last update, e.g. 07/18/2011*	**Start update**	The program has been updated during the last 24 hours. **Note** You can update your Avira product to the latest version via the **Start update** button.
!	*Date of last update, e.g. 07/18/2011*	**Start update**	24 hours have already passed since the update but you are still within the update reminder cycle you chose. This depends on the setting in the configuration. **Note** You can update your Avira product to the latest version via the **Start update** button.
✕	*Not performed*	**Start update**	Since installation no update has been performed -or- The update reminder cycle you chose has been exceeded (see Configuration) and no update has been performed -or- The virus definition file is older than the update reminder cycle you have selected (see Configuration). **Note** You can update your Avira product to the latest version via the **Start update** button.
		Not available	If the license has expired, no updates can be performed.

Your Product is activated

Information on the current status of your license is displayed in this field.

The following possibilities are available:

Full version

Icon	Status	Option	Meaning
✓	*Validity date of the current license for a full version, e.g. 10/31/2011*	**Renew**	You have a valid license for your Avira product. You can access the Avira online shop via the **Renew** button. There you have the opportunity to adapt your current license to your needs and to upgrade to Avira Premium.
!	*Validity date of the current license for a full version, e.g. 10/31/2011*	**Renew**	You have a valid license for your Avira product. The licensing period, however, is thirty or fewer days. Use the **Renew** button to access the Avira online shop. There you have the option to extend the current license.
✕	*License expired on: e.g. 08/31/2011*	**Buy**	Your license for your Avira product has expired. Use the **Buy** button to access the Avira online shop. There you have the option of purchasing a valid license. **Warning** If your license has expired, updates are no longer possible. The program's protective functions are deactivated and can no longer be activated.

Evaluation license

Icon	Status	Option	Meaning
✓	*Validity date of the evaluation license, e.g. 10/31/2011*	**Buy**	You have an evaluation license that allows you to test the full range of functions of your Avira product for a certain period of time. Use the **Buy** button to access the Avira online shop. There you have the option of purchasing a valid license.
!	*Validity date of the evaluation license, e.g. 10/31/2011*	**Renew**	You have an evaluation license. The licensing period, however, is thirty or fewer days. Use the **Renew** button to access the Avira online shop. There you have the option of purchasing a valid license.
✕	*Evaluation license expired on: 10/31/2011*	**Buy**	Your license for your Avira product has expired. Use the **Buy** button to access the Avira online shop. There you have the option of purchasing a valid license. Warning If your license has expired, updates are no longer possible. The program's protective functions are deactivated and can no longer be activated.

Internet Protection

Information on the current status of the service protecting your computer against viruses and malware from the Internet, is displayed in this section.

- **FireWall**: The service monitors the communication channels to and from your computer.
- **Web Protection**: The service checks the data that is transmitted and loaded into your web browser while you are surfing the Internet (monitoring of ports 80, 8080, 3128).
- **Mail Protection**: The service checks emails and their attachments for viruses and malware.
- **Presentation Mode**: If set to automatic, your Avira product switches automatically to the Presentation Mode for every application that runs in full screen.

Other options for these processes can be accessed from a context menu by clicking the configuration icon next to the **ON/OFF** button.

- **Configure**: Go to the Configuration to define settings for the process component.

The following possibilities are available: *Services*

Icon	Status	Process status	Option	Meaning
✓	*OK*	*Activated*	**Deactivate**	All services for Internet Protection are active. Note You can deactivate a service by clicking the **ON/OFF** button. Note, however, that you are no longer fully protected against viruses and malware once a service has been deactivated.
!	*Restricted*	*Deactivated*	**Activate**	A service is deactivated, i.e. the service has been started but is not active. Warning Your computer system is not being fully monitored. There is a possibility that viruses and unwanted programs can access your computer system. Note To activate the service, click the **ON/OFF** button.

✖	*Warning*	*Service stopped*	**Start service**	A service has been stopped **Warning** Your computer system is not being fully monitored. There is a possibility that viruses and unwanted programs can access your computer system. **Note** Click the **ON/OFF** button to start the service so that your computer system is monitored. The service is started and activated.
		Unknown	**Help**	This status is displayed when an unknown error occurs. In this case, please get in touch with our Support.

7.3.2 Presentation Mode

If an application is executed in full-screen mode on your computer system, you may intentionally suspend desktop notifications as pop-up windows and in-product messages by activating the Presentation Mode. All defined adapter and application rules that you have configured in Avira FireWall, apply, but no popup windows appear with network event notification.

You may enable the Presentation Mode or keep it in automatic mode by clicking the **ON/OFF** button. By default the Presentation Mode is set to **automatic** and displayed in green color. The default setting sets the feature to automatic, so that whenever you run an application that needs the full-screen mode, your Avira product switches automatically to Presentation Mode.

- Click the button on the left next to the **OFF** button to activate the Presentation Mode.
  - ↳ The Presentation Mode is enabled and displayed in yellow color.

Note
We recommend to change the default setting **OFF** with its automatic full-screen recognition mode only temporarily, because you won't receive visible desktop notifications and warnings concerning network events and possible threats.

7.3.3 System Scanner

The **System Scanner** section enables you to easily configure and start a system scan. Predefined profiles enable a system scan with already adapted default options. In the same way it is possible to adapt the system scan for viruses and unwanted programs to your personal requirements with the help of manual selection or by creating user-defined profiles. The required action can be selected either via the icon in the toolbar, via shortcut or via the context menu. Start a system scan via the item Start scan with selected profile.

The display and handling of the editable profiles corresponds to that of the Windows Explorer. Every folder in the main directory corresponds to one profile. Folders or files to be scanned are selected or can be selected with a check mark in front of the folder or file to be scanned.

- To change directories, double-click the required directory.
- To change drives, double-click the required letter of the drive.
- To select folders and drives, you can click on the box in front of the folder or drive icon or select via the context menu.
- You can navigate through the menu structure with the aid of the scroll bar and the scroll arrows.

Predefined profiles

Predefined scan profiles are available if required.

Note
These profiles are read-only and cannot be altered or deleted. To adapt a profile to your requirements, select for a one-off scan the folder Manual selection or Create new profile to create a user-defined profile, which can be saved.

Note
The scanning options for the predefined profiles can be set in Configuration > System Scanner > Scan > Files. You can adapt these settings to your requirements.

Local Drives

All local drives on your system are scanned for viruses or unwanted programs.

Local Hard Disks

All local hard disks on your system are scanned for viruses or unwanted programs.

Removable Drives

All available removable drives of your system are scanned for viruses or unwanted programs.

Windows System Directory

The Windows system directory of your system is scanned for viruses or unwanted programs.

Complete system scan

All local hard disks on your computer are scanned for viruses or unwanted programs. During the scan, all scanning processes, with the exception of the integrity checking of system files, are employed: Standard scan of files, scanning of registry and boot sectors, scanning for rootkits, etc. (see System Scanner > Overview). The scanning processes are performed regardless of the scanner setting in the configuration under System Scanner > Scan: Other settings.

Quick system scan

The most important folders of your system (directories *Windows*, *Programs*, *Documents and Settings\Local User*, *Documents and Settings\All Users*) are scanned for viruses and unwanted programs.

My Documents

The default "*My Documents*" location of the logged-in user is scanned for viruses and unwanted programs.

> **Note**
> Under Windows, "*My Documents*" is a directory in the profile of the user that is used as the default location for documents that have been saved. The default setting for the directory is *C:\Documents and Settings\[user name]\My Documents*.

Active Processes

All current processes are scanned for viruses or unwanted programs.

Scan for Rootkits and active malware

The computer is scanned for rootkits and active (running) malware programs. All running processes are checked.

Note
In interactive mode you have several ways of reacting to a detection. In automatic mode the detection is recorded in the report file.

Note
The rootkits scan is not available for Windows XP 64 bit !

7.3.4 Manual selection

Select this folder if you want to adapt the scan to your individual requirements. Mark the required directories and files to be scanned. If your Avira product is managed by the Avira Management Console, you can use the **Manual Selection** field in the **Commands** dialog to scan multiple directories, separated by '?' (for example: `c:\temp?d:\test`).

Note
The profile **Manual selection** is used to scan data without first creating a new profile.

User-defined profiles

A new profile can be created via the toolbar, via shortcut or via the context menu.

New profiles can be saved under the name you require and in addition to the manually controlled scan are useful for creating scheduled scans with the aid of the Scheduler.

Toolbar and Shortcuts

Icon	Shortcut	Description
🔍	**F3**	**Start scan with the selected profile** The selected profile is scanned for viruses or unwanted programs.
🔍	**F6**	**Start scan with selected icon as administrator** The selected profile is scanned with administrative rights

+	**Ins**	**Create new profile** A new profile is created.
▭	**F2**	**Rename selected profile** A new name for the selected profile is saved.
↗	**F4**	**Create desktop link for the selected profile** A link to the selected profile is created on the desktop.
×	**Del**	**Delete selected profile** The selected profile is irretrievably deleted.

Context menu

The context menu for this section can be obtained by selecting a required profile with the mouse and keeping the right-hand mouse button pressed.

Start scan

The selected profile is scanned for viruses or unwanted programs.

Start scan (admin)

(This function is only available as of Windows Vista. Administrator rights are required to carry out this action.)

The selected profile is scanned for viruses or unwanted programs.

Create new profile

A new profile is created. Select the directories and files to be scanned.

Rename profile

Gives the selected profile the name chosen by you.

> **Note**
> This entry cannot be selected in the context menu if a predefined profile is selected.

Delete profile

The selected profile is irretrievably deleted.

Note
This entry cannot be selected in the context menu if a predefined profile is selected.

File filter

Default:

Means that the files are scanned according to the setting in the Files group of the Configuration. You can adapt this setting to your requirements in the Configuration. You can access Configuration via the Configuration button or link.

Scan all files:

All files are scanned irrespective of the setting in the configuration.

User-defined:

A dialog box is opened in which all file extensions are displayed that are scanned. Default entries are defined for the extensions. However, entries can be added or deleted.

Note
This entry can only be selected in the context menu when the mouse is over a check box.
The option is not available with predefined profiles.

Select

With sub-directories:

Everything is scanned in the selected node (black check mark).

Without sub-directories:

Only the files are scanned in the selected node (green check mark).

Only sub-directories:

Only the sub-directories are scanned in the selected node, not the files that are in the node (gray check mark, sub-directories have a black check mark).

No selection:

Selection is canceled, the currently selected node is not scanned (no check mark).

Note
This entry can only be selected in the context menu when the mouse is over a check box.
The option is not available with predefined profiles.

Create desktop link

Creates a link to the selected profile on the desktop.

> **Note**
> This entry cannot be selected in the context menu if the profile Manual selection is selected, as the settings of the Manual selection are not permanently saved.

7.3.5 Real-Time Protection

The **Real-Time Protection** section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".

> **Note**
> If the Real-Time Protection service is not started, the button next to the module is displayed in yellow color. However, the report file of the Real-Time Protection can be displayed.

Toolbar

Icon	Description
📋	**Display report file** The report file of the Real-Time Protection is displayed.
📊	**Reset statistics data** The statistical information in this section is set to zero.

Displayed information

Last file found

Shows the name and location of the file last found by the Real-Time Protection.

Last virus or unwanted program found

Gives the name of the last virus or unwanted program found.

Icon/link	Description
Virus information	Click the icon or link to display detailed information about the virus or unwanted program if an Internet connection is present.

Last file scanned

Shows the name and path of the file last scanned by the Real-Time Protection.

Statistics

Number of files

Shows the number of files scanned so far.

Number of detections

Shows the number of viruses and unwanted programs found so far.

Number of suspicious files

Displays the number of files reported by the heuristics.

Number of deleted files

Shows the number of files deleted so far.

Number of repaired files

Shows the number of files repaired so far.

Number of moved files

Shows the number of files moved so far.

Number of renamed files

Shows the number of files renamed so far.

7.3.6 FireWall

Avira FireWall (only for Avira Professional Security)

The current data transfer rate is displayed in the FireWall section. The FireWall section enables you to configure the basic settings for the Avira FireWall: You can set the required **Security level** via a slider. To configure a user-defined security level, you must switch to **Configuration**.

Toolbar

Icon	Description
📊	**Reset statistics** The statistical information in this section is set to zero.

Security level

You can select one of the following security levels:

> **Note**
> You can change the security level by simply dragging the slider along the security scale. The selected security level is applied immediately after selection. For more detailed information please refer to the configuration of the FireWall: Configuration > FireWall > Avira FireWall > Adapter rules.

Low

Flooding and port scan are detected.

Medium

Suspicious TCP and UDP packages are discarded.

Flooding and port scan are prevented.

(Set as default level.)

High

Computer is not visible on the network.

New connections from outside are not allowed.

Flooding and port scan are prevented.

Custom

User-defined rules.

Block all

All existing network connections will be closed.

Transfer

Information on the current and total amount of data sent (*Upload*) and received (*Download*) is displayed in this box. You can see the maximum value displayed in the top left corner of the graphic.

The red color represents the incoming packets, the green color the outgoing packets. The area where the two states overlap is colored in gray.

Windows Firewall (as of Windows 7)

Avira manages the Windows Firewall from the Control and Configuration Center.

The FireWall section enables you to check the status of the Windows Firewall and restore the recommended settings by clicking the **Fix problem** button.

7.3.7 Web Protection

The **Web Protection** section shows information on scanned URLs, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".

Toolbar

Icon	Description
📋	**Show report file** The report file of the Web Protection is displayed.
📊	**Reset statistics data** The statistical information in this section is set to zero.

Displayed information

Last reported URL

Displays the last URL detected by Web Protection.

Last detected virus or unwanted program

Gives the name of the last virus or unwanted program found.

Icon/link	Description
Virus information	Click the icon or link to display detailed information about the virus or unwanted program if an Internet connection is present.

Last scanned URL

Shows the name and path of the last URL checked by Web Protection.

Statistics

Number of URLs

Shows the number of URLs checked to that point.

Number of detections

Shows the number of viruses and unwanted programs found so far.

Number of blocked URLs

Shows the number of previously blocked URLs.

Number of ignored URLs

Shows the number of previously ignored URLs.

7.3.8 Mail Protection

The **Mail Protection** section shows you all the emails scanned by Mail Protection, their properties and other statistical data.

> **Note**
> If the Mail Protection service is not started, button next to the module is displayed in yellow color. However, the report file of the Mail Protection can be displayed. If the module is not available in your Avira product,the boxes of this section are grayed out and cannot be selected.
>
> **Note**
> Exemption of individual email addresses from the malware scan obviously only

applies to incoming emails. To disable the scanning of outgoing emails, deactivate the scan in the configuration under Mail Protection > Scan.

Toolbar

Icon	Description
📋	**Display report file** The report file of the Mail Protection is displayed.
i	**Display properties of the selected email** Opens a dialog box with more information on the selected email.
🔍	**Do not scan email address for malware** The selected email address will no longer be scanned for viruses and unwanted programs in future. You can undo this setting again in the configuration under Mail Protection > General > Exceptions.
×	**Delete selected email(s)** The selected email is deleted from the cache. However, the email remains in your email program.
📊	**Reset statistics data** The statistical information in this section is set to zero.

Scanned emails

This area shows the emails scanned by Mail Protection.

Icon	Description
✓	No virus or unwanted program was found.
⚠	A virus or unwanted program was found.

Type

Shows the protocol used to send or receive the email:

- POP3: email received via POP3
- IMAP: email received via IMAP
- SMTP: email sent via SMTP

From/To

Shows the email sender’s address.

Subject

Shows the subject of the email received.

Date/Time

Shows when the email was scanned.

> **Note**
> You can obtain further information on an email by double-clicking the relevant email.

Statistics

Email action

Shows the action performed when Mail Protection finds a virus or an unwanted program in an email. In interactive mode no display is available here, as you can select yourself which procedure is to be followed in the event of detection.

> **Note**
> You can adapt this setting to your requirements in the Configuration. You can access Configuration via the **Configuration** button or link.

Affected attachments

Shows the action performed when Mail Protection finds a virus or an unwanted program in an affected attachment. In interactive mode no display is available here, as you can select yourself which procedure is to be followed in the event of detection.

> **Note**
> You can adapt this setting to your requirements in the Configuration. You can access Configuration via the **Configuration** button or link.

Number of emails

Shows the number of emails scanned by Mail Protection.

Last detection

Gives the name of the last virus or unwanted program found.

Number of detections

Shows the number of viruses and unwanted programs previously detected and reported.

Suspicious emails

Shows the number of emails reported by the heuristics.

Number of incoming emails

Shows the number of emails received.

Number of outgoing emails

Shows the number of emails sent.

7.3.9 Quarantine

The **Quarantine manager** manages affected objects (files and emails). Your Avira product can move affected objects to the quarantine directory in a special format. They can neither be executed nor opened.

> **Note**
> To move objects to the Quarantine manager, select the relevant option for quarantine in the **Configuration** under **System Scanner** and **Real-Time Protection** and **Mail Protection** - **Scan > Action on detection** if you are working in **automatic mode**.
> Alternatively you can select the relevant quarantine option in **interactive mode**.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
🔍	**F2**	**Rescan object(s)** A selected object is scanned again for viruses and unwanted programs. The settings of the on-demand scan are used for this.
i	**Return**	**Properties** Opens a dialog box with more detailed information on the selected object. Note You may obtain detailed information also by double-clicking an object.

↻ ↻ (Windows Vista)	**F3**	**Restore object(s)** A selected object is restored. Hereafter the object is placed in its original location. **Note** This option is not available for objects of the type email. **Warning** Enormous damage in the system due to viruses and unwanted programs! If you restore files: ensure that only files that were able to be cleaned by another scan are restored. **Note** As of Windows Vista, you must have administrator rights to restore objects.
↻	**F6**	**Restore object(s) to...** A selected object can be restored at a location defined by you. If you select this option, the "Save as" dialog opens in which you can select the storage location. **Warning** Enormous damage in the system due to viruses and unwanted programs! If you restore files: ensure that only files that were able to be cleaned by another scan are restored.

+	**Ins**	**Add file to quarantine** If you regard a file as suspicious, you can add it to the quarantine manager manually with this option. If appropriate upload the file to an Avira Malware Research Center web server for investigation using the Send object option.
✉	**F4**	**Send object(s)** The object is uploaded to an Avira Malware Research Center web server for investigation by the Avira Malware Research Center. When you click on the **Send Object** button, a dialog opens containing a form for entering your contact data. Enter all the required data. Select a type: **Suspicious file** or **False positive**. Click **OK** to upload the suspicious file. Note The size of the files you upload is limited to 20 MB uncompressed or 8 MB compressed. Note You can upload several files at once by selecting all the files you want to upload and then clicking the **Send Object** button.
×	**Del**	**Delete object(s)** A selected object is deleted from the quarantine manager. The object cannot be restored.
⧉		**Copy object(s) to** The highlighted quarantined object is saved to the selected directory. Note The quarantined object is not identical to the restored file. The quarantined object is encrypted and cannot be executed or read in its original format.

⬋	**F7**	**Export all properties** The properties of the highlighted quarantined object are exported in a text file.
📁	**F10**	**Open quarantine directory** Opens the directory INFECTED.

> **Note**
> You have the option of executing actions on multiple highlighted objects.
> To highlight multiple objects (objects in columns), hold down the control key or the shift key while selecting the objects in quarantine manager. Press **Ctrl + A** to select all the displayed objects.
> When executing the action **Display properties** multiple objects cannot be selected.

Table

Status

An object placed in quarantine can have different statuses:

Icon	Description
✅	No virus or unwanted program was found, the object is "clean".
⚠	A virus or unwanted program was found.
!	If a suspect file was added to the quarantine manager with the option Add file, it has this warning icon.

Type

Designation	Description
Email	The object detected is an email.
File	The object detected is a file.

Detection

Shows the name of the malware found.
Heuristic findings are identified with the abbreviation HEUR/.

Source

Shows the path under which the object was found.

Date/Time

Shows the date and time of the detection.

Detailed information

File name

Full path and file name of the object.

Quarantined object

File name of the quarantined object.

Restored

YES/ NO

YES: The selected object has been restored.

NO: The selected object has not been restored.

Uploaded to Avira

YES/ NO

YES: The object has already been uploaded to an Avira Malware Research Center web

server for investigation by the Avira Malware Research Center.

NO: The object has not yet been uploaded to an Avira Malware Research Center web

server for investigation by the Avira Malware Research Center.

Operating system

Windows XP: The malware has been identified by an Avira desktop product.

Scan engine

Version number of scan engine

Virus definition file

Version number of the virus definition file

Detection

Name of the malware detected.

Date/Time

Date and time of the detection

7.3.10 Scheduler

The **Scheduler** gives you the option of creating scheduled scanning and update jobs , and adapting or deleting existing jobs.

The following job is created by default after installation:

- Scan job **Quick System Scan** (enabled by default): A weekly quick system scan is automatically performed. During the quick system scan, only important files and folders on your computer are scanned for viruses or unwanted programs. You can modify the job **Quick System Scan**, but it is recommended to create other scan jobs, that would better reflect your needs.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
+	**Ins**	**Insert new job** Creates a new job. A wizard clearly guides you through the necessary settings.
i	**Return**	**Properties** Opens a dialog box with more information on the selected job.
✎	**F2**	**Edit job** Opens the wizard to create and alter a job.
×	**Del**	**Delete job** Deletes the selected jobs from the list.

📋		**Display report file** The report file of the Scheduler is displayed.
▶	**F3**	**Start job** Start a marked job from the list.
■	**F4**	**Stop job** Stops a started and marked job.

Table

Type of job

Icon	Description
🔄	The job is an update job.
🔍	The job is a scan job.

Name

Name of the job.

Action

Indicates whether the job is a **scan** or an **update**.

Frequency

Indicates how often and when the job is started.

Display mode

The following display modes are available:

Invisible: The job is performed in the background and is not visible. This applies to scanning jobs and update jobs.

Minimize: The job window only displays a progress bar.

Maximize: The job window is completely visible.

Enabled

The job is activated when you activate the check box.

Note
If the frequency of the job was set to **Immediate**, the job is started as soon as it is activated. This gives you the ability to restart the job if necessary.

Status

Displays the status of the job:

Ready: The job is ready for execution.

Running: The job has started and is being executed.

Create jobs with the Scheduler

The planning wizard supports you in planning, configuring and creating

- a timed scan for viruses and unwanted programs
- a timed update via the Internet or Intranet

For both types of jobs you must enter

- the name and the description of the job
- when the job should be started
- how often the job should be performed
- the display mode of the job

Frequency of the job

Frequency of the job	Description
Immediately	Job is started immediately after ending the planning wizard.
Daily	Job is started daily at a certain time, e.g. 22:00.
Weekly	Job is started weekly on a certain day or on several weekdays at a certain time, e.g. Tuesday and Friday, 16:26.
Interval	Job is performed at specific intervals, e.g. every 24 hours.

Single	Job is performed once at a defined time, e.g. on 10.04.04 at 10:04.
Login	Job is performed at each login of a Windows user.

Start time of the job

You can define a weekday, date, time or interval for the job start time. This is not displayed if you have entered **Immediately** as the start time.

Depending on the job type, there are various additional options

Also start job when connecting to Internet (dial-up)

In addition to the defined frequency, the job is performed when an Internet connection is set up.
This option can be selected with an update job that is to be performed daily, weekly or at other intervals.

Repeat job if the time has already expired

Past jobs are performed that could not be performed at the required time, for example because the computer was switched off.
This option can be selected both with an update job and with a scan job that is to be performed daily, weekly, at intervals or once.

Shut down computer if job is done

The computer is shut down when the job is finished. Scan jobs can be displayed minimized and maximized.

> **Note**
> With a scan job, it is possible to select pre-defined profiles and user-defined profiles in the dialog box **Selection of the profile**. The profile Manual selection is always performed with the current selection.

7.3.11 Reports

The **Reports** section enables you to access the results of actions performed by the program.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
📋	**Return**	**Display report** Opens a window in which the result of the selected action is displayed. For example the result of a scan.
i	**F3**	**Display report file** Displays the report file of the selected report.
🖨	**F4**	**Print report file** Opens the Windows print dialog to print the report file.
✕	**Del**	**Delete report(s)** Deletes the selected report and the relevant report file.

Table

Status

Icon	Description
✓	**Action scan**: Finished successfully without detecting virus.
⚠	**Action scan**: Virus detected or finished unsuccessfully.
↻	**Action update**: Successfully completed.
↻	**Action update**: Not successfully completed.

- **Action**

  Shows the action performed.

- **Result**

  Shows the result of the action.

- **Date/Time**

Shows the date and time when the report was created.

7.3.12 Contents of a report for a scan

- *Date of the scan:*

  The date of the scan.
- *Start time of the scan:*

  The start time of the scan in hh:mm.
- *Scanning time required:*

  The duration of the scan in mm:ss format.
- *Scan status:*

  Shows if the scan was completed.
- *Last detection:*

  Name of the last found virus or unwanted program.
- *Scanned directories:*

  Total number of scanned directories.
- *Scanned files:*

  Total number of scanned files.
- *Scanned archives:*

  Number of scanned archives.
- *Hidden objects:*

  Total number of hidden objects detected
- *Detections:*

  Total number of viruses and unwanted programs detected.
- *Suspicious:*

  Number of suspicious files.
- *Warnings:*

  Number of alerts about detected viruses.
- *Information:*

  Number of information items issued, for example further information that may arise during a scan.
- *Repaired:*

  Total number of repaired files
- *Quarantine:*

  Total number of files placed in quarantine.
- *Renamed:*

Total number of renamed files.

- *Deleted:*

  Total number of deleted files.

- *Wiped:*

  Total number of overwritten files.

> **Note**
> Rootkits have the ability to hide processes and objects, such as registry entries or files. However not every hidden object is necessarily proof of the existence of a rootkit. Hidden objects can also be harmless objects. If a scan detects hidden objects but does not issue a virus detection alert, you should use the report to determine which object is referred to and obtain more information about the detected object.

7.3.13 Events

Events that have been generated by the various program components are displayed under **Events**.

The events are stored in a database. You can limit the size of the event database or disable the restriction on the database size (see). Only the events of the last 30 days are saved in the default setting. The event display is automatically updated when you select the **Events** section.

> **Note**
> The display is not automatically updated when the section is selected if there are more than 20,000 events stored in the event database. In this case, press **F5** to update the event viewer.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
i	**Return**	**Show selected event** Opens a window in which the result of the selected action is displayed. For example the result of a scan.
	F3	**Export selected event(s)** Exports selected events.

☒	**Del**	**Delete selected event(s)** Deletes the selected event.

Note
You have the option of carrying out actions on a number of selected events. To select a number of events, press and hold the **Ctrl key** or the **Shift key** (selects consecutive events) as you select the events you want. To select all displayed events, press **Ctrl + A**.
In the case of the **Show selected event** action, performing the action on a multiple selection of objects is not possible.

Modules

The events of the following modules (here in alphabetical order) can be displayed by the event viewer:

Module's name
FireWall
Helper Service
Mail Protection
Real-Time Protection
Scheduler
System Scanner
Updater
Web Protection
ProActiv

By checking the box **All** you can display the events of all available modules. To display only the events of a specific module, please check the box next to the required module.

Filter

The following event classification can be displayed by the event viewer.

Icon	Description
ℹ	Information
❗	Warning
☒	Error
⚠	Detection

By checking the box **Filter** ▼ you can display all events. To display only certain events, please check the box next to the required event.

Table

The event list contains the following information:

- **Icon**

  The icon of the event classification.
- **Type**

  A classification of the event severity: *Information*, *Warning*, *Error*, *Detection*.
- **Module**

  The module that has logged the event. For example the Real-Time Protection module that made a detection.
- **Action**

  Event description of the respective module.
- **Date/Time**

  The date and the local time the event occurred.

7.3.14 Refresh

Updates the view of the opened section.

7.4 Extras

7.4.1 Boot records scan

You can also scan the boot sectors of the drives of your workstation with a system scan. This is recommended, for example, when a system scan detects a virus and you want to make sure that the boot sectors are not affected.

It is possible to select more than one boot sector by keeping the Shift key pressed and selecting the required drives with the mouse.

> **Note**
> You can have the boot sectors automatically scanned with a system scan (see Scan boot sectors of selected drives).

> **Note**
> As of Windows Vista, you must have administrator rights to scan the boot sectors.

7.4.2 Detection list

This function lists the names of the viruses and unwanted programs recognized by your Avira product. A convenient search function for the names is integrated.

Search detection list

Enter a search word or character sequence in the *Search for:* box.

Search for character sequence within a name

You can enter a consecutive sequence of letters or characters here on the keyboard and the marker moves to the first point in the list of names that includes this sequence – even in the middle of a name (example: "raxa" finds "Abraxas").

Search from the first character of a name

You can enter the initial letter and the following characters here on the keyboard and the marker scrolls alphabetically in the list of names (example: "Ra" finds "Rabbit").

If the name or sequence of characters searched for is available, the position found is marked in the list.

Search forwards

Starts the search forwards in alphabetical order.

Search backwards

Starts the search backwards in alphabetical order.

First match

Moves in the list to the first entry found.

Entries of the detection list

Under this title is a list of the names of viruses or unwanted programs that can be recognized. Most entries in this list can also be removed with your Avira product. They are listed in alphabetical order (first special characters and numbers, then the letters). Use the scroll bar to scroll up or down in the list.

7.4.3 Download rescue CD

The menu command **Download rescue CD** initiates the download of the Avira Rescue CD package. The package contains a bootable live system for PCs and an Avira anti-virus Scanner with the most up-to-date virus definition file and scan engine. You can use the Avira rescue CD to boot and operate your PC from the CD or DVD if the operating system is damaged, to rescue data or to execute a scan for viruses and malware.

Once the Avira rescue CD package has been downloaded, a dialog box appears in which you select a CD/DVD drive to burn the rescue CD. You also have the option of saving the Avira rescue CD package and burning the CD at a later date.

> **Note**
> You need an active Internet connection to download the Avira rescue CD package. You need a CD/DVD drive and a writable CD or DVD to burn the rescue CD.

7.4.4 Configuration

The menu item **Configuration** in the **Extras** menu opens the Configuration.

7.5 Update

7.5.1 Start update...

The menu item **Start update...** in the **Update** menu starts an immediate update. The virus definition file and scan engine are updated.

7.5.2 Manual update...

The menu item **Manual update...** in the **Update** menu opens a dialog box to select and load a VDF/search engine update package. The update package can be downloaded from the manufacturer's website and contains the current virus definition file and scan engine: http://www.avira.com

> **Note**
> As of Windows Vista, you must have administrator rights to perform a manual update.

7.6 Help

7.6.1 Topics

The menu item **Topics** in the **Help** menu opens the list of contents of the online help.

7.6.2 Help me

If an Internet connection is active, the **Help me** item in the **Help** menu opens the relevant Support page for your product on the Avira website. There you can read the answers to frequently asked questions, consult the knowledgebase and contact Avira Support.

7.6.3 Download manual

When an Internet connection is active, the menu command **Download Manual** in the **Help** menu opens the download page of your Avira product. This is where you will find the link for downloading the current version of the manual for your Avira product.

7.6.4 Load license file

The menu item **Load license file** in the **Help** menu opens a dialog to load the *.KEY* license file.

> **Note**
> As of Windows Vista, you must have administrator rights to load the license file.

7.6.5 Send feedback

When an Internet connection is active, the menu command **Send feedback** in the **Help** menu opens an feedback page for Avira products. Here you will find a product evaluation form that you can send to Avira with your assessments of product quality and other suggestions.

7.6.6 About Avira Professional Security

- **General**

  Addresses and information about your Avira product.
- **Version information**

  Version information for files in the Avira product package.
- **License information**

  License data for the current license and links to the online shop (buying or extending a license).

> **Note**
> You can save the license data in the cache. Right click on the *License data* area. A context menu opens. In the context menu, click on the menu command **Copy to clipboard**. Your license data is now saved to the clipboard and can be added to emails, forms or documents via the Windows **Add** command.

8. Configuration

- Overview of configuration options
- Configuration profiles
- Buttons

8.1 Overview of configuration options

The following configuration options are available:

- **System Scanner**: Configuration of a system scan (on-demand)
  - Scan options
  - Action on detection
  - Further actions
  - Archive scan options
  - System scan exceptions
  - System scan heuristics
  - Report function setting
- **Real-Time Protection**: Configuration of a realtime scan (on-access)
  - Scan options
  - Action on detection
  - Further actions
  - On-access scan exceptions
  - On-access scan heuristics
  - Report function setting
- **Update**: Configuration of the update settings, download via Web server or fileserver, set-up of product updates
  - Download via fileserver
  - Download via web server
  - Proxy settings
- **FireWall**: Configuration of the FireWall
  - Adapter rule setting
  - User-defined application rule settings
  - List of trusted vendors (exceptions for network access by applications)
  - Expanded settings: Automatic rule timeout, stop Windows Firewall, notifications
  - Popup settings (alerts for network access by applications)
- **Web Protection**: Configuration of Web Protection

  - Scan options, enabling and disabling the Web Protection
  - Action on detection
  - Blocked access: Unwanted file types and MIME types, Web filter for known unwanted URLS (malware, phishing, etc.)
  - Web Protection scan exceptions: URLs, file types, MIME types
  - Web Protection heuristics
  - Report function setting

- **Mail Protection**: Configuration of Mail Protection

  - Scan options: Enable the monitoring of POP3 accounts, IMAP accounts, outgoing emails (SMTP)
  - Actions on detection
  - Further actions
  - Mail Protection scan heuristics
  - AntiBot function: Permitted SMTP servers, permitted email senders
  - Mail Protection scan exceptions
  - Configuration of cache, empty cache
  - Configuration of a footer in sent emails
  - Report function setting

- **General**:

  - Configuration of email using SMTP
  - Threat categories for System Scanner and Real-Time Protection
  - Application filter: Block or allow applications
  - Advanced protection: Options to enable the ProActiv and Protection Cloud features.
  - Password protection for access to the Control Center and the Configuration
  - Security: block autostart function, complete system scan status display, product protection, protect Windows hosts file
  - WMI: Enable WMI support
  - Event log configuration
  - Configuration of report functions
  - Setting of directories used
  - Alerts:
    Configuration of network alerts for component(s):
    System Scanner
    Real-Time Protection
    Configuration of email alerts for component(s):
    System Scanner
    Real-Time Protection
    Updater
  - Configuration of acoustic alerts when malware is detected

8.2 Configuration profiles

To manage the configuration profiles click the tray icon on the right side of the standard configuration (see Tray Icon).
Once you click there, a number of options will be displayed, and you can save configuration options for profiles in groups: first add a new configuration and then enter the required values in the new configuration, that is, define the rules by which these profiles will be applied.

You can choose between a manual change of the configuration or an automatic one. If you want to set the change as automatic, you will have to define the rules to apply.
The options you are given are: to choose a default rule that will apply every time that an unassigned gateway is used, or to set an IP or MAC address (or an IP address and a network mask) to define the default gateway. These configuration profiles will be applied every time the defined gateway is used.

If no switching rules have been defined, you can switch to a configuration manually in the context menu. You can manage the configuration profiles using the menu of the configuration heading:

8.3 Context menu

Shortcut	Context menu / description
Ins	**Create new configuration** Creates a new configuration with standard values for the various configuration options.
F2	**Rename configuration** Edits the name of the configuration.
Del	**Delete configuration** Deletes the highlighted configuration: First a dialog is opened in which you can cancel or confirm the selected configuration.
F4	**Copy configuration** Copies the highlighted configuration.

F6	**Reset configuration** Resets the configuration options of the highlighted configuration to default values.
	Rules: Shows the different options to set rules for the configuration profiles: **None** There are no valid rules for switching to the highlighted configuration. The switchover to the relevant configuration must be executed manually. **Default rule** The selected configuration is used as the default configuration. An automatic switchover to the selected configuration takes place when the used gateway has not been assigned to any configuration. **Default gateway** An IP address or MAC address of the default gateway can be specified as the switching rule for the highlighted configuration. An automatic switchover to the selected configuration takes place when the specified default gateway is used. **IP address** An IP address with the network mask of a network adapter can be specified as the switching rule for the highlighted configuration. An automatic switchover to the selected configuration takes place when the specified IP address is used.

Note
You can save up to eight configurations.

Note
If an applicable rule is not found when switching the gateway, the last configuration found remains active.

8.3.1 Buttons

Button	Description
Default values	All settings of the configuration are restored to default values. All amendments and custom entries are lost when default settings are restored.
OK	All the settings made are saved. The configuration is closed. The User Account Control (UAC) will ask for your permission to apply changes in operating systems as of Windows Vista.
Cancel	The configuration is closed without saving your settings in the configuration.
Apply	All the settings made are saved. The User Account Control (UAC) will ask for your permission to apply changes in operating systems as of Windows Vista.

8.4 System Scanner

The **System Scanner** section of configuration is responsible for the configuration of the on-demand scan.

8.4.1 Scan

You can define the behavior of the on-demand scan routine. If you select certain directories to be scanned, depending on the configuration, the System Scanner scans:

- with a certain scanning priority,
- also boot sectors and main memory,
- all or selected files in the directory.

Files

The System Scanner can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and file extension. The filter is not used.

> **Note**
> If **All files** is enabled, the button **File extensions** cannot be selected.

Use smart extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by the program. This means that your Avira program decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since not only on the basis of the file extension is scanned. This option is enabled as the default setting and is recommended.

> **Note**
> If **Use smart extensions** is enabled, the button **File extensions** cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button "**File extension**".

> **Note**
> If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "*No file extensions*" under the button **File extensions**.

File extensions

With the aid of this button, a dialog box is opened in which all file extensions are displayed that are scanned in "**Use file extension list"** mode. Default entries are set for the extensions, but entries can be added or deleted.

> **Note**
> Please note that the default list may vary from version to version.

Additional settings

Scan boot sectors of selected drives

If this option is enabled, the System Scanner scans the boot sectors of the drives selected for the system scan. This option is enabled as the default setting.

Scan master boot sectors

If this option is enabled, the System Scanner scans the master boot sectors of the hard disk(s) used in the system.

Ignore offline files

If this option is enabled, the direct scan ignores so-called offline files completely during a scan. This means that these files are not scanned for viruses and unwanted programs. Offline files are files that were physically moved by a so-called Hierarchical Storage Management System (HSMS) from the hard disk onto a tape, for example. This option is enabled as the default setting.

Integrity checking of system files

When this option is enabled, the most important Windows system files are subjected to a particularly secure check for changes by malware during every on-demand scan. If an amended file is detected, this is reported as suspect. This function uses a lot of computer capacity. That is why the option is disabled as the default setting.

> **Note**
> This option is only available with Windows Vista and higher. The option is **not** available if you are managing the Avira program under AMC.

> **Note**
> This option should not be used if you are using third-party tools that modify system files and adapt the boot or start screen to your own requirements. Examples of such tools are skinpacks, TuneUp utilities or Vista Customization.

Optimized scan

When the option is enabled, the processor capacity is optimally utilized during a System Scanner scan. For performance reasons, an optimized scan is only logged on standard level.

> **Note**
> This option is only available on multi-processor systems. If your Avira program is managed with AMC, the option is always displayed and can be enabled: If the managed system does not have more than one processor, the System Scanner option is not used.

Follow symbolic links

If this option is enabled, System Scanner performs a scan that follows all symbolic links in the scan profile or selected directory and scans the linked files for viruses and malware.

> **Note**
> The option does not include any shortcuts, but refers exclusively to symbolic links (generated by mklink.exe) or Junction Points (generated by junction.exe) that are transparent in the file system.

Search for Rootkits before scan

If this option is enabled and a scan is started, the System Scanner scans the Windows system directory for active rootkits in a so-called shortcut. This process does not scan your computer for active rootkits as comprehensively as the scan profile "**Scan for rootkits**", but it is significantly quicker to perform. This option only changes the settings of profiles created by you.

> **Note**
> The rootkits scan is not available for Windows XP 64 bit

Scan Registry

If this option is enabled, the Registry is scanned for references to malware. This option only changes the settings of profiles created by you.

Ignore files and paths on network drives

If this option is enabled, network drives connected to the computer are excluded from the on-demand scan. This option is recommended when the servers or other workstations are themselves protected with anti-virus software. This option is disabled as the default setting.

Scan process

Allow stopping the Scanner

If this option is enabled, the scan for viruses or unwanted programs can be terminated at any time with the button "**Stop"** in the "Luke Filewalker" window. If you have disabled this setting, the **Stop** button in the "Luke Filewalker" window has a gray background. Premature ending of a scan process is thus not possible! This option is enabled as the default setting.

Scanner priority

With the on-demand scan, the System Scanner distinguishes between priority levels. This is only effective if several processes are running simultaneously on the workstation. The selection affects the scanning speed.

low

The System Scanner is only allocated processor time by the operating system, if no other process requires computation time, i.e. as long as only the System Scanner is running, the speed is maximum. All in all, work with other programs is optimal: The computer responds more quickly if other programs require computation time while the System Scanner continues running in the background.

medium

The System Scanner is executed with normal priority. All processes are allocated the same amount of processor time by the operating system. This option is enabled as the default setting and is recommended. Under certain circumstances, work with other applications may be affected.

high

The System Scanner has the highest priority. Simultaneous work with other applications is almost impossible. However, the System Scanner completes its scan at maximum speed.

Action on detection

You can define the actions to be performed by System Scanner when a virus or unwanted program is detected.

Interactive

If this option is enabled, the results of the System Scanner scan are displayed in a dialog box. When carrying out a scan with the System Scanner, you will receive an alert with a list of the affected files at the end of the scan. You can use the content-sensitive menu to select an action to be executed for the various infected files. You can execute the standard actions for all infected files or cancel the System Scanner.

> **Note**
> In the System Scanner dialog, the action **Quarantine** is displayed as the default action.

Permitted actions

In this box actions can be specified, which can be selected in individual or expert notification mode in case of a virus detection. You must activate the corresponding options for this.

Repair

The System Scanner repairs the infected file if possible.

Rename

The System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. The file can be repaired at a later time and renamed again.

Quarantine

The System Scanner moves the file to Quarantine. The file can be recovered from quarantine manager if it has an informative value or - if necessary - sent to the Avira

Malware Research Center. Depending on the file, further selection options are available in the quarantine manager.

Delete

The file will be deleted. This process is much faster than "overwrite and delete".

Ignore

The file is to be ignored.

Overwrite and delete

The System Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Default

The button is used to define a default action by the System Scanner to handle the files encountered. Highlight an action and click the "**Default"** button. Only the selected default action for the relevant files can be executed in combined notification mode. The selected default action for the relevant files is preselected in individual and expert notification mode.

> **Note**
> The action **repair** cannot be selected as the default action.

> **Note**
> If you have selected **Delete** or **Overwrite and delete** as the default action and wish to set the notification mode to combined, please note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

Automatic

If this option is enabled, no dialog box in case of a virus detection appears. The System Scanner reacts according to the settings you predefine in this section as primary and secondary action.

Copy file to quarantine before action

If this option is enabled, the System Scanner creates a backup copy before carrying out the requested primary or secondary action. The back-up copy is saved in Quarantine, where the file can be restored if it is of informative value. You can also send the backup copy to the Avira Malware Research Center for further investigation.

Display detection alerts

If this option is activated, then for each detection of a virus or unwanted program an alert appears showing the actions being executed.

Primary action

Primary action is the action performed when the System Scanner finds a virus or an unwanted program. If the option "**Repair"** is selected but the affected file cannot be repaired, the action selected under "**Secondary action"** is performed.

> Note
> The option **Secondary action** can only be selected if the setting **Repair** was selected under **Primary action**.

Repair

If this option is enabled, the System Scanner repairs affected files automatically. If the System Scanner cannot repair an affected file, it carries out the action selected under Secondary action.

> Note
> An automatic repair is recommended, but means that the System Scanner modifies files on the workstation.

Rename

If this option is enabled, the System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the System Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

> Warning
> The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the System Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Secondary action

The option "**Secondary action"** can only be selected if the setting **Repair** was selected under "**Primary action"**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

Rename

If this option is enabled, the System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the System Scanner moves the file to Quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the System Scanner overwrites the file with a default pattern and then deletes (wipes) it. It cannot be restored.

Note
If you have selected **Delete** or **Overwrite and delete** as the primary or secondary action, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

Further actions

Launch program following detection

After the on-demand scan, the System Scanner can open a file of your choice if at least one virus or unwanted program has been detected, for example an email program, so that you can inform other users or the administrator.

Note
For security reasons it is only possible to start a program after a detection when

> a user is logged on the computer. The file is then opened with the rights that apply to the logged on user. If no user is logged on, this option is not performed.

Program name

In this input box you can enter the name and the relevant path of the program that the System Scanner should start after a detection.

This button opens a window in which you can select the desired program with the aid of the file selection dialog.

Arguments

In this input box you can enter command line parameters for the program to be started if necessary.

Event log

Use event log

If this option is enabled, an event report with the results of the scan is transferred to the Windows Event Log after a System Scanner scan has been completed. The events can be called up in the Windows Event Viewer. The option is disabled as the default setting.

Archives

When scanning archives, the System Scanner uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again.

Scan archives

If this option is enabled, the selected archives in the archive list are scanned. This option is enabled as the default setting.

All archive types

If this option is enabled, all archive types in the archive list are selected and scanned.

Smart Extensions

If this option is enabled, the System Scanner detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. However every file must be opened for this, which reduces the scanning speed. Example: If a *.zip archive has the file extension *.xyz, the System Scanner also unpacks this archive and scans it. This option is enabled as the default setting.

Note
Only those archive types marked in the archive list are supported.

Limit recursion depth

Unpacking and scanning recursive archives can require a great deal of computer time and resources. If this option is enabled, you limit the depth of the scan in multi-packed archives to a certain number of packing levels (maximum recursion depth). This saves time and computer resources.

Note
In order to find a virus or an unwanted program in an archive, the System Scanner must scan up to the recursion level in which the virus or the unwanted program is located.

Maximum recursion depth

In order to enter the maximum recursion depth, the option Limit recursion depth must be enabled.
You can either enter the requested recursion depth directly or by means of the right arrow key on the entry field. The permitted values are 1 to 99. The standard value is 20 which is recommended.

Default values

The button restores the pre-defined values for scanning archives.

Archives

In this display area you can set which archives the System Scanner should scan. For this, you must select the relevant entries.

Exceptions

File objects to be omitted for the System Scanner

The list in this window contains files and paths that should not be included by the System Scanner in the scan for viruses or unwanted programs.

Please enter as few exceptions as possible here and really only files that, for whatever reason, should not be included in a normal scan. We recommend that you always scan these files for viruses or unwanted programs before they are included in this list!

Note
The entries in the list must not result in more than 6000 characters in total.

Warning
These files are not included in a scan!

Note
The files included in this list are recorded in the report file. Please check the report file from time to time for unscanned files, as perhaps the reason you excluded a file here no longer exists. In this case you should remove the name of this file from this list again.

Input box

In this input box you can enter the name of the file object that is not included in the on-demand scan. No file object is entered as the default setting.

...

The button opens a window in which you can select the required file or the required path.
When you have entered a file name with its complete path, only this file is not scanned for infection. If you have entered a file name without a path, all files with this name (irrespective of the path or drive) are not scanned.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Note
If you are managing the Avira program in AMC, you can use variables in the path details for file exceptions. You can find a list of variables you can use under Variables: Real-Time Protection und System Scanner Exceptions.

Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristic

Macrovirus heuristic

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

8.4.2 Report

The System Scanner has a comprehensive reporting function. You thus obtain precise information on the results of an on-demand scan. The report file contains all entries of the system as well as alerts and messages of the on-demand scan.

> **Note**
> To be able to establish what actions the System Scanner has performed, when viruses or unwanted programs have been detected, you should activate the report file in the configuration.

Reporting

Off

If this option is enabled, the System Scanner does not report the actions and results of the on-demand scan.

Default

When this option is activated, the System Scanner logs the path and names of the concerning files. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

Extended

When this option is activated, the System Scanner logs alerts and tips in addition to the default information. The report also contains a '(cloud)' suffix to identify the detections from Protection Cloud.

Complete

When this option is activated, the System Scanner also logs all scanned files. In addition, all files involved as well as alerts and tips are included in the report file.

> **Note**
> If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

8.5 Real-Time Protection

The **Real-Time Protection** section of the configuration is responsible for the configuration of the on-access scan.

8.5.1 Scan

You will normally want to monitor your system constantly. To this end, use the Real-Time Protection (= on-access System Scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

Files

The Real-Time Protection can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and their file extension.

> **Note**
> If **All files** is enabled, the **File extensions** button cannot be selected.

Use smart extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by the program. This means that the program decides whether the files are scanned or not based on their content. This procedure is somewhat slower than **Use file extension list**, but more secure, since not only on the basis of the file extension is scanned.

> **Note**
> If **Use smart extensions** is enabled, the **File extensions** button cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the "**File extensions"** button. This option is enabled as the default setting and is recommended.

> **Note**
> If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the **File extensions** button.

File extensions

With the aid of this button, a dialog box is opened in which all file extensions are displayed that are scanned in "**Use file extension list"** mode. Default entries are set for the extensions, but entries can be added or deleted.

> **Note**
> Please note that the file extension list may vary from version to version.

Drives

Monitor network drives

If this option is enabled, files on network drives (mapped drives) such as server volumes, peer drives etc., are scanned.

Note
In order not to reduce the performance of your computer too much, the option **Monitor network drives** should only be enabled in exceptional cases.

Warning
If this option is disabled, the network drives are **not** monitored. They are no longer protected against viruses or unwanted programs!

Note
When files are executed on network drives, they are scanned by the Real-Time Protection irrespective of the setting for the **Monitor network drives** option. In some cases files on network drives are scanned while being opened, even though the **Monitor network drives** option is disabled. Reason: These files are accessed with ‘Execute File’ rights. If you want to exclude these files or even executed files on network drives from scanning by the Real-Time Protection, enter the files in the list of file objects to be excluded (see: Real-Time Protection > Scan > Exceptions).

Enable caching

If this option is enabled, monitored files on network drives will be made available in the Real-Time Protection's cache. Monitoring of network drives without the caching function is more secure, but does not perform as well as the monitoring of network drives with caching.

Archives

Scan archives

If this option is enabled, then archives will be scanned. Compressed files are scanned, then decompressed and scanned again. This option is deactivated by default. The archive scan is restricted by the recursion depth, the number of files to be scanned and the archive size. You can set the maximum recursion depth, the number of files to be scanned and the maximum archive size.

Note
This option is deactivated by default, since the process puts heavy demands on the computer's performance. It is generally recommended that archives be checked using an on-demand scan.

Max. recursion depth

When scanning archives, the Real-Time Protection uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. You can define the recursion depth. The default value for the recursion depth is 1 and is recommended: all files that are directly located in the main archive are scanned.

Max. number of files

When scanning archives, you can restrict the scan to a maximum number of files in the archive. The default value for the maximum number of files to be scanned is 10 and is recommended.

Max. size (KB)

When scanning archives, you can restrict the scan to a maximum archive size to be unpacked. The standard value of 1000 KB is recommended.

Action on detection

You can define the actions to be performed by Real-Time Protection when a virus or unwanted program is detected.

Interactive

If this option is enabled, a desktop notification appears when Real-Time Protection detects a virus or unwanted program. You have the option of removing the detected malware or accessing other possible virus treatment actions via the "**Details**" button. The actions are displayed in a dialog box. This option is enabled as the default setting.

Permitted actions

In this display box you can specify the virus management actions that should be available as further actions in the dialog box. You must activate the corresponding options for this.

Repair

Real-Time Protection repairs the infected file if possible.

Rename

Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. The file can be repaired at a later time and renamed again.

Quarantine

Real-Time Protection moves the file to Quarantine. The file can be recovered from Quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center. Depending on the file, further options are available in the Quarantine manager.

Delete

The file will be deleted. This process is much faster than **Overwrite and delete** (see below).

Ignore

Access to the file is permitted and the file is ignored.

Overwrite and delete

Real-Time Protection overwrites the file with a default pattern before deleting it. It cannot be restored.

Warning
If Real-Time Protection is set to **Scan when writing**, the affected file is not written.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that should be activated by default and click on the "**Default**" button.

Note
The action **Repair** cannot be selected as the default action.

Click here for more information.

Automatic

If this option is enabled, no dialog box in case of a virus detection appears. Real-Time Protection reacts according to the settings you predefine in this section as primary and secondary action.

Copy file to quarantine before action

If this option is enabled, the Real-Time Protection creates a backup copy before carrying out the requested primary or secondary action. The backup copy is saved in quarantine. It can be restored via the Quarantine manager if it is of informative value. You can also send the backup copy to the Avira Malware Research Center. Depending on the object, more selection options are available in the Quarantine manager.

Display detection alerts

If this option is enabled, then for each detection of a virus or unwanted program an alert appears.

Primary action

Primary action is the action performed when the Real-Time Protection finds a virus or an unwanted program. If the "**Repair**" option is selected but the affected file cannot be repaired, the action selected under "**Secondary action**" is performed.

Note
The **Secondary action** option can only be selected if the **Repair** setting was selected under **Primary action**.

Repair

If this option is enabled, the Real-Time Protection repairs affected files automatically. If the Real-Time Protection cannot repair an affected file, it carries out the action selected under **Secondary action**.

> Note
> An automatic repair is recommended, but means that the Real-Time Protection modifies files on the workstation.

Rename

If this option is enabled, the Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the Real-Time Protection moves the file to Quarantine. The files in this directory can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than **Overwrite and delete**.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

> Warning
> The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the Real-Time Protection overwrites the file with a default pattern and then deletes it. It cannot be restored.

Deny access

If this option is enabled, the Real-Time Protection only enters the detection in the report file if the report function is enabled. In addition, the Real-Time Protection writes an entry in the Event log, if this option is enabled.

> Warning
> If Real-Time Protection is set to **Scan when writing**, the affected file is not written.

Secondary action

The option **Secondary action** can only be selected if the **Repair** option was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

Rename

If this option is enabled, the Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the Real-Time Protection moves the file to Quarantine. The files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than **Overwrite and delete**.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

> **Warning**
> The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the Real-Time Protection overwrites the file with a default pattern and then deletes it. It cannot be restored.

Deny access

If this option is enabled, the affected file is not written; the Real-Time Protection only enters the detection in the report file if the report function is enabled. In addition, the Real-Time Protection writes an entry in the Event log, if this option is enabled.

> **Note**
> If you have selected **Delete** or **Overwrite and delete** as the primary or secondary action, please note: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

Further actions

Use event log

If this option is enabled, an entry is added to the Windows event log for every detection. The events can be called up in the Windows event viewer. This option is enabled as the default setting.

Exceptions

With these options you can configure exception objects for the Real-Time Protection (on-access scan). The relevant objects are then not included in the on-access scan. The Real-Time Protection can ignore file accesses to these objects during the on-access scan via the list of processes to be omitted. This is useful, for example, with databases or backup solutions.

Please note the following when specifying processes and file objects to be omitted: The list is processed from top to bottom. The longer the list is, the more processor time is required for processing the list for each access. Therefore, keep the list as short as possible.

Processes to be omitted by the Real-Time Protection

All file accesses of processes in this list are excluded from monitoring by Real-Time Protection.

Input box

In this field, enter the name of the process that is to be ignored by the real-time scan. No process is entered as the default setting.

The specified path and file name of the process should contain a maximum of 255 characters. You can enter up to 128 processes. The entries in the list must not result in more than 6000 characters in total.

When entering the process, Unicode symbols are accepted. You can therefore enter process or directory names containing special symbols.

Drive information must be entered as follows: `[Drive letter]:\`

The colon symbol (:) is only used to specify drives.

When specifying the process, you can use the wildcards * (any number of characters) and ? (a single character).

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

To avoid the process being excluded globally from monitoring by Real-Time Protection, specifications exclusively comprising the following characters are invalid: * (asterisk), ? (question mark), / (forward slash), \ (backslash), . (dot), : (colon).

You have the option of excluding processes from monitoring by the Real-Time Protection without full path details. For example: `application.exe`

This however only applies to processes where the executable files are located on hard disk drives.

Full path details are required for processes where the executable files are located on connected drives, e.g. network drives. Please note the general information on the notation of Exceptions on connected network drives.

Do not specify any exceptions for processes where the executable files are located on dynamic drives. Dynamic drives are used for removable disks, such as CDs, DVDs or USB sticks.

> **Warning**
> Please note that all file accesses done by processes recorded in the list are excluded from the scan for viruses and unwanted programs!

...

The button opens a window in which you can select an executable file.

Processes

The "**Processes**" button opens the "**Process selection**" window in which the running processes are displayed.

Add

With this button, you can add the process entered in the input box to the display window.

Delete

With this button you can delete a selected process from the display window.

File objects to be omitted by the Real-Time Protection

All file accesses to objects in this list are excluded from monitoring by the Real-Time Protection.

Input box

In this box you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.

The entries in the list must have no more than 6000 characters in total.

When specifying file objects to be omitted, you can use the wildcards* (any number of characters) and ? (a single character): Individual file extensions can also be excluded (including wildcards):

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

Directory names must end with a backslash \ .

If a directory is excluded, all its sub-directories are automatically also excluded.

For each drive you can specify a maximum of 20 exceptions by entering the complete path (starting with the drive letter). For example:

```
C:\Program Files\Application\Name.log
```

The maximum number of exceptions without a complete path is 64. For example:

```
*.log
\computer1\C\directory1
```

In case of dynamic drives that are mounted as a directory on another drive, the alias of the operating system for the integrated drive in the list of the exceptions has to be used, e.g.:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

If you use the mount point itself, for example, `C:\DynDrive`, the dynamic drive will be scanned nonetheless. You can determine the alias of the operating system to be used from the Real-Time Protection report file.

The button opens a window in which you can select the file object to be excluded.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

With this button you can delete a selected file object from the display window.

Please note the further information when specifying exceptions:

In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.

A file name that contains wildcards may not be terminated with a backslash. For example:
`C:\Program Files\Application\applic*.exe\`
This entry is not valid and not treated as an exception!

Please note the following with regard to **exceptions on connected network drives**: If you use the drive letter of the connected network drive, the files and folders specified are NOT excluded from the Real-Time Protection scan. If the UNC path in the list of exceptions differs from the UNC path used to connect to the network drive (IP address specification in the list of exceptions – specification of computer name for connection to network drive), the specified folders and files are NOT excluded by the Real-Time Protection scan. Locate the relevant UNC path in the Real-Time Protection report file:
`\\<Computer name>\<Enable>\` - OR - `\\<IP address>\<Enable>\`

You can locate the path Real-Time Protection uses to scan for infected files in the Real-Time Protection report file. Indicate exactly the same path in the list of exceptions.

Proceed as follows: Set the protocol function of the Real-Time Protection to **Complete** in the configuration under Real-Time Protection > Report. Now access the files, folders, mounted drives or connected network drives with the activated Real-Time Protection. You can now read the path to be used from the Real-Time Protection report file. The report file can be accessed in the Control Center under Local protection > Real-Time Protection.

If you are managing the Avira product in AMC, you can use variables in the path details for process and file exceptions. You can find a list of variables you can use under Variables: Real-Time Protection and Scanner Exceptions.

Examples for processes to be excluded:

- `application.exe`
  The *application.exe* process is excluded from the Real-Time Protection scan, irrespective of which hard disk drive it is located on and which directory it is in.
- `C:\Program Files1\Application.exe`
  The process for the file *application.exe*, which is located under the path *C:\Program Files1*, is excluded from the Real-Time Protection scan.
- `C:\Program Files1\*.exe`
  All processes for executable files located under the path *C:\Program Files1* are excluded from the Real-Time Protection scan.

Examples for files to be excluded:

- `*.mdb`
  All files with the extension '*mdb*' are excluded from the Real-Time Protection scan.
- `*.xls*`
  All files with a file extension beginning '*xls*' are excluded from the Real-Time Protection scan, e.g. files with the extensions *.xls* and *.xlsx*.
- `C:\Directory\*.log`
  All log files with the extension '*log*', located under the path *C:\Directory*, are excluded from the Real-Time Protection scan.
- `\\Computer name\Shared1\`
  All files are excluded from the Real-Time Protection scan accessed via a connection '*\\Computer name1\Shared1*'. This is generally a connected network drive which accesses another computer with a shared folder via the computer name '*Computer name1*' and the shared name '*Shared1*'.
- `\\1.0.0.0\Shared1\*.mdb`
  All files with the extension '*mdb*' are excluded from the Real-Time Protection scan accessed via a connection '*\\1.0.0.0\Shared1*'. This is generally a connected network drive which accesses another computer with a shared folder via the IP address '1.0.0.0' and the shared name '*Shared1*'.

Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

8.5.2 Report

Real-Time Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then Real-Time Protection does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, Real-Time Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, Real-Time Protection logs less important information to the report file as well.

Complete

If this option is enabled, Real-Time Protection logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size. Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Backup report file before shortening

If this option is enabled, the report file is backed up before shortening. For the save location see Report directory.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

> **Note**
> If you have not specified any report file restriction, a new report file is automatically created when the report file reaches 100 MB. A backup of the old report file is created. Up to three backups of old report files are saved. The oldest backups are deleted first.

8.6 Variables: Real-Time Protection and System Scanner exceptions

If your Avira product is managed with AMC, you may use variables to configure exceptions for the Real-Time Protection and the System Scanner. When saving the configuration on the managed system, the variables are automatically replaced by true values corresponding to the operating system and its language.

The following variables may be used:

8.6.1 Variables for Windows XP 32-Bit (**English)

Variable	Windows XP 32-Bit (**English)
`%WINDIR%`	*C:\Windows*
`%SYSDIR%`	*C:\Windows\System32*
`%ALLUSERSPROFILE%`	*C:\Documents and Settings\All Users ***
`%PROGRAMFILES%`	*C:\Program Files ***
`%PROGRAMFILES(x86)%`	*C:\Program Files (x86) ***
`%SYSTEMROOT%`	*C:\Windows*
`%INSTALLDIR%`	*C:\Program Files\Avira\Antivir Desktop ***
`%AVAPPDATA%`	*C:\Documents and Settings\All Users\Avira\AntiVir Desktop ***

The paths marked with ****** are language dependent. The above mentioned examples name the relevant paths on an English operating system.

8.6.2 Variables for Windows 7 32-Bit/ 64-Bit (**English)

Variable	Windows 7 32-Bit (**English)	Windows 7 64-Bit (**English)
%WINDIR%	*C:\Windows*	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\ProgramData*	*C:\ProgramData*
%PROGRAMFILES%	*C:\Program Files ** *	*C:\Program Files ** *
%PROGRAMFILES(x86)%	*C:\Program Files (x86) ** *	*C:\Program Files (x86) ** *
%SYSTEMROOT%	*C:\Windows*	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop ** *	*C:\Program Files (x86)\Avira\Antivir Desktop ** *
%AVAPPDATA%	*C:\ProgramData\Avira\AntiVir Desktop*	*C:\ProgramData\Avira\AntiVir Desktop*

The paths marked with ****** are language dependent. The above mentioned examples name the relevant paths on an English operating system.

8.7 Update

In the **Update** section you can configure the automatic receiving of updates and the connection to the download servers. You can specify various update intervals and activate or deactivate automatic updating.

> **Note**
> If you configure your Avira product in the Avira Management Console, automatic updates are not available.

Automatic update

Activate

If this option is enabled, automatic updates are performed for the enabled events at the specified interval.

All n Day(s) / Hour(s) / Minute(s)

In this box you can specify the interval at which the automatic update is performed. To change the update interval, highlight one of the time options in the box and change it using the arrow keys to the right of the input box.

Also start job when Internet connection is established

If this option is enabled, in addition to the specified update interval, the update job is performed every time an Internet connection is established.

Repeat job if the time has already expired

If this option is enabled, past update jobs are performed that could not be performed at the time specified, for example because the computer was switched off.

> .
> If this option is enabled, you can configure the Web server and, where necessary, the proxy server.

via file server / shared folders

The update is performed via a file server on an intranet which obtains the update files from a proprietary download server on the Internet.

> **Note**
> You can access further settings for updating via a file server under:
> Configuration > PC Protection > Update > File server.
> If this option is enabled, you can configure the file server you are using.

8.7.1 File server

In the case of more than one workstation on a network, your Avira product can download an update from a file server in the intranet, which in turn obtains the update files from a proprietary download server on the Internet. This ensures that the Avira product is up-to-date on all workstations.

> **Note**
> The Configuration heading is only enabled if under Configuration > PC Protection > Update the **via File Server / Shared folders** option has been selected.

Download

Enter the name of the file server on which the update files for your Avira product and the required directories *'/release/update/'* are located. The following must be specified:

`file://<IP address of the file server>/release/update/`. The 'release' directory must be a directory that can be accessed by all users.

The button opens a window in which you can select the required download directory.

Server login

Login name

Enter a user name to log in on the server. Use a user account with access rights to the used shared folders on the server.

Login password

Enter the password for the user account. The characters entered are masked with *.

> **Note**
> If you do not specify any data in the Server login section, no authentication will be performed when accessing the file server. In this case the user must have sufficient rights for the file server.

8.7.2 Web server

Web server

The update can be performed directly via a web server on the Internet or the intranet.

Web server connection

Use existing connection (network)

This setting is displayed if your connection is used via a network.

Use the following connection

This setting is displayed if you define your connection individually.

The Updater automatically detects which connection options are available. Connection options that are not available are grayed out and cannot be activated. A dial-up connection can be established manually via a phone book entry in Windows, for example.

User

Enter the user name of the selected account.

Password

Enter the password for this account. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

> **Note**
> If you have forgotten an existing Internet account name or password, contact your Internet Service Provider.

> **Note**
> The automatic dial-up of the updater through so-called dial-up tools (e.g. SmartSurfer, Oleco, etc.) is currently not yet available.

Terminate a dial-up connection that was set up for the update

If this option is enabled, the dial-up connection made for the update is automatically interrupted again as soon as the download has been successfully performed.

> **Note**
> This option is only available under Windows XP. Under newer operating systems the dial-up connection opened for the update is always terminated as soon as the download has been performed.

Download

Priority server

In this field, enter the update directory and URL of the web server that will first be requested to provide the update. If this server cannot be reached, the standard servers indicated will be used. The format for the address of the web server is as follows: `http://<hostname or IP>[:port]/update`. If you do not specify a port, port 80 will be used.

Default server

Enter the URL and update directory of the web servers from which the updates are to be downloaded. Multiple entries are separated by commas. The address format is: `http://<hostname or IP>[:port]/update`. If you do not specify a port, port 80 will be used. By default, the accessible Avira web servers are specified for updating. You can, however, use your own web servers on the company intranet. If a number of web servers are specified, separate each one by a comma.

Default

The button restores the predefined addresses.

Proxy settings

Proxy server

Do not use a proxy server

If this option is enabled, your connection to the web server is not established via a proxy server.

Use proxy system settings

When the option is enabled, the current Windows system settings are used for the connection to the web server via a proxy server. Configure the Windows system settings to use a proxy server under **Control panel > Internet options > Connections > LAN settings**. You can also access the Internet options in the **Extras** menu in Internet Explorer.

> **Warning**
> If you are using a proxy server which requires authentication, enter all the required data under the option **Use this proxy server**. The **Use proxy system settings** option can only be used for proxy servers without authentication.

Use this proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

Address

Enter the computer name or IP address of the proxy server you want to use to connect to the web server.

Port

Please enter the port number of the proxy server you want to use to connect to the web server.

Login name

Enter a user name to log in on the proxy server.

Login password

Enter the relevant password for logging in on the proxy server here. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

Examples:

Address: `proxy.domain.com` Port: `8080`

Address: `192.168.1.100` Port: `3128`

8.8 FireWall

Avira Professional Security allows you to configure to manage the Windows Firewall (starting from Windows 7):

- Avira FireWall

- Avira FireWall under AMC
- Windows Firewall

8.8.1 Avira FireWall

The **FireWall** section under **Configuration > Internet Protection** is responsible for configuration of the Avira FireWall (in operating systems up to Windows 7).

Adapter rules

In the Avira FireWall, an adapter represents a software simulated hardware device (e.g. miniport, bridge connection, etc.) or a real hardware device (e.g. network card).

The Avira FireWall displays the adapter rules of all existing adapters on your computer for which a driver was installed.

- ICMP protocol
- TCP Port Scan
- UDP Port Scan
- Incoming Rules
- Outgoing Rules
- Buttons to manage the rules

A predefined adapter rule depends on the security level. You can change the *Security level* under **Internet Protection > FireWall** in the Control Center or define your own adapter rules. If you have defined your own adapter rules, the *Security level* in the FireWall section of the Control Center is set to **Custom**.

> **Note**
> The default *Security level* setting for all predefined rules of the Avira FireWall is **Medium.**

ICMP protocol

The Internet Control Message Protocol (ICMP) is used to exchange error and information messages on networks. The protocol is also used for status messages with ping or tracer. With this rule, you can define the incoming and outgoing blocked message types, the behavior in case of flooding and the reaction to fragmented ICMP packets. This rule serves for preventing so-called ICMP flood attacks, which results in an increase of the CPU load of the attacked machine as it responds to every packet.

Predefined rules for the ICMP protocol

Setting	Rules
Low	Incoming blocked types: **no type**. Outgoing blocked types: **no type**. Assume flooding if delay between packets is less than **50** ms. **Reject** fragmented ICMP packets.
Medium	Same rule as for the Low level.
High	Incoming blocked types: **several types** Outgoing blocked types: **several types** Assume flooding if delay between packets is less than **50** ms. **Reject** fragmented ICMP packets.

Incoming blocked types: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can specify the desired incoming ICMP message types you want to block.

Outgoing blocked types: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can select the desired outgoing ICMP message types you want to block.

Assume Flooding

With a mouse click on the link, a dialog box is displayed where you can enter the maximum allowed ICMP delay. Example: `50` milliseconds.

Fragmented ICMP packets

With a mouse click on the link, you have the choice between **Reject** and **Don't reject** fragmented ICMP packets.

TCP port scan

With this rule, you can define when a TCP port scan is assumed by the FireWall and what should be done in this case. This rule serves for preventing so-called TCP port scan attacks that result in a detection of open TCP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the TCP Port Scan

Setting	Rules
Low	Assume a TCP Port Scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **don't add** rule to block the attack.
Medium	Assume a TCP Port Scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.
High	Same rule as for Medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a TCP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a TCP port scan is assumed.

Event database

With a mouse click on the link you have the choice between **log** and **don't log** the attacker's IP address.

Rule

With a mouse click on the link you have the choice between **add** and **don't add** the rule to block the TCP port scan attack.

UDP Port Scan

With this rule, you can define when a UDP port scan is assumed by the FireWall and what should be done in this case. This rule prevents so-called UDP port scan attacks that result in a detection of open UDP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the UDP Port Scan

Setting	Rules
Low	Assume a UDP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected,**log** attacker's IP and **don't add** rule to block the attack.
Medium	Assume a UDP Port Scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.
High	Same rule as for Medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a UDP Port Scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a UDP Port Scan is assumed.

Event database

With a mouse click on the link you have the choice between **log** and **don't log** the attacker's IP address.

Rule

With a mouse click on the link you have the choice between **add** and **don't add** the rule to block the UDP port scan attack.

Incoming Rules

Incoming rules are defined to control incoming data traffic by the Avira FireWall.

> **Warning**
> When a packet is filtered, the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Predefined rules for the TCP traffic monitor

Setting	Rules
Low	No incoming data traffic is blocked by the Avira FireWall.
Medium	**Allow Established TCP Connections on 135** **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{135}** and remote port is in **{0-65535}**. Apply for **packets of existing connections**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. **Deny TCP packets on 135** **Deny** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{135}** and remote port is in **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. **TCP healthy traffic Monitor** **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and remote port is in **{0-65535}**. Apply for **connection initiation and existing connection packets**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. **Discard TCP traffic** **Deny** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and remote port is in **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.
High	**Monitor established TCP traffic** **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and remote port is in **{0-65535}**. Apply for **packets of existing connections**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

Allow/ Deny TCP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming TCP packets.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply the rule for "**connection initiation and existing connection packets**" or only for "**packets of existing connections**" or for "**all packets**".

Event database

By clicking on the link with the mouse you can choose between "**Log**" and "**Don't log**" to the event database, if the packet complies with the rule.

Advanced

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option, do not select a file or choose an empty file.

Filtered content: bytes

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where TCP header ends.

Predefined rules for the UDP data traffic monitor

Setting	Rules
Low	-
Medium	**UDP accepted traffic monitor** **Allow** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0- 66535}** and remote port is in **{0-66535}**. Apply rule to **open ports** for **all streams**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. **Discard UDP traffic** **Deny** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and the remote port is in **{0-65535}**. Apply rule for **all ports** for **all streams**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.
High	**Monitor established UDP traffic** **Allow** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if the local port is in **{0-65535}** and the remote port is in **{53, 67, 68, 123}.** Apply rule to **open ports** for **all streams**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

Allow/ Deny UDP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming UDP packets.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

Ports

With a mouse click on this link you have the choice to apply this rule to all ports or only to all opened ports.

Streams

With a mouse click on this link you have the choice to apply this rule for all streams or only for outbound streams.

Event database

By clicking on the link with the mouse you can choose between "**Log**" and "**Don't log**" to the event database, if the packet complies with the rule.

Advanced

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: bytes

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where UDP header ends.

Predefined rules for the ICMP traffic monitor

Setting	Rules
Low	-
Medium	**Do not discard ICMP based on IP address** **Allow** ICMP packets from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.
High	Same rule as for medium level.

Allow/ Deny ICMP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming ICMP packets.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 mask.

Event database

By clicking on the link with the mouse you can choose between "**Log**" and "**Don't log**" to the event database, if the packet complies with the rule.

Advanced

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: bytes

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where ICMP header ends.

Predefined rules for IP packets

Setting	Rules
Low	-
Medium	-
High	**Deny all IP packets** **Deny IPv4** packets from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule.

Allow/ Deny

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IPv4/IPv6

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Event database

By clicking on the link with the mouse you can decide whether to write to the event database or not if the packet complies with the rule.

Outgoing Rules

Outgoing rules are defined to control outgoing data traffic by the Avira FireWall. You can define an outgoing rule for one of the following protocols: IP, ICMP, UDP, TCP. See Add new rule.

Warning
When a packet is filtered, the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Buttons to manage the rules

Button	Description
Add rule	Allows you to create a new rule. If you press this button, the **Add new rule** dialog box is opened. In this dialog box you can select new rules.
Remove rule	Removes the selected rule.
Rule up	Moves the selected rule up one line, i.e. increases the rule priority.
Rule down	Moves the selected rule down one line, i.e. reduces the rule priority.
Rename rule	Allows you to give the selected rule another name.

Note
You can add new rules for individual adapters or for all adapters present on the computer. To add an adapter rule for all adapters, select **My Computer** from the adapter hierarchy that is displayed and click on the **Add rule** button. See Add new rule.

Note
To change the position of a rule you can also use the mouse to drag the rule to the required position.

Add new rule

In this window you can select new incoming and outgoing rules. The selected rule is included with default information in the **Adapter rules** window and can be defined in more detail in this location. More rules are available, in addition to incoming and outgoing rules.

Possible rules

Allow Peer-To-Peer network

Allows peer-to-peer connections: Incoming TCP communications on Port 4662 and incoming UDP communications on Port 4672

TCP port

With a mouse click on the link a dialog box appears in which you can enter the permitted TCP port.

UDP port

With a mouse click on the link a dialog box appears in which you can enter the permitted UDP port.

Allow VMWARE connections

Allows communication between VMWare systems

Block IP

Blocks all traffic from a specified IP address

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog window opens in which you can enter the required IP address.

Block subnet

Blocks all traffic from a specified IP address and subnet mask

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog window opens in which you can enter the required IP address.

Subnet mask

By clicking on the link with the mouse, a dialog window opens in which you can enter the required subnet mask.

Allow IP

Allows all traffic from a specified IP address

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog window opens in which you can enter the required IP address.

Allow subnet

Allows all traffic from a specified IP address and subnet mask

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog window opens in which you can enter the required IP address.

Subnet mask

By clicking on the link with the mouse, a dialog window opens in which you can enter the required subnet mask.

Allow Web server

Allows communication from a web server on Port 80: Incoming TCP communication on Port 80

Port

With a mouse click on the link a dialog box appears in which you can enter the port used by the web server.

Allow VPN connections

Allows VPN (Virtual Private Network) connections with a specified IP: Incoming UDP data traffic on x ports, incoming TCP data traffic on x ports, incoming IP data traffic with the protocols ESP(50), GRE(47)

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog window opens in which you can enter the required IP address.

Allow Remote Desktop connection

Allows "Remote Desktop" connections (Remote Desktop Protocol) on Port 3389

Port

With a mouse click on the link a dialog box is displayed where you can enter the port to be used for the permitted remote desktop connection.

Allow VNC connection

Allows VNC (Virtual Network Computing) connections on Port 5900

Port

With a mouse click on the link a dialog box is displayed where you can enter the port to be used for the permitted remote desktop connection.

Allow File and Printer sharing.

Allows access to printer and file approvals: Incoming TCP data traffic on Ports 137, 139 and incoming UDP data traffic on Port 445 from a specified IP address.

Possible incoming rules

- **Incoming IP rule**
- **Incoming ICMP rules**
- **Incoming UDP rules**
- **Incoming TCP rules**
- **Incoming IP Protocol rule**

Possible outgoing rules

- **Outgoing IP rule**
- **Outgoing ICMP rules**
- **Outgoing UDP rules**
- **Outgoing TCP rules**
- **Outgoing IP Protocol rule**

> Note
> The syntax for the possible incoming and outgoing rules is identical with the one for the predefined rules of the relevant protocols, described under FireWall > Adapter rules.

Buttons

Button	Description
OK	The highlighted rule is included as a new adapter rule.
Cancel	The window is closed without adding a new rule.

Application rules

Application rules for user

This list contains all users in the system. If you are logged in as an administrator, you can select the user to whom you want to apply the rules. If you are not a privileged user, you can see only the user currently logged on.

Application

This table shows the list of applications for which rules are defined. The application list contains the settings of each application that was executed and had a rule saved since the Avira FireWall was installed.

Normal view

Column	Description
Application	Name of the application.
Active Connections	Number of active connections opened by the application.
Action	Shows the action that the Avira FireWall will automatically take when the application is using the network, whatever the network usage type is. With a mouse click on the link you can switch to another action type. The action types are **Ask**, **Allow** or **Deny**. **Ask** is the default action.

Advanced configuration

If the network accesses of an application require individual rules, you can create the application rules based on packet filters in the same way as you created the adapter rules.

- Go to **Configuration > Internet Protection > FireWall > Settings** and enable the **Advanced settings** option under *Application rules*.
- Save the setting by clicking **Apply** or **OK**.
  - ↳ Under **Configuration > Internet Protection > FireWall > Application rules** section, an additional column with the heading **Filtering** is displayed in the list of application rules, with the entry **Basic** for each application.

Column	Description
Application	Name of the application.
Active Connections	Number of active connections opened by the application.
Action	Shows the action that the Avira FireWall will automatically take when the application is using the network, whatever the network usage type is. If you choose **Basic** in the **Filtering** column, you can click the link to select another action type. The values are **Ask**, **Allow** or **Deny**. If you choose **Advanced** in the **Filtering** column, the **Rules** action type is displayed. The **Rules** link opens the **Advanced application rules** window, in which you can enter specific rules for the application.
Filtering	Shows the type of filtering. You can select another type of filtering by clicking the link. **Basic**: In the case of simple filtering, the specified action is carried out on all network activities performed by the software application. **Advanced**: With this type of filtering, the rules that were added to the extended configuration are applied.

- If you want to create specific rules for an application, select the **Advanced** entry under **Filtering**.
  - ↳ The **Rules** entry is then displayed in the **Action** column.
- Click on **Rules** to open the window for creating specific application rules.

Specified application rules in the advanced configuration

Using the specified application rules, you can allow or deny specified data traffic for the application or you can allow or deny passive listening to individual ports. The following options are available:

Allow / Deny Code injection

Code injection is a technique for introducing code into the address space of another process to execute actions, forcing this process to load a dynamic link library (DLL). Code injection is used by malware, amongst other things, to execute code under cover of another program. In this way, access to the Internet in front of the Avira FireWall can be hidden. In default mode, code injection is enabled for all signed applications.

Allow / Deny passive listening to the application of ports

Allow / Deny Traffic

Allow or deny incoming and/or outgoing IP packets

Allow or deny incoming and/or outgoing TCP packets

Allow or deny incoming and/or outgoing UDP packets

You can create as many application rules as you like for each application. The application rules are executed in the sequence shown (You will find more information under Advanced application rules).

> **Note**
> If you switch from **Advanced** to **Basic** filtering of an application rule, the already existing application rules in the advanced configuration are simply deactivated, not irretrievably deleted. When you select **Advanced** filtering again, the existing advanced application rules will be reactivated and displayed in the **Application rules** configuration window.

Application details

In this box you can see details of the application selected in the application list box.

- *Name* - Name of the application.
- *Path* - Full path to the executable file.

Buttons

Button	Description
Add application	Allows you to create a new application rule. If you press this button, a dialog box is opened. Here you can select the required application for creating a new rule.
Remove rule	Removes the selected application rule.
Show details	The window "**Show details"** displays the details of the application selected in the application list box.
Reload	Reloads the list of applications and simultaneously discards the changes just made.

Advanced application rules

The **Advanced application rules** window allows you to create specified rules for the data traffic of applications and for listening to ports. A new rule can be created with the **Add rule** button. You can further specify the rules in the lower part of the window. You can create as many rules as you like for an application. The rules are executed in the order displayed. You can use the **Rule up** and **Rule down** buttons to change the sequence of the rules.

> **Note**
> To change the position of an application rule you can also use the mouse to drag the rule to the required position.

Application details

Information about the selected application is displayed in the *Application details* area.

- *Name* - Name of the application.
- *Path* - Path to the executable file for the application.

Rule options

Deny/ Allow Code injection

By clicking on the link with the mouse, you can decide whether you want to allow or deny the code injection for the selected application.

Rule Type: Traffic/ Listen

By clicking on the link with the mouse, you can decide whether you want to create a rule for traffic monitoring or for listening to ports.

Deny/ Allow action

By clicking on the link with the mouse, you can decide which action is executed with the rule.

Port

With a mouse click on the link, a dialog box appears in which you can enter the local port to which the Listen rule applies. You can also enter several ports or port areas.

Outgoing, incoming, all packages

With a mouse click on this link, you can decide if the Traffic rule is to monitor just outgoing packets or just incoming packets.

IP packets / TCP packets / UDP packets

By clicking on the link with the mouse, you can decide which protocol monitors the Traffic rule.

IP packages options:

IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IP address.

IP mask

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IP mask.

TCP packages / UDP package options:

Local IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the local IP address.

Local IP mask

By clicking on the link with the mouse, a dialog box opens in which you can enter the required local IP mask.

Remote IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required remote IP address.

Remote IP mask

By clicking on the link with the mouse, a dialog box opens in which you can enter the required remote IP mask.

Local port

With a mouse click on the link a dialog box appears in which you can define the local ports or even complete port ranges.

Remote port

With a mouse click on the link a dialog box appears in which you can define one or more required remote ports or even complete port ranges.

Report file

With a mouse click on the link you have the choice between "**log**" and "**don't log**" to the program’s report file when a rule is fulfilled.

Buttons

Button	Description
Add rule	A new application rule is created.
Remove rule	The selected application rule is deleted.
Rule up	The selected rule is moved up one line, i.e. the rule priority is increased.
Rule down	The selected application rule is moved down one line, i.e. the rule priority is decreased.
Rename rule	The selected rule is edited so a new rule name can be entered.
Apply	The changes made are accepted and immediately applied by the Avira FireWall.
OK	The changes made are applied. The window for configuring the application rules is closed.
Cancel	The window for configuring the application rules is closed without applying the changes made.

Trusted vendors

A list of trusted software producers is displayed under **Trusted vendors**.

You can add / remove producers to / from the list using the **Always trust this provider** option in the **Network Event** popup window. You can allow network access from applications that are signed by the listed providers by default, by enabling the **Automatically allow applications created by trusted vendors** option.

Trusted vendors for user

This list contains all users in the system. If you are logged in as an administrator, you can select the user whose list of trusted vendors you want to view or update. If you are not a privileged user, you can see only the current user logged on.

Automatically allow applications created by trusted vendors

If this option is enabled, the application provided with the signature of a known and trusted provider is automatically permitted access to the network. The option is enabled as the default setting.

Vendors

The list shows all vendors classified as trusted.

Buttons

Button	Description
Remove	The highlighted entry is removed from the list of trusted vendors. To permanently remove the selected provider from the list, click **Apply** or **OK** in the configuration window.
Reload	The changes made are reversed. The last list saved is loaded.

> **Note**
> If you remove vendors from the list and then select **Apply** the vendors will be permanently removed from the list. The change cannot be reversed with **Reload**. However, you can use the **Always trust this vendor** option in the **Network Event** popup window to add a vendor to the list of trusted vendors again.

> **Note**
> The Avira FireWall prioritizes application rules before making entries in the list of trusted vendors: If you have created an application rule and the application provider is listed in the list of trusted vendors, the application rule will be executed.

Settings

Advanced options

Turn on FireWall

If the option is activated, the Avira FireWall is enabled and protects your computer from risks originating from the Internet and other networks.

Stop Windows Firewall on startup

If this option is enabled, the Windows Firewall is deactivated when the computer is rebooted. This option is enabled as the default setting.

Automatic rule timeout

Block forever

If this option is enabled, a rule that was automatically created, for example during a port scan, is retained.

Remove rule after n seconds

If this option is enabled, a rule that was automatically created, for example during a port scan, is removed again after the time you have defined. This option is enabled as the default setting. In the box you can specify the number of seconds after which the rules is to be removed.

Notifications

Notifications define the events under which you wish to receive a desktop notification from the Avira FireWall.

Port scan

If the option is activated, you will receive a desktop notification if a port scan has been detected by the Avira FireWall.

Flooding

If the option is activated, you will receive a desktop notification if a flooding attack has been detected by the Avira FireWall.

Applications blocked

If the option is activated, you will receive a desktop notification if the Avira FireWall has denied, i.e. blocked, network activity by an application.

IP blocked

If the option is activated, you will receive a desktop notification if the Avira FireWall has denied, i.e. blocked, data traffic from an IP address.

Application rules

The application rules options are used to set the configuration options for application rules in the FireWall > Application rules section.

Advanced settings

If this option is enabled, you can regulate different network accesses of an application on an individual basis.

Basic settings

If this option is enabled, only one action can be set for different network accesses of the application.

Popup settings

Inspect process launch stack

If this option is enabled, the process stack inspection allows a more accurate control. The Avira FireWall will assume that any of the untrustworthy processes in the stack may actually be the one accessing the network through its child process. Therefore a different popup window will be opened for each untrustworthy process in the process stack. This option is disabled as the default setting.

Allow multiple popups per process

If this option is enabled, every time an application is making a network connection, a popup is triggered. Alternatively you will be informed only on the first connection attempt. This option is disabled as the default setting.

Remember action for this application

Always enabled

When this option is enabled, the option "**Remember action for this application**" of the dialog box "**Network event**" is enabled as the default setting.

Always disabled

When this option is enabled, the option "**Remember action for this application**" of the dialog box "**Network event**" is disabled as the default setting.

Enabled for signed applications

When this option is enabled, the option "**Remember action for this application**" of the dialog box "**Network event**" is automatically enabled during network access by signed applications. Signed applications are distributed by so-called "trusted vendors" (see Trusted Vendors).

Remember last used state

When this option is enabled, the option "**Remember action for this application**" in the dialog box "**Network event**" is enabled in the same way as for the last network event. If the option "**Remember action for this application**" was enabled, this option is enabled for the following network event. If the option "**Remember action for this application**" was disabled for the last network event, this option is also disabled for the following network event.

Show details

In this group of configuration options, you can setup the display of detailed information in the **Network event** window.

Show details on demand

If this option is enabled, the detailed information is only displayed in the "**Network event**" window on request, i.e. the detailed information is displayed by clicking on the "**Show details**" button in the "**Network event**" window.

Always show details

If this option is enabled, detailed information is always displayed in the "**Network event**" window.

Remember last used state

If this option is enabled, the display of detailed information is managed in the same way as for the previous network event. If detailed information was displayed or accessed during the last network event, detailed information is displayed for the following network event. If detailed information was hidden and not displayed during the last network event, detailed information is not displayed for the following network event.

8.8.2 Avira FireWall under AMC

The FireWall is configured to meet the specific requirements of administration through the Avira Management Console. Extended options and restrictions exist for individual configuration options:

- The FireWall settings apply to all users of the client computer
- Adapter rules: Security levels for individual adapters can be set using context menus
- Application rules: Network access by applications can be allowed or denied. There is no way of creating specific application rules.

If your Avira product is managed by the Avira Management Console, the following FireWall setting options in the Control Center are deactivated on client computers:

- Setting of the FireWall security levels
- Setting of adapter and application rules

General settings

Advanced options

Enable FireWall

If the option is activated, the Avira FireWall is enabled and protects your computer from risks originating from the Internet and other networks.

Stop Windows FireWall on startup

If this option is enabled, the Windows FireWall is deactivated when the computer is rebooted. This option is enabled as the default setting.

Learn mode

If the option is activated, the learn mode of Avira FireWall is enabled.

Automatic rule timeout

Block forever

If this option is enabled, a rule that was automatically created, for example during a port scan, is retained.

Remove rule after n seconds

If this option is enabled, a rule that was automatically created, for example during a port scan, is removed again after the time you have defined. This option is enabled as the default setting.

Generic adapter rules

Network connections that have been set up are designated adapters. Adapter rules can be drawn up for the following Client network connections:

- **Default** adapter: LAN or high-speed Internet
- **Wireless**
- **Dial-up** connection

From the adapter's context menu (in the **Generic adapter rules** window, right-click **My Computer** or **Default, Wireless, Dial-up,** etc) you can specify predefined adapter rules for each available adapter:

- **Set security level Low**
- **Set security level Medium**
- **Set security level High**

You also have the option of modifying individual adapter rules to suit your own particular requirements.

> **Note**
> The default security level setting for all predefined rules of the Avira FireWall is **Medium**.

- ICMP protocol
- TCP Port Scan

- UDP Port Scan
- Incoming rules
- Incoming IP protocol rule
- Outgoing rules
- Buttons to manage the rules

ICMP protocol

The Internet Control Message Protocol (ICMP) is used to exchange error and information messages on networks. The protocol is also used for status messages with ping or tracer. With this rule, you can define the incoming and outgoing blocked message types, the behavior in case of flooding and the reaction to fragmented ICMP packets. This rule serves for preventing so-called ICMP flood attacks, which results in an increase of the CPU load of the attacked machine as it responds to every packet.

Predefined rules for the ICMP protocol

Setting	Rules
Low	Incoming blocked types: **no type**. Outgoing blocked types: **no type**. Assume flooding if delay between packets is less than **50** ms. **Reject** fragmented ICMP packets.
Medium	Same rule as for the low level.
High	Incoming blocked types: **several types** Outgoing blocked types: **several types** Assume flooding if delay between packets is less than **50** ms. **Reject** fragmented ICMP packets.

Incoming blocked types: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can specify the desired incoming ICMP message types you want to block.

Outgoing blocked types: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can select the desired outgoing ICMP message types you want to block.

Flooding

With a mouse click on the link, a dialog box is displayed where you can enter the maximum allowed ICMPA delay.

Fragmented ICMP packets

With a mouse click on the link, you have the choice to reject or not to reject fragmented ICMP packets.

TCP port scan

With this rule, you can define when a TCP port scan is assumed by the FireWall and what should be done in this case. This rule serves for preventing so-called TCP port scan attacks that result in a detection of open TCP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the TCP port scan

Setting	Rules
Low	Assume a TCP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **don't add** rule to block the attack.
Medium	Assume a TCP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.
High	Same rule as for medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a TCP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a TCP port scan is assumed.

Report file

With a mouse click on the link you have the choice to log or not to log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or not to add the rule to block the TCP port scan attack.

UDP port scan

With this rule, you can define when a UDP port scan is assumed by the FireWall and what should be done in this case. This rule prevents so-called UDP port scan attacks that result in a detection of open UDP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the UDP port scan

Setting	Rules
Low	Assume a UDP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **don't add** rule to block the attack.
Medium	Assume a UDP port scan if **50** or more ports were scanned in **5,000** milliseconds. When detected, **log** attacker's IP and **add** rule to block the attack.
High	Same rule as for medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a UDP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of port scans, so that a UDP port scan is assumed.

Report file

With a mouse click on the link you have the choice to log or not to log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or not to add the rule to block the UDP port scan attack.

Incoming Rules

Incoming rules are defined to control incoming data traffic by the Avira FireWall.

> **Warning**
> When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Predefined rules for the TCP traffic monitor

Setting	Rules
Low	No incoming data traffic is blocked by the Avira FireWall.
Medium	• Allow established TCP connections on 135 **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{135}** and remote port is in **{0-65535}**. Apply for **packets of existing connections**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0** • Deny TCP packets on 135 **Deny** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local ports is in **{135}** and remote port is in **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. • TCP healthy traffic Monitor **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and remote port is in **{0-65535}**. Apply for **connection initiation and existing connection packets**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. • Discard TCP traffic **Deny** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and remote port is in **{0-65535}**. Apply for **all packets**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

High	Monitor established TCP traffic **Allow** TCP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-65535}** and remote port is in **{0-65535}**. Apply for **packets of existing connections**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

Accept / reject TCP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming TCP packets.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply the rule for connection initiation and existing connection packets or only for packets of existing connections or for all packets.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where TCP header ends.

Predefined rules for the UDP traffic data monitor

Setting	Rules
Low	-
Medium	• UDP accepted traffic monitor **Allow** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in **{0-66535}** and remote port is in **{0-66535}**. Apply rule to **open ports** for **all streams**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**. • Discard UDP traffic **Deny** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if local port is in {**0-65535}** and the remote port is in **{0-65535}**. Apply rule for **all ports** for **all streams**. **Don't log** when packet matches rule. Advanced: Select packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

High	Monitor established UDP traffic **Allow** UDP packets from address **0.0.0.0** with mask **0.0.0.0** if the local port is in **{0-65535}** and the remote port is in **{53, 67, 68, 123}**. Apply rule to **open ports** for **all streams**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.

Accept / reject UDP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming UDP packets.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply this rule to all ports or only to all opened ports.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where UDP header ends.

Predefined rules for the ICMP traffic data monitor

Setting	Rules
Low	-
Medium	Do not discard ICMP based on IP address **Allow** ICMP packets from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule. Advanced: Discard packets that have following bytes **<empty>** with mask **<empty>** at offset **0**.
High	Same rule as for medium level.

Accept / reject ICMP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming ICMP packets.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

The **advanced feature** enables content filtering. For example packets can be rejected if they contain some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content: Data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content: Mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content: Offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where ICMP header ends.

Predefined rules for IP packets

Setting	Rules
Low	-
Medium	-
High	Deny all IP packets **Deny IP** packets from address **0.0.0.0** with mask **0.0.0.0**. **Don't log** when packet matches rule.

Accept / deny IP packets

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

Incoming IP Protocol rule

IP packages

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

IP mask

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 mask.

Protocol

By clicking on this link with the mouse, a dialog box opens in which you can enter the required IP protocol.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

Outgoing Rules

Outgoing rules are defined to control outgoing data traffic by the Avira FireWall. You can define an outgoing rule for one of the following protocols: IP, ICMP, UDP and TCP. See Add new rule.

> **Warning**
> When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only if you are completely aware of what you are doing.

Buttons to manage the rules

Button	Description
Add rule	Allows you to create a new rule. If you press this button, the "**Add new rule**" dialog box is opened. In this dialog box you can select new rules.
Remove rule	Removes the selected rule.
Rule up	Moves the selected rule up one line, i.e. increases the rule priority.
Rule down	Moves the selected rule down one line, i.e. reduces the rule priority.
Rename rule	Allows you to give the selected rule another name.

Note
You can add new rules for individual adapters or for all adapters present on the computer. To add an adapter rule for all adapters, select **My Computer** from the adapter hierarchy that is displayed and click on the **Add rule** button. See Add new rule.

Note
To change the position of a rule you can also use the mouse to drag the rule to the required position.

Application list

You can use the application list to create rules specifying how applications access networks. You can add applications to lists and set the **Allow** and **Deny** rules for the selected application using a context menu:

- Access to networks by applications with the **Allow** rule is permitted.
- Access to networks by applications with the **Deny** rule is denied.

When applications are added, the **Allow** rule is set.

Application list

This table shows the list of applications for which rules are defined. The symbols indicate whether network access by the applications is allowed or denied. The rules for the applications can be changed using a context menu.

Buttons

Button	Description
Add by path	This button opens a dialog box in which you can select applications. The application is added to the application list with the rule "**Allow**". If you use the option "**Add by path**" the added FireWall application are identified by path and file name.
Add by md5	This button opens a dialog box in which you can select applications. The application is added to the application list with the rule "**Allow**". If you use the option "**Add by md5**" all added applications are uniquely identified using the MD5 checksum. This allows the FireWall to identify changes to the file content. If an application changes following an update, for example, the application with the rule in question is automatically removed from the application list. Following a change, the application must be added to the list again and the desired rule reapplied.
Add group	This button opens a dialog box in which you can select a directory. All applications in the selected path are added to the application list with the rule "**Allow**".
Remove	The selected application rule is removed.
Remove all	All application rules are removed.

Trusted vendors

A list of trusted software producers is displayed under **Trusted vendors**. Applications from the listed software manufacturers will be granted access to the network. You can add and remove manufacturers from the list.

Vendors

The list shows all vendors classified as trusted.

Buttons

Button	Description
Add	This button opens a dialog box in which you can select applications. The manufacturer of the application is established and added to the list of trusted vendors.
Add group	This button opens a dialog box in which you can select a directory. The manufacturers of all the applications in the selected path are established and added to the list of trusted vendors.
Remove	The highlighted entry is removed from the list of trusted vendors. To permanently remove the selected provider from the list, click "**Apply**" or "**OK**" in the configuration window.
Remove all	All entries are removed from the list of trusted vendors.
Reload	The changes made are reversed. The last list saved is loaded.

Note
If you remove vendors from the list and then select **Apply** the vendors will be permanently removed from the list. The change cannot be reversed with **Reload**.

Note
The FireWall prioritizes application rules before making entries in the list of trusted vendors: If you have created an application rule and the application provider is listed in the list of trusted vendors, the application rule will be executed.

Further settings

Notifications

Notifications define the events under which you wish to receive a desktop notification from the FireWall.

Port scan

If the option is activated, you will receive a desktop notification if a port scan has been detected by the FireWall.

Flooding

If the option is activated, you will receive a desktop notification if a flooding attack has been detected by the FireWall.

Applications blocked

If the option is activated, you will receive a desktop notification if the FireWall has denied, i.e. blocked, network activity by an application.

IP blocked

If the option is activated, you will receive a desktop notification if the FireWall has denied, i.e. blocked, data traffic from an IP address.

Popup settings

Inspect process launch stack

If this option is enabled, the process stack inspection allows a more accurate control. The FireWall will assume that any of the untrustworthy processes in the stack may actually be the one accessing the network through its child process. Therefore a different popup window will be opened for each untrustworthy process in the process stack. This option is disabled as the default setting.

Allow multiple popups per process

If this option is enabled, every time an application is making a network connection, a popup is triggered. Alternatively you will be informed only on the first connection attempt. This option is disabled as the default setting.

Display settings

Remember the action for this application

Always enabled

When this option is enabled, the option "**Remember action for this application**" of the dialog box "**Network event**" is enabled as the default setting. This option is enabled as the default setting.

Always disabled

When this option is enabled, the option "**Remember action for this application**" of the dialog box "**Network event**" is disabled as the default setting.

Enabled for signed applications

When this option is enabled, the option "**Remember action for this application**" of the dialog box "**Network event**" is automatically enabled during network access by signed applications. The manufacturers are: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Remember last used state

When this option is enabled, the option "**Remember action for this application**" in the dialog box "**Network event**" is enabled in the same way as for the last network event. If the option "**Remember action for this application**" was enabled, this option is enabled for the following network event. If the option "**Remember action for this application**" was disabled for the last network event, this option is also disabled for the following network event.

Show details

In this group of configuration options, you can setup the display of detailed information in the **Network event** window.

Show details on demand

If this option is enabled, the detailed information is only displayed in the "**Network event**" window on request, i.e. the detailed information is displayed by clicking on the "**Show details**" button in the "**Network event**" window.

Always show details

If this option is enabled, detailed information is always displayed in the "**Network event**" window.

Remember last used state

If this option is enabled, the display of detailed information is managed in the same way as for the previous network event. If detailed information was displayed or accessed during the last network event, detailed information is displayed for the following network event. If detailed information was hidden and not displayed during the last network event, detailed information is not displayed for the following network event.

Add new rule

In this window you can select new incoming and outgoing rules. The selected rule is included with default information in the Adapter rules window and can be defined in more detail in this location. More rules are available, in addition to incoming and outgoing rules.

Possible rules

Allow Peer-To-Peer network

Allows peer-to-peer connections: Incoming TCP communications on Port 4662 and incoming UDP communications on Port 4672.

TCP port

With a mouse click on the link a dialog box appears in which you can enter the permitted TCP port.

UDP port

With a mouse click on the link a dialog box appears in which you can enter the permitted UDP port.

Allow VMWARE connections

Allows communication between VMware systems.

Block IP

Blocks all traffic from a specified IP address.

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

Block subnet

Blocks all traffic from a specified IP address and subnet mask.

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

Subnet mask

By clicking on the link with the mouse, a dialog box opens in which you can enter the required subnet mask.

Allow IP

Allows all traffic from a specified IP address.

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

Allow subnet

Allows all traffic from a specified IP address and subnet mask.

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

Subnet mask

By clicking on the link with the mouse, a dialog box opens in which you can enter the required subnet mask.

Allow Web server

Allows communication from a web server on Port 80: Incoming TCP communication on Port 80.

Port

With a mouse click on the link a dialog box appears in which you can enter the port used by the web server.

Allow VPN connections

Allows VPN (Virtual Private Network) connections with a specified IP: Incoming UDP data traffic on x ports, incoming TCP data traffic on x ports, incoming IP data traffic with the protocols ESP(50), GRE(47)

Internet Protocol version

By clicking on the link with the mouse, you can choose IPv4 or IPv6.

IP address

By clicking on the link with the mouse, a dialog box opens in which you can enter the required IPv4 or IPv6 address.

Allow Remote Desktop connection

Allows "Remote-Desktop" connections (Remote Desktop Protocol) on Port 3389

Port

With a mouse click on the link a dialog box is displayed where you can enter the port to be used for the permitted remote desktop connection.

Allow VNC connection

Allows VNC (Virtual Network Computing) connections on Port 5900.

Port

With a mouse click on the link a dialog box is displayed where you can enter the port to be used for the permitted remote desktop connection.

Allow File and Printer sharing

Allows access to printer and file approvals: Incoming TCP data traffic on Ports 137, 139 and incoming UDP data traffic on Port 445 from a specified IP address.

Possible incoming rules

- Incoming IP rule
- Incoming ICMP rule
- Incoming UDP rule
- Incoming TCP rule
- Incoming IP Protocol rule

Possible outgoing rules

- Outgoing IP rule
- Outgoing ICMP rule
- Outgoing UDP rule
- Outgoing TCP rule
- Outgoing IP Protocol rule

Note
The options for the possible incoming and outgoing rules are identical with the options for the predefined rules of the relevant protocols (see FireWall > Adapter rules).

Buttons

Button	Description
OK	The highlighted rule is included as a new adapter rule.
Cancel	The window is closed without adding a new rule.

8.8.3 Windows Firewall

The **FireWall** section under **Configuration > Internet Protection** is responsible for configuration of the Windows Firewall, starting from Windows 7.

Windows Firewall

Enable Avira-managed Windows Firewall

If this option is enabled, Avira will manage the Windows Firewall.

Network profiles

Network profiles

Windows Firewall blocks the unathorized access of programs and apps to your computer based on three network location profiles:

- Private network: for home or office networks
- Public network: for public places' networks
- Domain network: for networks with a domain controller

You can manage these profiles from the configuration of your Avira product under **Internet protection > Windows Firewall > Network profiles**.

For further information about these network profiles, please visit the official Microsoft website.

> **Warning**
> Windows Firewall applies the same rules for all networks that belong to the same network location, this means that, if you allow to run a program or application, this program or application will also be granted access in all the networks that have the same profile.

Private network

Private network settings

The private network settings manage the access other computers or devices in your home or office network have to your computer. These settings allow by default the users of the private network to see and access your computer.

Enable

If this option is enabled, Windows Firewall is activated and working through the Avira product.

Block all incoming connections

If this option is enabled, Windows Firewall will reject all unsolicited attempts to connect to your computer, including incoming connections from allowed applications.

Notify me when a new app is blocked

If this option is enabled, you will receive a notification every time that Windows Firewall blocks a new program or app.

Disable (not recommended)

If this option is enabled, Windows Firewall is deactivated. This option is not recommended, it puts your computer at risk.

Public network

Public network settings

The public network settings manage the access other computers or devices in public places' networks have to your computer. These settings do not allow, by default, the users of the public network to see and access your computer.

Enable

If this option is enabled, Windows Firewall is activated and working through the Avira product.

Block all incoming connections

If this option is enabled, Windows Firewall will reject all unsolicited attempts to connect to your computer, including incoming connections from allowed applications.

Notify me when a new app is blocked

If this option is enabled, you will receive a notification every time that Windows Firewall blocks a new program or app.

Disable (not recommended)

If this option is enabled, Windows Firewall is deactivated. This option is not recommended, it puts your computer at risk.

Domain network

Domain network settings

The domain network settings manage the access other computers or devices have to your computer in a network that authenticates through a domain controller. These settings allow, by default, authenticated users of the domain to see and access your computer.

Enable

If this option is enabled, Windows Firewall is activated and working through the Avira product.

Block all incoming connections

If this option is enabled, Windows Firewall will reject all unsolicited attempts to connect to your computer, including incoming connections from allowed applications.

Notify me when a new app is blocked

If this option is enabled, you will receive a notification every time that Windows Firewall blocks a new program or app.

Disable (not recommended)

If this option is enabled, Windows Firewall is deactivated. This option is not recommended, it puts your computer at risk.

> **Note**
> This option is only available if your computer is connected to a network with a domain controller.

Application rules

If you click the link under **Windows Firewall > Application rules**, you will be redirected to the menu **Allowed apps and features** of the Windows Firewall configuration.

Advanced settings

If you click the link under **Windows Firewall > Advanced settings**, you will be redirected to the menu **Windows Firewall with Advanced Security** of the Windows Firewall configuration.

8.9 Web Protection

The **Web Protection** section under **Configuration > Internet Protection** is responsible for the configuration of the Web Protection.

8.9.1 Scan

Web Protection protects you against viruses or malware that reach your computer from web pages that you load on your web browser from the Internet. The **Scan** options can be used to set the behavior of the Web Protection component.

Scan

Enable Web Protection

If this option is enabled, the Web Protection feature is active.

Enable IPv6 support

If this option is enabled, Internet Protocol version 6 is supported by the Web Protection. This option is not available for new or changed installations under Windows 8.

Drive-by protection

Drive-by protection allows you to make settings to block I-Frames, also known as inline frames. I-Frames are HTML elements, i.e. elements of Internet pages that delimit an area of a web page. I-Frames can be used to load and display different web content - usually other URLs - as independent documents in a sub-window of the browser. I-Frames are mostly used for banner advertising. In some cases, I-Frames are used to conceal malware. In these cases the area of the I-Frame is mostly invisible or almost invisible in the browser. The **Block suspicious I-frames** option allows you to check and block the loading of I-Frames.

Block suspicious I-frames

If this option is enabled, I-Frames on the web pages you request are scanned according to certain criteria. If there are suspect I-Frames on a requested web page, the I-Frame is blocked. An error message is displayed in the I-Frame window.

Action on detection

You can define the actions to be performed by Web Protection when a virus or unwanted program is detected.

Interactive

If this option is enabled, a dialog box appears when a virus or unwanted program is detected during an on-demand scan, in which you can choose what is to be done with the affected file. This option is enabled as the default setting.

Show progress bar

If this option is enabled, a desktop notification appears with a download progress bar if a download of website content exceeds a 20 second timeout. This desktop notification is designed in particular for downloading websites with larger data volumes: If you are surfing with Web Protection, website contents are not downloaded incrementally in the Internet browser, as they are scanned for viruses and malware before being displayed in the Internet browser. This option is disabled as the default setting.

Permitted actions

In this box actions can be specified, which can be selected to be displayed in case of a virus detection. You must activate the corresponding options for this.

Deny access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. Web Protection logs the detection to the report file if the report function is activated.

Move to quarantine

In the event of a virus or malware being detected, the website requested from the web server and/or the transferred data and files are moved into quarantine. The affected file can be recovered from the quarantine manager if it has any informative value or - if necessary - sent to the Avira Malware Research Center.

Ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by Web Protection to your web browser.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that is to be activated by default and click on the "Default" button.

Click here for more information.

Automatic

If this option is enabled, no dialog box in case of a virus detection appears. Web Protection reacts according to the settings you predefine in this section as primary and secondary action.

Display detection alerts

If this option is activated, then for each detection of a virus or unwanted program an alert appears showing the actions being executed.

Primary action

The primary action is the action performed when Web Protection finds a virus or an unwanted program.

Deny access

The website requested from the web server and/ or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. Web Protection logs the detection to the report file if the report function is activated.

Move to quarantine

In the event of a virus or malware being detected, the website requested from the web server and/ or the transferred data and files are moved into quarantine. The affected file can be recovered from the quarantine manager if it has any informative value or - if necessary - sent to the Avira Malware Research Center.

Ignore

The website requested from the web server and/ or the data and files that were transferred are forwarded on by Web Protection to your web browser. Access to the file is permitted and the file is ignored.

> **Warning**
> The affected file remains active on your workstation! It may cause serious damage on your workstation!

Blocked requests

In **Blocked requests** you can specify the file types and MIME types (content types for the transferred data) to be blocked by Web Protection. The Web filter lets you block known phishing and malware URLs. Web Protection prevents the transfer of data from the Internet to your computer system.

Web Protection blocks the following file types / MIME-Types

All file types and MIME types (content types for the transferred data) in the list are blocked by Web Protection.

Input box

In this box, enter the names of the MIME types and file types you want Web Protection to block. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.

> **Note**
> Files which are already stored on your system as temporary Internet files and blocked by Web Protection can, however, be downloaded locally from the Internet by your computer's Internet browser. Temporary Internet files are files saved on your computer by the Internet browser so that websites can be accessed more quickly.

> **Note**
> The list of blocked file and MIME types is ignored if they are entered in the list of excluded file and MIME types under Web Protection > Scan > Exceptions.

Note
No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples of excluded file and MIME types

- `application/octet-stream` = application/octet-stream MIME type files (executable files *.bin, *.exe, *.com, *dll, *.class) are blocked by Web Protection.
- `application/olescript` = application/olescript MIME type files (ActiveX script-files *.axs) are blocked by Web Protection.
- `.exe` = All files with the extension .exe (executable files) are blocked by Web Protection.
- `.msi` = All files with the extension .msi (Windows Installer files) are blocked by Web Protection.

Add

The button allows you to copy MIME and file types from the input field into the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Web filter

The web filter is based on an internal database, updated daily, that classifies URLs according to content.

Activate web filter

When the option is enabled, all URLs matching the selected categories in the web filter list are blocked.

Web filter list

In the web filter list you can select the content categories whose URLs are to be blocked by Web Protection.

Note
The web filter is ignored for entries in the list of excluded URLs under Web Protection > Scan > Exceptions.

Note
Spam URLs are URLs sent with spam emails. The **Fraud / Deception** category covers web pages with “Subscription Expires” and other offers of services whose costs are hidden by the provider.

Exceptions

These options allow you to set exceptions based on MIME types (content types for the transferred data) and file types for URLs (Internet addresses) for scanning by Web Protection. The MIME types and URLs specified are ignored by Web Protection, i.e. that data is not scanned for viruses and malware when it is transferred to your computer system.

MIME types skipped by Web Protection

In this field you can select the MIME types (content types for the transferred data) to be ignored by Web Protection during scanning.

File types/MIME types skipped by Web Protection (user-defined)

All MIME types (content types for the transferred data) in the list are ignored by Web Protection during scanning.

Input box

In this box you can input the name of the MIME types and file types to be ignored by Web Protection during scanning. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.

Note
No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

Warning
All file types and content types on the exclusion list are downloaded into the Internet browser without further scanning of the blocked requests (list of file and MIME types to be blocked in Web Protection > Scan > Blocked requests) or by

Web Protection: For all entries on the exclusion list, the entries on the list of file and MIME types to be blocked are ignored. No scan for viruses and malware is performed.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples of excluded file and MIME types:

- `audio/` = All audio media type files are excluded from Web Protection scans
- `video/quicktime` = All Quicktime sub-type video files (*.qt, *.mov) are excluded from Web Protection scans
- `.pdf` = All Adobe PDF files are excluded from Web Protection scans.

Add

The button allows you to copy MIME and file types from the input field into the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

URLs skipped by Web Protection

All URLs in this list are excluded from Web Protection scans.

Input box

In this box you can input URLs (Internet addresses) to be excluded from Web Protection scans, e.g. `www.domainname.com`. You can specify parts of the URL, using leading or following dots to indicate the domain level: `.domainname.com` for all pages and all subdomains of the domain. Indicate websites with any top-level domain (`.com` or `.net`) with a following dot: `domainname.`. If you indicate a string without a leading or concluding dot, the string is interpreted as a top-level domain, e.g. `net` for all NET domains (`www.domain.net`).

Note
You can also use the wildcard * for any number of characters when specifying URLs. You can also use leading or following dots in combination with wildcards to indicate the domain level:

.domainname.*
*.domainname.com
.*name*.com (valid but not recommended)
Specifications without dots, like *name*, are interpreted as part of a top-level domain and are not advisable.

Warning
All websites on the list of excluded URLs are downloaded into the Internet browser without further scanning by the web filter or by Web Protection: For all entries in the list of excluded URLs, the entries in the web filter (see Web Protection > Scan > Blocked requests) are ignored. No scan for viruses and malware is performed. Only trusted URLs should therefore be excluded from Web Protection scans.

Add

The button allows you to copy the URL entered in the input field (Internet address) to the viewer window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Examples: Skipped URLs

- `www.avira.com` -OR- `www.avira.com/*`
  = All URLs with the domain `www.avira.com` are excluded from Web Protection scans: *www.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*, etc.
  URLs with the domain `www.avira.de` are not excluded from Web Protection scans.
- `avira.com` -OR- `*.avira.com`
  = All URLs with the second and top-level domain `avira.com` are excluded from Web Protection scans: The specification implies all existing subdomains for `.avira.com`: *www.avira.com*, *forum.avira.com*, etc.
- `avira.` -OR- `*.avira.*`
  = All URLs with the second-level domain `avira` are excluded from Web Protection scans: The specification implies all existing top-level domains or subdomains for `.avira`: *www.avira.com*, *www.avira.de*, *forum.avira.com*, etc.
- `.*domain*.*`
  All URLs containing a second-level domain with the string `domain` are excluded from Web Protection scans: *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -OR- `*.net`
  = All URLs with the top-level domain `net` are excluded from Web Protection scans: *www.name1.net*, *www.name2.net*, etc.

Warning
Enter the URLs you want to exclude from the Web Protection scan as precisely as possible. Avoid specifying an entire top-level domain or parts of a second-level domain because there is a risk that Internet pages that distribute malware and undesirable programs will be excluded from the Web Protection scan through global specifications under exclusions. You are recommended to specify at least the complete second-level domain and the top-level domain: `domainname.com`

Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristic

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

8.9.2 Report

The Web Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then Web Protection does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, Web Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, Web Protection logs less important information to the report file as well.

Complete

If this option is enabled, Web Protection logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, old entries are then deleted until the indicated size has been reduced by 20%.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

Note
If you have not specified any report file restriction, older entries are automatically deleted when the report file reaches 100 MB. Entries are deleted until the size of the report file reaches 80 MB.

8.10 Mail Protection

The **Mail Protection** section of the Configuration is responsible for the configuration of the Mail Protection.

8.10.1 Scan

Use Mail Protection to scan incoming emails for viruses and malware. Outgoing emails can be scanned for viruses and malware by Mail Protection. Outgoing emails which are spam sent from an unknown bot on your computer can be blocked by Mail Protection to prevent spam.

Enable Mail Protection

If this option is enabled, email traffic is monitored by Mail Protection. Mail Protection is a proxy server which checks data traffic between the email server you use and the email client program on your computer system: incoming emails are scanned for malware by default. If this option is disabled, the Mail Protection service is still started, but monitoring by Mail Protection is disabled.

Scan incoming emails

If this option is enabled, incoming emails are scanned for viruses and malware. Mail Protection supports POP3 and IMAP protocols. Enable the inbox account used by your email client to receive emails for monitoring by Mail Protection.

Monitor POP3 accounts

If this option is enabled, the POP3 accounts are monitored on the specified ports.

Monitored ports

In this field you should enter the port to be used as the inbox by the POP3 protocol. Multiple ports are separated by commas.

Default

This button resets the specified port to the default POP3 port.

Monitor IMAP accounts

If this option is enabled, the IMAP accounts are monitored on the specified ports.

Monitored ports

In this field you should enter the port to be used as the inbox by the IMAP protocol. Multiple ports are separated by commas.

Default

This button resets the specified port to the default IMAP port.

Scan outgoing emails (SMTP)

If this option is enabled, outgoing emails are scanned for viruses and malware. Emails which are spam sent by unknown bots are blocked.

Monitored ports

In this field you should enter the port to be used as the outbox by the SMTP protocol. Multiple ports are separated by commas.

Default

This button resets the specified port to the default SMTP port.

> Note
> To verify the protocols and ports used, call up the properties of your email accounts in your email client program. Default ports are mostly used.

Enable IPv6 support

If this option is enabled, Internet Protocol version 6 is supported by the Mail Protection. (Option not available for new or changed installations under Windows 8.)

Action on detection

This configuration section contains settings for actions performed when Mail Protection finds a virus or unwanted program in an email or in an attachment.

> Note
> These actions are performed both when a virus is detected in incoming emails and when a virus is detected in outgoing emails.

Interactive

If this option is enabled, a dialog box appears when a virus or unwanted program is detected in an email or attachment in which you can choose what is to be done with the email or attachment concerned. This option is enabled as the default setting.

Show progress bar

If this option is enabled, the Mail Protection shows a progress bar during downloading of emails. This option can only be enabled if the option "**Interactive**" has been selected.

Permitted actions

In this box actions can be specified, which can be selected to be displayed in case of a virus detection. You must activate the corresponding options for this.

Move to quarantine

When this option has been activated, the email including all attachments is moved to quarantine. It can be later be delivered via the quarantine manager. The affected email is deleted. The body of the text and any attachments of the email are replaced by a default text.

Delete mail

If this option is enabled, the affected email is deleted when a virus or unwanted program is detected. The body of the text and any attachments of the email are replaced by a default text.

Delete attachment

If this option has been activated, the affected attachment is replaced by a default text. If the body of the email is affected, it will be erased and also replaced by a default text. The email itself is delivered.

Move attachment to quarantine

If this option has been activated, the affected attachment is moved to quarantine and then deleted (replaced by a default text). The body of the email is delivered. The affected attachment can later be delivered via the quarantine manager.

Ignore

If this option is enabled, an affected email is delivered despite detection of a virus or unwanted program.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that should be activated by default and click on the "**Default"** button.

Automatic

If this option is enabled, you are no longer notified when a virus or unwanted program is found. Mail Protection reacts according to the settings you define in this section.

Affected emails

The action chosen for "*Affected emails*" is performed when the Mail Protection finds a virus or an unwanted program in an email. If the option "**Ignore**" is selected, it is also possible, under "*Affected attachments*", to select the process for dealing with a virus or unwanted program detected in an attachment.

Delete

If this option is enabled, the affected email is automatically deleted if a virus or unwanted program is found. The body of the email is replaced by the default text given below. The same applies to all attachments included; these are also replaced by a default text.

Ignore

If this option is enabled, the affected email is ignored despite detection of a virus or unwanted program. However, you can decide what is to be done with the affected attachment.

Move to quarantine

If this option is enabled, the complete email including all attachments is placed in Quarantine if a virus or unwanted program is found. If required, it can later be restored. The affected email itself is deleted. The body of the email is replaced by the default text given below. The same applies to all attachments included; these are also replaced by a default text.

Affected attachments

The option "*Affected attachments*" can only be selected if the setting "**Ignore**" has been selected under "*Affected emails*". With this option it is now possible to decide what is to be done if a virus or unwanted program is found in an attachment.

Delete

If this option is enabled, the affected attachment is deleted if a virus or unwanted program is found and replaced by a default text.

Ignore

If this option is enabled, the attachment is ignored despite detection of a virus or unwanted program and delivered.

Warning
If you select this option, you have no protection against viruses and unwanted programs by the Mail Protection. Only select this item if you are certain you know what you are doing. Disable the preview in your email program, never open attachments by double-clicking!

Move to quarantine

If this option is enabled, the affected attachment is placed in Quarantine and then deleted (replaced by a default text). If required, the affected attachment(s) can later be restored.

Further actions

This configuration section contains further settings for actions performed when Mail Protection finds a virus or unwanted program in an email or in an attachment.

Note
These actions are performed exclusively when a virus is detected in incoming emails.

Default text for deleted and moved emails

The text in this box is inserted in the email as a message instead of the affected email. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combination for formatting:

Ctrl + Enter = inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

Default text for deleted and moved attachments

The text in this box is inserted in the email as a message instead of the affected attachment. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combination for formatting:

Ctrl + Enter = inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristic

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

AntiBot

The AntiBot function of Mail Protection prevents your computer from becoming part of a so-called bot-net and being used to send out spam emails: To send spam via a bot-net, an attacker usually infects a number of computers with a bot that then connects to an IRC server, opens a particular channel and waits for the command to send the spam emails. To distinguish spam emails from an unknown bot from genuine emails, Mail Protection checks if the SMTP server and email sender for an outgoing email are included in the lists of permitted servers and senders. If this is not the case, the outgoing emails are blocked, i.e. the email is not sent. The blocked email is displayed in a dialog box.

> **Note**
> The AntiBot function can only be used, if the Mail Protection scan of outgoing emails is enabled (see the option **Scan outgoing emails** under Mail Protection > Scan).

Allowed Servers

All servers in this list are authorized by Mail Protection to send emails: Emails sent to these servers are **not** blocked by Mail Protection. If no servers are included in the list, the SMTP server used to send outgoing emails is not scanned. If the list is populated, Mail Protection blocks emails sent to any SMTP server not included in the list.

Input box

Enter the host name or IP address of the SMTP server you use to send your emails in this box.

> **Note**
> You can find details of the SMTP server used by your email program to send emails in your email program under the date the user account was created.

Add

You can use this button to include servers specified in the input box in the list of permitted servers.

Delete

This button deletes a highlighted entry from the list of permitted servers. This button is inactive if no entry is selected.

Clear all

This button deletes all entries from the list of permitted servers.

Allowed Sender(s)

All senders in this list are authorized by Mail Protection to send emails: Emails sent from this email address are **not** blocked by Mail Protection. If no senders are included in the list, the email address used to send outgoing emails is not scanned. If the list is populated, Mail Protection blocks emails from senders not included in the list.

Input box

Enter your email sender address(es) in this box.

Add

You can use this button to include senders specified in the input box in the list of permitted senders.

Delete

This button deletes a highlighted entry from the list of permitted senders. This button is inactive if no entry is selected.

Clear all

This button deletes all entries from the list of permitted senders.

8.10.2 General

Exceptions

Scanning exceptions

This table shows you the list of email addresses excluded from scanning by Mail Protection (white list).

> **Note**
> The list of exceptions is used exclusively by Mail Protection with regard to incoming emails.

Scanning exceptions

Input box

In this box you enter the email address that you want to add to the list of email addresses not to be scanned. Depending on your settings, the email address will no longer be scanned in future by the Mail Protection.

Add

With this button you can add the email address entered in the input box to the list of email addresses not to be scanned.

Delete

This button deletes a highlighted email address from the list.

Email address

Email that is no longer to be scanned.

Malware

When this option is enabled, the email address is no longer scanned for malware.

Up

You can use this button to move a highlighted email address to a higher position. If no entry is highlighted or the highlighted address is at the first position in the list, this button is not enabled.

Down

You can use this button to move a highlighted email address to a lower position. If no entry is highlighted or the highlighted address is at the last position in the list, this button is not enabled.

Cache

The Mail Protection cache contains data regarding the scanned emails that is displayed as statistical data in the Control Center under **Mail Protection**.

Maximum number of emails in the cache

This field is used to set the maximum number of emails that are stored by Mail Protection in the cache. Emails are deleted oldest first.

Maximum days for an email to be stored

The maximum storage period of an email in days is entered in this box. After this time, the email is removed from the cache.

Empty Cache

Click on this button to delete the emails stored in the cache.

Footer

Under **Footer** you can configure an email footer which is displayed in the emails you send.

This function requires activation of the Mail Protection scan of outgoing emails (see option **Scan outgoing emails (SMTP)** under **Configuration > Mail Protection > Scan**). You can use the defined Avira Mail Protection footer to confirm the sent email has been scanned by a virus protection program. You also have the option of inserting text yourself for a user-defined footer. If you use both footer options, the user-defined text is preceded by the Avira Mail Protection footer.

Footer for emails to be sent

Attach Mail Protection footer

If this option is enabled, the Avira Mail Protection footer is displayed beneath the message text of the sent email. The Avira Mail Protection footer confirms that the sent email has been scanned for viruses and unwanted programs by Avira Mail Protection and does not originate from an unknown bot. The Avira Mail Protection footer contains the following text: "*Scanned with Avira Mail Protection [product version] [initials and version number of search engine] [initials and version number of virus definition file]*".

Attach the following footer

If this option is enabled, the text which you insert into the input box is displayed as a footer in sent emails.

Input box

In this input box, you can insert a text which is displayed as a footer in sent emails.

8.10.3 Report

Mail Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then Mail Protection does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, Mail Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, Mail Protection logs less important information to the report file as well.

Complete

If this option is enabled, Mail Protection logs all information to the report file.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Backup report file before shortening

If this option is enabled, the report file is backed up before shortening. For the save location see Configuration > General > Directories > Report directory.

Write configuration in report file

If this option is enabled, the Mail Protection configuration is recorded in the report file.

> **Note**
> If you have not specified any report file restriction, a new report file is automatically created when the report file reaches 100 MB. A backup of the old report file is created. Up to three backups of old report files are saved. The oldest backups are deleted first.

8.11 General

8.11.1 Threat categories

Selection of extended threat categories

Your Avira product protects you against computer viruses. In addition, you can scan according to the following extended threat categories.

- Adware
- Adware/Spyware
- Applications
- Backdoor Clients
- Dialer
- Double Extension Files
- Fraudulent software
- Games
- Jokes
- Phishing
- Programs that violate the private domain
- Unusual runtime packers

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

Select all

If this option is enabled, all types are enabled.

Default values

This button restores the predefined default values.

> **Note**
> If a type is disabled, files recognized as being of the relevant program type are no longer indicated. No entry is made in the report file.

8.11.2 Advanced protection

ProActiv

Enable ProActiv

If this option is enabled, programs on your system are monitored and checked for suspicious actions. You will receive a message if typical malware behavior is detected. You can block the program or select "**Ignore**" to continue to use the program. The monitoring process excludes: Programs classified as trusted, trusted and signed programs included by default in the permitted applications filter, and all programs which you have added to the application filter for permitted programs.

ProActiv protects you from new and unknown threats for which there are not yet any virus definitions or heuristics available. ProActiv technology is integrated into the Real-Time Protection component and observes and analyzes the program actions performed. The behavior of the program is checked against typical malware action patterns: Type of action and action sequences. If a program exhibits typical malware behavior, this is treated as a virus detection: You have the option of blocking the program or ignoring the notification and continuing to use the program. You can classify the program as trusted and add it to the application filter for permitted programs. You have the option of adding the program to the application filter for blocked programs using the **Always block** command.

The ProActiv component uses rule sets developed by the Avira Malware Research Center to identify suspicious behavior. The rule sets are supplied by Avira databases. ProActiv sends information on any suspicious programs to the Avira databases for logging. During Avira installation, you have the option of disabling data transmission to the Avira databases.

> **Note**
> ProActiv technology is not yet available for 64 bit systems!

Protection Cloud

Enable Protection Cloud

Fingerprints of all suspicious files are sent to the Protection Cloud for dynamic online inspection. Executables are instantly identified as clean, infected or unknown.

The Protection Cloud serves as a central location to observe attempted cyber attacks throughout our user base. The files accessed by your computer are matched against the fingerprints of files stored in the cloud. As more scanning is done in the cloud, less processing power is required by the antivirus application.

A list of file locations frequently targeted by malware is generated when the **Quick system scan** job runs. The list includes running processes, programs that run at start-up and services. The fingerprint of each file is generated and sent to the Protection Cloud, which is then categorized as "clean" or "malware". Unknown program files are uploaded to the Protection Cloud for analysis.

Confirm manually when sending suspicious files to Avira

You can see a list of the suspicious files that should be sent to the Protection Cloud, and you can choose which files you want to send.

Real-time file scanning

If this option is enabled, unknown files are sent to the Protection Cloud for analysis as soon as they are accessed.

Show progress for uploads to the Avira Protection Cloud

A window displays the following information about the uploaded file(s) in form of a progress bar:

- file location

- file name

- status (uploading/analyzing)

- result (clean/infected)

Blocked applications

Under *Applications to be blocked* you can enter applications which you classify as harmful and which you want Avira ProActiv to block by default. The applications added cannot be executed on your computer system. You can also add programs to the application filter for blocking via Real-Time Protection notifications of suspicious program behavior, by selecting the **Always block this program** option.

Applications to be blocked

Application

The list contains all applications which you have classified as harmful which you have entered via the configuration or by notifying the ProActiv component. The applications on the list are blocked by Avira ProActiv and cannot be executed on your computer system. An operating system message appears when a blocked program starts up. The applications to be blocked are identified by Avira ProActiv on the basis of the path specified and the file name, and are blocked irrespective of their content.

Input box

Enter the application you want to block in this box. To identify the application, the full path, file name and file extension must be specified. The path must either show the drive on which the application is located or start with an environment variable.

The button opens a window in which you can select the application to be blocked.

Add

With the "**Add"** button you can transfer the application specified in the input box to the list of applications to be blocked.

> **Note**
> Applications required for the proper operation of the operating system cannot be added.

Delete

The "**Delete"** button lets you remove a highlighted application from the list of applications to be blocked.

Allowed applications

The section *Applications to be skipped* lists the applications excluded from monitoring by the ProActiv component: signed programs classified as trusted and included in list by default, all applications classified as trusted and added to the application filter: You can add permitted applications to the list in Configuration. You also have the option of adding applications to suspicious program behavior via Real-Time Protection notifications by using the **Trusted program** option in the Real-Time Protection notification.

Applications to be skipped

Application

The list contains applications excluded from monitoring by the ProActiv component. In the default installation settings, the list contains signed applications from trusted vendors. You have the option of adding applications that you consider to be trustworthy via the configuration or via Real-Time Protection notifications. The ProActiv component identifies applications using the path, the file name and the content. We recommend checking the content as malware can be added to a program through changes such as updates. You can determine whether a contents check should be performed from the **Type** specified: For the "*Contents*" type, the applications specified by path and file name are checked for changes to the file content before they are excluded from monitoring by the ProActiv component. If the file contents have been modified, the application is again monitored by the ProActiv component. For the "*Path*" type, no contents check is performed before the application is excluded from monitoring by the Real-Time Protection. To change the exclusion type, click on the type displayed.

> **Warning**
> Only use the *Path* type in exceptional cases. Malcode can be added to an application through an update. The originally harmless application is now malware.

> **Note**
> Some trusted applications, including for example all application components of your Avira product, are by default excluded from monitoring by the ProActiv component even though they are not included in the list.

Input box

In this box you enter the application to be excluded from monitoring by the ProActiv component. To identify the application, the full path, file name and file extension must be specified. The path must either show the drive on which the application is located or start with an environment variable.

...

The button opens a window in which you can select the application to be excluded.

Add

With the "**Add**" button you can transfer the application specified in the input box to the list of applications to be excluded.

Delete

The "**Delete**" button lets you remove a highlighted application from the list of applications to be excluded.

8.11.3 Password

You can protect your Avira product in different areas with a password. If a password has been issued, you will be asked for this password every time you want to open the protected area.

Password

Enter password

Enter your required password here. For security reasons, the actual characters you type in this space are replaced by asterisks (*). The password can only have a maximum of 20 chars. Once the password has been issued, the program refuses access if an incorrect password is entered. An empty box means "No password".

Confirmation

Confirm the password entered above by entering again here. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

> **Note**
> The password is case-sensitive!

Areas protected by password

Your Avira product can protect individual areas with a password. By clicking the relevant box, the password request can be disabled or re-enabled for individual areas as required.

Password-protected area	Function
Control Center	If this option is enabled, the pre-defined password is required to start the Control Center.
Activate / deactivate Real-Time Protection	If this option is enabled, the pre-defined password is required to enable or disable Avira Real-Time Protection.
Activate / deactivate Mail Protection	If this option is enabled, the pre-defined password is required to enable/disable Mail Protection.
Activate / deactivate FireWall	If this option is enabled, the pre-defined password is required to enable/disable the FireWall.
Activate / deactivate Web Protection	If this option is enabled, the pre-defined password is required to enable/disable Web Protection.
Quarantine	If this option is enabled, all areas of the quarantine manager protected by a password are enabled. By clicking on the relevant box, the password enquiry can be disabled or enabled again on request for individual areas.
Restore affected objects	If this option is enabled, the pre-defined password is required to restore an object.
Rescan affected objects	If this option is enabled, the pre-defined password is required to rescan an object.

Affected object properties	If this option is enabled, the pre-defined password is required to display the properties of an object.
Delete affected objects	If this option is enabled, the pre-defined password is required to delete an object.
Send email to Avira	If this option is enabled, the pre-defined password is required to send an object to the Avira Malware Research Center for examination.
Copying affected objects	If this option is enabled, the pre-defined password is required to copy the affected object.
Add and modify jobs	If this option is enabled, the pre-defined password is required to add and modify jobs in the Scheduler.
Download rescue CD from the Internet	If this option is enabled, the pre-defined password is required to start the Avira Rescue CD download.
Configuration	If this option is enabled, configuration of the program is only possible after entering the pre-defined password.
Manually switch configuration	If this option is enabled, the pre-defined password is required to manually switch to a different configuration profile .
Installation / uninstallation	If this option is enabled, the pre-defined password is required for installation or uninstallation of the program.

8.11.4 Security

Autorun

Block autorun function

If this option is enabled, the execution of the Windows autorun function is blocked on all connected drives, including USB sticks, CD and DVD drives and network drives. With the Windows autorun function, files on data media or network drives are read immediately on loading or connection, and files can therefore be started and copied automatically. This functionality carries with it a high security risk, however, as malware and unwanted programs can be installed with the automatic start. The autorun function is especially critical for USB sticks as data on a stick can be changed at any time.

Exclude CDs and DVDs

When this option is enabled, the autorun function is permitted on CD and DVD drives.

> **Warning**
> Only disable the autorun function for CD and DVD drives if you are sure you are only using trusted data media.

System protection

Protect Windows hosts files from changes

If this option is set to activated, the Windows hosts files are write-protected. Manipulation is no longer possible. For example, malware is not able to redirect you to undesired websites. This option is activated as the default setting.

Product protection

> **Note**
> The product protection options are not available if the Real-Time Protection has not been installed using the user-defined installation option.

Protect processes from unwanted termination

If this option is enabled, all processes of the program are protected against unwanted termination by viruses and malware or against 'uncontrolled' termination by a user, e.g. via Task-Manager. This option is enabled as the default setting.

Advanced process protection

If this option is enabled, all processes of the program are protected with advanced options against unwanted termination. Advanced process protection requires considerably more computer resources than simple process protection. The option is enabled as the default setting. To disable this option, you have to restart your computer.

Note
Process protection is not available for Windows XP 64 bit !

Warning
If process protection is enabled, interaction problems can occur with other software products. Disable process protection in these cases.

Protect files and registry entries from manipulation

If this option is enabled, all registry entries of the program and all program files (binary and configuration files) are protected from manipulation. Protection against manipulation entails preventing write, delete and, in some cases, read access to the registry entries or program files by users or external programs. To enable this option, you have to restart your computer.

Warning
Please note that, if this option is disabled, the repair of computers infected with specific types of malware may fail.

Note
When this option is activated, changes can only be made to the configuration, including changes to scan or update requests, by means of the user interface.

Note
Protection for files and registration entries is not available for Windows XP 64 bit !

8.11.5 WMI

Support for Windows Management Instrumentation

Windows Management Instrumentation is a basic Windows management technology that uses script and programming languages to allow read and write access, both local and remote, to settings on Windows systems. Your Avira product supports WMI and provides data (status information, statistical data, reports, planned requests, etc.) as well as events and methods (stopping and starting processes) via an interface. WMI gives you the option of downloading operating data from the program and controlling the program. You can request a complete reference guide to the WMI interface from the manufacturer. The reference file is available in PDF format when you sign a confidentiality agreement.

Enable WMI support

When this option is enabled, you can download operating data from the program via WMI.

Allow services to be enabled/disabled

When this option is enabled, you can enable and disable program services via WMI.

8.11.6 Events

Limit size of event database

Limit size to max. n entries

If this option is enabled, the maximum number of events listed in the event database can be limited to a certain size; possible values: 100 to 10000 entries. If the number of entered entries is exceeded, the oldest entries are deleted.

Delete all events older than n day(s)

If this option is enabled, events listed in the event database are deleted after a certain period of time; possible values: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

No limit

When this option has been activated, the size of the event database is not limited. However, a maximum of 20,000 entries are displayed in the program interface under Events.

8.11.7 Reports

Limit reports

Limit number to max. n piece

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

Delete all reports older than n day(s)

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

No limit

If this option is enabled, the number of reports is not restricted.

8.11.8 Directories

Temporary path

Use default system settings

If this option is enabled, the settings of the system are used for handling temporary files.

> **Note**
> You can see where your system saves temporary files - for example with Windows XP - under: **Start > Settings > Control Panel > System > Index card** "**Advanced**" Button "**Environment Variables**". The temporary variables (`TEMP`, `TMP`) for the currently registered user and for system variables (`TEMP`, `TMP`) are shown here with their relevant values.

Use following directory

If this option is enabled, the path displayed in the input box is used.

Input box

In this input box, enter the path where the program will store its temporary files.

...

The button opens a window in which you can select the required temporary path.

Default

The button restores the pre-defined directory for the temporary path.

Report directory

Input box

This input box contains the absolute path to the report directory.

...

The button opens a window in which you can select the required directory.

Default

The button restores the pre-defined path to the report directory.

Quarantine directory

Input box

This box contains the path to the quarantine directory.

...

The button opens a window in which you can select the required directory.

Default

The button restores the predefined path to the quarantine directory.

8.11.9 Acoustic alerts

When a virus or malware is detected by the System Scanner or Real-Time Protection, an acoustic alert is heard in interactive action mode. You can now choose to activate or deactivate the acoustic alert and select an alternative WAVE file for the alert.

> **Note**
> The action mode of the System Scanner is set in the configuration under System Scanner > Scan > Action on detection. The action mode of the Real-Time Protection is set in the configuration under Real-Time Protection > Scan > Action on detection.

No warning

When this option is enabled, there is no acoustic alert when a virus is detected by the System Scanner or Real-Time Protection.

Use PC speakers (only in interactive mode)

If this option is enabled, there is an acoustic alert with the default signal when a virus is detected by the System Scanner or Real-Time Protection. The acoustic alert is sounded on the PC's internal speaker.

Use the following WAVE file (only in interactive mode)

If this option is enabled, there is an acoustic alert with the selected WAVE file when a virus is detected by the System Scanner or Real-Time Protection. The selected WAVE file is played over a connected external speaker.

WAVE file

In this input box you can enter the name and the associated path of an audio file of your choice. The program's default acoustic signal is entered as standard.

...

The button opens a window in which you can select the required file with the aid of the file explorer.

Test

This button is used to test the selected WAVE file.

8.11.10 Alerts

Network

You can send individually configurable alerts from the System Scanner or from the Realtime Protection to any workstations in your network.

> **Note**
> Please check whether the "Message service" has been started. You will find the service (i.e. in Windows XP, for example) under **Start > Settings > System control > Administration > Services**.

> **Note**
> An alert is always sent to computers, **not** to a certain user.

> **Warning**
> This functionality is **no longer supported** by the following operating systems:
> Windows Server 2008 and higher
> Windows Vista and higher

Send message to

The list in this window shows names of computers that receive a message when a virus or unwanted program is found.

> **Note**
> A computer can always be entered only once in this list.

Insert

With this button you can add a further computer. A window is opened in which you can enter the names of new computers. A computer name can be a maximum of 15 characters long.

...

The button opens a window in which you can alternatively select a computer directly from your computer environment.

Delete

With this button you can delete the currently selected entry from the list.

Real-Time Protection network alerts

Network alerts

If this option is enabled, network alerts are sent. This option is disabled as the default setting.

> **Note**
> To be able to activate this option, at least one recipient must be entered under Configuration > General > Alerts > Network.

Message to be sent

The window shows the message sent to the selected workstation when a virus or unwanted program is detected. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combinations for formatting the message:

Shortcut	Description
Ctrl + Tab	Inserts a tab The current line is indented by several characters to the right.
Ctrl + Enter	Inserts a line break

The message can include wildcards for information found during the search. These wildcards are replaced by the actual text when sent.

The following wildcards can be used:

Wildcard	Description
`%VIRUS%`	Contains the name of the detected virus or of the unwanted program
`%FILE%`	Contains the path and file name of the affected file
`%COMPUTER%`	Contains the name of the computer on which the Real-Time Protection is running
`%NAME%`	Contains the name of the user who accessed the affected file

%ACTION%	Contains the action performed after the detection of the virus
%MACADDR%	Contains the MAC address of the computer on which the Real-Time Protection is running

Default

The button restores the predefined default text for an alert.

System Scanner network alerts

Enable network alerts

If this option is enabled, network alerts are sent. This option is disabled as the default setting.

> **Note**
> To be able to activate this option, at least one recipient must be entered under Configuration > General > Alerts > Network.

Message to be sent

The window shows the message sent to the selected workstation when a virus or unwanted program is detected. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combinations for formatting the message:

Shortcuts	Description
Ctrl + Tab	Inserts a tab The current line is indented by several characters to the right
Ctrl + Enter	Inserts a line break

The message can include wildcards for information found during the search. These wildcards are replaced by the actual text when sent.

The following wildcards can be used:

Wildcard	Description
`%VIRUS%`	Contains the name of the detected virus or of the unwanted program
`%NAME%`	Contains the name of the logged in user using the System Scanner
`%COMPUTER%`	Contains the name of the computer on which the System Scanner is running

Default

The button restores the predefined default text for an alert.

Email

The Avira product can send alerts and messages via email to one or more recipients with certain events. This is done with the Simple Message Transfer Protocol (SMTP).

The messages can be triggered by various events. The following components support email sending:

- Real-Time Protection email alerts
- System Scanner email alerts
- Updater email alerts

> **Note**
> Please note that ESMTP is not supported. In addition, an encrypted transfer via TLS (Transport Layer Security) or SSL (Secure Sockets Layer) is currently not possible.

Email messages

SMTP Server

Enter the name of the host to be used here - either its IP address or the direct host name.
The maximum possible length of the host name is 127 characters.

For example*:*

`192.168.1.100` or `mail.samplecompany.com.`

Port

Enter the port to be used here.

Sender address

In this input box, enter the email address of the sender. The maximum length of the sender's address is 127 characters.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an email is sent. Alerts can be transmitted with authentication to an SMTP server via email.

Use authentication

If this option is enabled, a user name and a password can be entered in the relevant boxes for login (authentication).

Login name:
Enter your user name here.

Password:
Enter the relevant password here. The password is saved in encrypted form. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

Send test email

When you click on the button, the program attempts to send a test email to the sender address to check the data entered.

Real-Time Protection email alerts

Avira Real-Time Protection can send alerts by email to one or more recipients for certain events.

Email alerts

If this option is enabled, Avira Real-Time Protection sends email messages with the most important information when a certain event occurs. This option is disabled as the default setting.

Email messages for the following events

The on-access scan detected a virus or unwanted program

If this option is enabled, you always receive an email with the name of the virus or unwanted program and the affected file when the on-access scan detects a virus or an unwanted program.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "On-access detection" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

A critical error occurred in Real-Time Protection

If this option is enabled, you will receive an email whenever an internal critical error is detected.

> **Note**
> In this case, please inform our technical support and include the data given in the email. The specified file should also be sent for examination.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for a "Critical error in Real-Time Protection" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

System Scanner email alerts

With certain events, the on-demand scan can send alerts and messages via email to one or more recipients.

Email alerts

If this option is enabled, the program sends email messages with the most important information when a certain event occurs. This option is disabled as the default setting.

Email messages for the following events

The on-demand scan detected a virus or unwanted program

If this option is enabled, you receive an email with the name of the virus or unwanted program and the affected file whenever the on-demand scan detects a virus or an unwanted program.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Scan detection" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

End of scheduled scan

When the option is activated, an email is sent when a scan job has been performed. The email contains data on the point and duration of the scan job, on the folders and files scanned as well as on the viruses found and warnings.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for the "End of scan" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Add report file as attachment

If this option is enabled, the current report file of the System Scanner component is added to the email as an attachment when sending System Scanner notifications.

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

Updater email alerts

The Updater component can send notifications by email to one or more recipients for specific events.

Email alerts

If this option is enabled, the Update component sends email messages with the most important data when a specific event occurs. This option is disabled as the default setting.

Email messages for the following events

No update necessary. Your program is up-to-date

If this option is enabled, an email is sent if the Updater has successfully made a connection to the download server but there are no new files available on the server. This means that your Avira product is up to date.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for a "No update necessary" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Update completed successfully. New files have been installed

If this option is enabled, an email is sent for all updates performed: This may be a product update or an update of the virus definition file or of the scanning engine.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Update successful – new files installed" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Update failed

If this option is enabled, an email is sent if the update has failed due to an error.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Update failed" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Add report file as attachment

If this option is enabled, the current report file of the Updater component is added to the email as an attachment when sending Updater notifications.

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

Email template

In the **Email template** window you can configure the email notifications for the individual components to the enabled events. You can insert text of up to a maximum of 128 characters in the subject line and up to a maximum of 1024 characters in the message field.

The following variables can be used in the email subject and email message:

Globally acceptable variables

Variable	Value
Windows environment variables	The email notifications component supports all Windows environment variables.
%SYSTEM_IP%	IP address of the computer
%FQDN%	Fully qualified domain name
%TIMESTAMP%	Event time stamp: Time and date format as per the language settings of the operating system
%COMPUTERNAME%	NetBIOS computer name
%USERNAME%	Name of user accessing the component
%PRODUCTVER%	Product version
%PRODUCTNAME%	Product name
%MODULENAME%	Name of the component sending the email
%MODULEVER%	Version of the component sending the email

Specific component variables

Variable	Value	Component emails
%ENGINEVER%	Version of scan engine used	Realtime Protection System Scanner
%VDFVER%	Version of virus definition file used	Realtime Protection System Scanner

%SOURCE%	Fully qualified file name	Real-Time Protection
%VIRUSNAME%	Name of the virus or unwanted program	Realtime Protection
%ACTION%	Action performed after the detection	Realtime Protection
%MACADDR%	MAC address of the first registered network card	Realtime Protection
%UPDFILESLIST%	List of updated files	Updater
%UPDATETYPE%	Update type: Update of scan engine and virus definition file, or product update with update of scan engine and virus definition file	Updater
%UPDATEURL%	URL of download server used for update	Updater
%UPDATE_ERROR%	Update error in words	Updater
%DIRCOUNT%	Number of scanned directories	System Scanner
%FILECOUNT%	Number of files scanned	System Scanner
%MALWARECOUNT%	Number of viruses or unwanted programs detected	System Scanner
%REPAIREDCOUNT%	Number of infected files repaired	System Scanner

%RENAMEDCOUNT%	Number of infected files renamed	System Scanner
%DELETEDCOUNT%	Number of infected files deleted	System Scanner
%WIPECOUNT%	Number of infected files overwritten and deleted	System Scanner
%MOVEDCOUNT%	Number of infected files moved to quarantine	System Scanner
%WARNINGCOUNT%	Number of warnings	System Scanner
%ENDTYPE%	Status of scan: Terminated/Successfully completed	System Scanner
%START_TIME%	Start time of the scan: Start time of the update	System Scanner, Updater
%END_TIME%	End of the scan End of the update	System Scanner, Updater
%TIME_TAKEN%	Duration of scan in minutes Duration of the update in minutes	System Scanner, Updater
%LOGFILEPATH%	Path and file name of the report file	System Scanner, Updater

Acoustic alerts

When a virus or malware is detected by the System Scanner or Real-Time Protection, an acoustic alert is heard in interactive action mode. You can now choose to activate or deactivate the acoustic alert and select an alternative WAVE file for the alert.

> **Note**
> The action mode of the System Scanner is set in the configuration under System Scanner > Scan > Action on detection. The action mode of the Real-Time Protection is set in the configuration under Real-Time Protection > Scan > Action on detection.

No warning

When this option is enabled, there is no acoustic alert when a virus is detected by the System Scanner or Real-Time Protection.

Use PC speakers (only in interactive mode)

If this option is enabled, there is an acoustic alert with the default signal when a virus is detected by the System Scanner or Real-Time Protection. The acoustic alert is sounded on the PC's internal speaker.

Use the following WAVE file (only in interactive mode)

If this option is enabled, there is an acoustic alert with the selected WAVE file when a virus is detected by the System Scanner or Real-Time Protection. The selected WAVE file is played over a connected external speaker.

WAVE file

In this input box you can enter the name and the associated path of an audio file of your choice. The program's default acoustic signal is entered as standard.

...

The button opens a window in which you can select the required file with the aid of the file explorer.

Test

This button is used to test the selected WAVE file.

Alerts

Your Avira product generates so-called slide-ups, desktop notifications for specific events, which give information on successful or failed program sequences such as updates. Under **Alerts** you can enable or disable the notifications for specific events.

With desktop notifications, you have the option of disabling the notification directly in the slide-up. You can reactivate the notification, in the **Alerts** configuration window.

Update

Alert, if last update is older than n day(s)

In this box, you can enter the maximum number of days allowed to have passed since the last update. If this number of days has passed, a red icon is displayed for the update status under **Status** in the Control Center.

Show notice if the virus definition file is out of date

If this option is enabled, you will obtain an alert if the virus definition file is not up-to-date. With the help of the alert option, you can configure the temporal interval for an alert if the last update is older than n day(s).

Warnings / Notes with the following situations

Dial-up connection is used

If this option is enabled, you will receive a desktop notification alert if a dialer creates a dial-up connection on your computer via the telephone or ISDN network. There is a danger that the connection may have been created by an unknown and unwanted dialer and that the connection may be chargeable (see Viruses and more > Threat categories: Dialer).

Files have been successfully updated

If this option is enabled, you will receive a desktop notification whenever an update has been successfully performed and files updated.

Update failed

If this option is enabled, you will receive a desktop notification whenever an update fails: No connection to the download server could be created or the update files could not be installed.

No update necessary

If this option is enabled, you will receive a desktop notification whenever an update is started but installation of the files is not necessary as your program is up to date.

9. Tray Icon

The tray icon in the system tray of the taskbar displays the status of the Real-Time Protection and the FireWall service.

Icon	Description
🟥	Avira Real-Time Protection is enabled and the FireWall is enabled
🟥	Avira Real-Time Protection is disabled or the FireWall is disabled

Entries in the context menu

- **Enable Real-Time Protection**: Enables or disables the Avira Real-Time Protection.
- **Enable Mail Protection**: Enables or disables the Avira Mail Protection.
- **Enable Web Protection**: Enables or disables the Avira Web Protection.
- **FireWall**:
  - **Enable FireWall**: Enables or disables the Avira FireWall
  - **Enable Windows Firewall**: Enables or disables the Windows Firewall (this feature is available starting from Windows 8).
  - **Block all traffic**: Enabled: Blocks all data transfers except transfers to the host computer system (Local Host/IP 127.0.0.1).
- **Start Avira Professional Security**: Opens the Control Center.
- **Configure Avira Professional Security**: Opens the Configuration.
- **Start update** Starts an update.
- **Select configuration**:
Opens a submenu with the available configuration profiles. Click on a configuration to activate this configuration. The menu command is disabled if you have already defined rules for automatic switching to a configuration.
- **Help**: opens the Online Help.
- **About Avira Professional Security**: Opens a dialog box with information on your Avira product: Product information, Version information, License information.
- **Avira on the Internet**: Opens the Avira web portal on the Internet. The condition for this is that you have an active connection to the Internet.

Note

The User Account Control (UAC) will ask for your permission to enable or disable the Real-Time Protection, FireWall, Web Protection and Mail Protection services in operating systems as of Windows Vista.

10. FireWall

Avira Professional Security allows you to manage the incoming and outgoing data traffic depending on computer settings:

- Avira FireWall

Avira Professional Security includes the Avira FireWall.

- Avira FireWall under AMC

If administrated through the Avira Management Console, your Avira Professional Security also includes the Avira FireWall.

- Windows Firewall

Starting from Windows 7, Avira Professional Security allows the Windows Firewall management through the Avira product.

10.1 Avira FireWall

10.1.1 Avira FireWall

Avira FireWall monitors and regulates incoming and outgoing data traffic on your computer system and protects you from a wide range of attacks and threats from the Internet: Incoming or outgoing data traffic or listening to ports will be allowed or denied based on security guidelines. You will receive a desktop notification if Avira FireWall denies network activity and thus blocks network connections. The following options are available for Avira FireWall settings:

setting a security level in the Control Center

You can define a security level in the Control Center. The *low*, *medium* and *high* security levels each contain several complementary security rules based on packet filters. These security rules are saved as predefined adapter rules in the Configuration under FireWall > Adapter rules

saving actions in the Network event window

When an application first tries to create a network or Internet connection, the *Network Event* popup window appears. The *Network Event* window allows the user to choose whether the network activity of the application is allowed or denied. If the **Save Action for this application** option is enabled, the action is created as an application rule and is saved in the configuration under **FireWall > Application rules**. Saving the actions in the Network event window gives you a set of rules for the network activities of applications.

> **Note**
> For applications from trusted vendors, network access is allowed by default unless an adapter rule prohibits network access. You have the option of removing providers from the list of trusted vendors.

creating adapter and application rules in the Configuration

You can alter predefined adapter rules or create new adapter rules in the Configuration. The security level of the Avira FireWall is automatically set to the value *Custom* if you add or change adapter rules.
Application rules allow you to define monitoring rules specified for applications:
You can use simple application rules to define whether all network activities of a software application are to be denied or allowed or whether they are to be handled by means of the *Network Event* popup window.
In the advanced configuration of the *Application rules* setting you can define different packet filters for an application, which are executed as specified application rules.

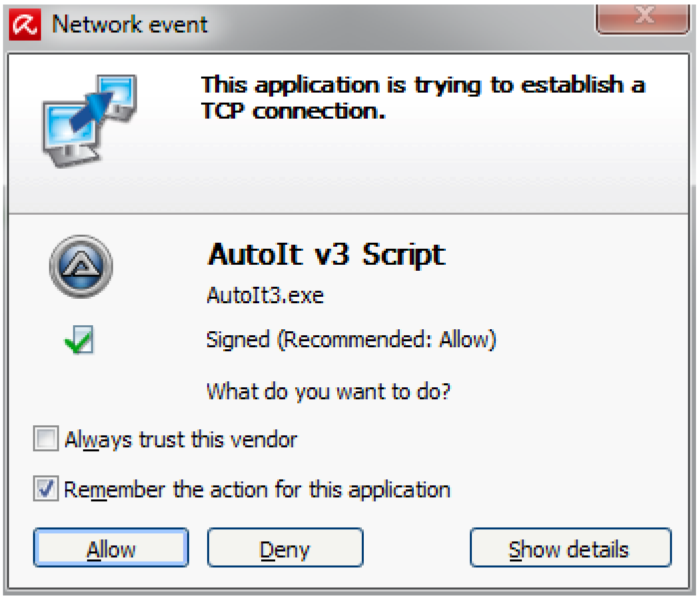
10.1.2 Network event

In the Network event window of the Avira FireWall component you can choose whether or not a software application of the network access is to be allowed to send data or to perform other network activities: You can allow or deny data traffic or passive listening to ports. Denying network activities may cause a connection to be canceled.

The Network event window opens in the following cases when applications are accessed from the network:

- No application rules have yet been created for the application. This is the case when an application establishes a connection to the network for the first time after the Avira FireWall is installed. However, applications whose vendors have been classified as trusted and whose network access was automatically permitted are excluded (see Chapter Configuration > FireWall > Avira FireWall > Trusted vendors).
- A simple application rule with action type **Ask** was created.
- Specified application rules were created for the application based on packet filters in the extended configuration, however no rule was detected for the network event that has arisen. In this case you can use the *Extended* button to call up the existing application rules and to add network access as a new rule.

Network event



Network event

This application is trying to establish a TCP connection.

AutoIt v3 Script

AutoIt3.exe

Signed (Recommended: Allow)

What do you want to do?

□ Always trust this vendor

☑ Remember the action for this application

Displayed information

Name of the application.

Name of the application.

File name

Name of the executable file.

Signature check and recommendation

Result of the signature check and recommended action.
If the application is signed with the certificate of a trusted provider, it is recommended that data traffic should be allowed.

Detailed information

Local address

Source address and source port.

Remote address

Target address and target port.

User

Registered user under which the application is executed.

Process ID

The process ID of the application.

Path

Path to the executable file for the application.

Company

Application provider (version information).

Version

Version of the application.

Signed by

Application provider (signature).

Actions and buttons

Always trust this vendor

If this option is enabled, the software provider is added to the list of trusted vendors when executing the *Network Event* request. The Deny button is disabled as soon as you enable this option.

> **Note**
> This action is only available with signed applications.

Remember the action for this application

If this option is enabled, the executed action is saved as an application rule. The application rule can be called up in the configuration under FireWall > Popup settings.

If the *Remember action for this application* option is enabled and specified application rules based on packet filters exist for the application, the window for advanced configuration of application rules is opened when you click the **Allow** or **Deny** buttons. The data traffic that has occurred has been automatically added to the top of the list as a specified application rule. You can change the position of the application rules added or remove the added application rules in the *FireWall* > *Application Rules* window.

Buttons	Description
Advanced	The window for the advanced configuration of application rules is opened. **Note** The button is only available if extended settings are activated for application rules (see Configuration > FireWall > Settings).
Allow	The relevant network activity is permitted.
Deny	The relevant network activity is denied.
Show/Hide details	Detailed information about the application is displayed or hidden.

10.2 Windows Firewall

Avira Professional Security gives you the option of managing directly the Windows Firewall via the Avira Control and Configuration Center. The following options are available for Windows Firewall:

enabling Windows Firewall through the Control Center

The *FireWall* option under **Status > Internet Protection** allows you to enable or disable the Windows Firewall by clicking the **ON/OFF** button.

checking the status of the Windows Firewall through the Control Center

You can check the status of the Windows Firewall under the section **INTERNET PROTECTION > FireWall** and restore the recommended settings by clicking the **Fix problem** button.

11. Updates

11.1 Updates

The effectiveness of anti-virus software depends on how up-to-date the program is, in particular the virus definition file and the scan engine. To carry out regular updates, the Updater component is integrated into your Avira product. The Updater ensures that your Avira product is always up-to-date and able to deal with the new viruses that appear every day. Updater updates the following components:

- Virus definition file:

  The virus definition file contains the virus patterns of the harmful programs which are used by your Avira product to scan for viruses and malware and repair infected objects.

- Scan engine:

  The scan engine contains the methods used by your Avira product to scan for viruses and malware.

- Program files (product update):

  Update packages for product updates make extra functions available to the individual program components.

An update checks whether the virus definition file, the scan engine and the product are up-to-date and if necessary, implements an update. After a product update, you may have to restart your computer system. If only the virus definition file and scan engine are updated, the computer does not have to be restarted.

When a product update requires a reboot, you can decide whether to continue with the update or to be reminded again later about the update. If you continue with the product update immediately, you are still able to choose when the reboot should take place.

If you want to be reminded about the update later on, the virus definition file and the scan engine will be updated anyway, but the product update will not be done.

> **Note**
> The product update will not be completed until a reboot has occurred.
>
> **Note**
> For security reasons, the Updater checks whether the Windows *hosts* file of your computer was altered, whether the Update URL, for example, was manipulated by malware and is diverting the Updater to unwanted download sites. If the Windows hosts file has been manipulated, this is shown in the Updater report file.

An update is automatically performed in the following interval: 60 minutes. You can edit or disable the automatic update through the configuration (Configuration > Update).

In the Control Center under **Scheduler**, you can create additional update jobs that are performed by Updater at the specified intervals. You also have the option to start an update manually:

- in the Control Center: in the **Update** menu and in the **Status** section
- via the context menu of the tray icon

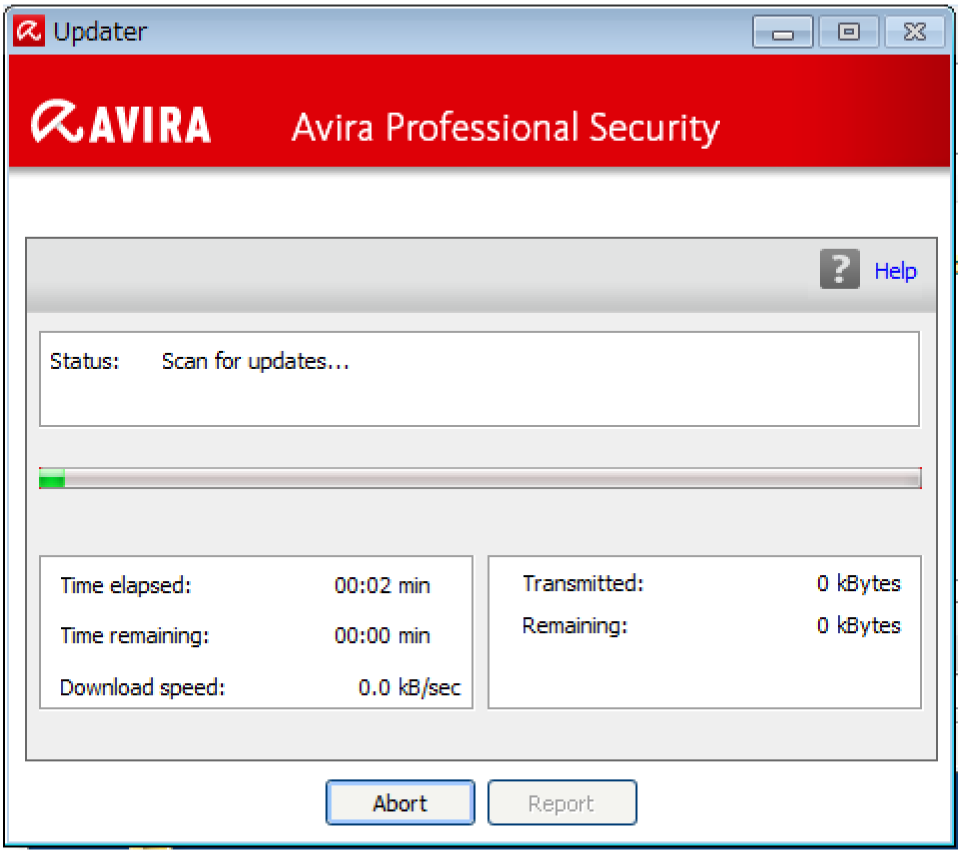
Updates can be obtained from the Internet via proprietary web server or via web or file server on an intranet which downloads the update files from the Internet and makes them available to other computers on the network. This is useful if you want to update Avira products on more than one computer in a network. A download server on an intranet can be used to ensure Avira products are up-to-date on the protected computers using a minimum of resources. To set up a functioning download server on an intranet, you need a server that is compatible with the update structure of your Avira product.

> **Note**
> You can use Avira Update Manager (file server or web server in Windows) as a web server or file server in the intranet. Avira Update Manager mirrors the download servers of Avira products and can be obtained from the Avira website on the Internet.
> http://www.avira.com

When a web server is used, the HTTP protocol is used for the download. When using a file server, access to the update file is provided via the network. You can configure the connection to the web server or file server under Configuration > Update. The default configuration uses the existing Internet connection as the connection to the Avira web servers.

11.2 Updater

The Updater window opens at the start of an update.



Status: Scan for updates...

Time elapsed:	00:02 min
Time remaining:	00:00 min
Download speed:	0.0 kB/sec

Transmitted:	0 kBytes
Remaining:	0 kBytes

Note
For update jobs created in Scheduler, you can define the display mode for the update window: You can select **Hide**, **Minimize** or **Maximize**.

Note
If you are using a program in fullscreen mode (e.g. games) and the updater's display mode is set to maximized or minimized, the updater will switch to the desktop. To prevent this, start the updater with the display mode set to hide. In this mode you will no longer be notified about updates by the update window.

Status: Shows the proceeding of the updater.

Time elapsed: Time which has elapsed since starting the download.

Time remaining: Time until download is finished.

Download speed: Speed of download.

Transmitted: Bytes already downloaded.

Remaining: Bytes left to download.

Buttons and links

Button / link	Description
? Help	This page of the online help is opened via this button or link.
Reduce	The display window of the updater will appear in a reduced size.
Enlarge	The display window of the updater will be re-established to its original size.
Abort	The update procedure will be canceled. The updater will be closed.
Close	The update procedure is completed. The display window will be closed.
Report	The report file of the update is displayed.

12. FAQ, Tips

This chapter contains important information on troubleshooting and further tips on using your Avira product.

- see Chapter Help in case of a problem
- see Chapter Shortcuts
- see Chapter Windows Security Center (Windows XP) or Windows Action Center (as of Windows 7)

12.1 Help in case of a problem

Here you will find information on causes and solutions of possible problems.

- The error message *The license file cannot be opened* appears.
- The error message *Connection failed while downloading the file* ... appears when attempting to start an update.
- Viruses and malware cannot be moved or deleted.
- The status of the tray icon is disabled.
- The computer is extremely slow when I perform a data back-up.
- My firewall reports Avira Real-Time Protection and Avira Mail Protection immediately after activation.
- Avira Mail Protection does not work.
- There is no network connection available in a virtual machine (e.g. VMWare, Virtual PC, ...) if Avira FireWall is installed on the host machine and the security level of Avira FireWall is set to *medium* or *high*.
- Virtual Private Network (VPN) connection is blocked, if the security level of Avira FireWall is set to *medium* or *high*.
- An email sent via a TLS connection has been blocked by Mail Protection.
- Webchat is not operational: Chat messages will not be displayed; data are being loaded in the browser

The error message *The license file cannot be opened* appears.

Reason: The file is encrypted.

- To activate the license, you do not need to open the file, but rather you save it in the program directory. See also Chapter License Manager.

The error message *Connection failed while downloading the file ...* appears when attempting to start an update.

Reason: Your Internet connection is inactive. No connection to the web server on the Internet can therefore be established.

- Test whether other Internet services such as WWW or email work. If not, re-establish the Internet connection.

Reason: The proxy server cannot be reached.

- Check whether the login for the proxy server has changed and adapt it to your configuration if necessary.

Reason: The *update.exe* file is not fully approved by your personal firewall.

- Ensure that the *update.exe* file is fully approved by your personal firewall.

Otherwise:

- Check your settings in the Configuration under PC Protection > Update.

Viruses and malware cannot be moved or deleted.

Reason: The file was loaded by windows and is active.

- Update your Avira product.
- If you use the Windows XP operating system, deactivate System Restore.
- Start the computer in Safe Mode.
- Start the Configuration of your Avira product .
- Select **System Scanner > Scan > Files > All files** and confirm the window with **OK**.
- Start a scan of all local drives.
- Start the computer in Normal Mode.
- Carry out a scan in Normal Mode.
- If no other viruses or malware have been found, activate System Restore if it is available and to be used.

The status of the tray icon is disabled.

Reason: Avira Real-Time Protection is disabled.

- In the Control Center click **Status** and enable the **Real-Time Protection** in the *PC Protection* area .

-OR-

- Open the context menu with a right-click on the Tray Icon. Click **Real-Time Protection enable**.

Reason: Avira Real-Time Protection is blocked by a firewall.

- Define a general approval for Avira Real-Time Protection in the configuration of your firewall. Avira Real-Time Protection only works with the address 127.0.0.1 (localhost). An Internet connection is not established. The same applies to Avira Mail Protection.

Otherwise:

- Check the startup type of the Avira Real-Time Protection service. If necessary, enable the service: In the taskbar, select **Start > Settings > Control Panel**. Start the configuration panel **Services** with a double-click (under Windows XP the services applet is located in the sub-directory *Administrative Tools*). Find the entry *Avira Real-Time Protection*. `Automatic` must be entered as the startup type and `Started` as the status. If necessary, start the service manually by selecting the relevant line and the button **Start**. If an error message appears, please check the event display.

The computer is extremely slow when I perform a data back-up.

Reason: During the backup procedure, Avira Real-Time Protection scans all files being used by the backup procedure.

- Select **Real-Time Protection > Scan > Exceptions** in the Configuration and enter the process names of the back-up software.

My firewall reports Avira Real-Time Protection and Avira Mail Protection immediately after activation.

Reason: Communication with Avira Real-Time Protection and Avira Mail Protection occurs via the TCP/IP Internet protocol. A firewall monitors all connections via this protocol.

- Define a general approval for Avira Real-Time Protection and Avira Mail Protection. Avira Real-Time Protection only works with the address 127.0.0.1 (localhost). An Internet connection is not established. The same applies to Avira Mail Protection.

Avira Mail Protection does not work.

Please check correct functioning of Avira Mail Protection with the aid of the following checklists if problems occur with Avira Mail Protection.

Checklist

- Check whether your mail client logs in to the server via Kerberos, APOP or RPA. These verification methods are currently not supported.
- Check whether your mail client reports to the server through SSL (also often called TLS – Transport Layer Security). Avira Mail Protection does not support SSL and therefore terminates any encrypted SSL connections. If you want to use encrypted SSL connections without having them protected by Mail Protection, you will have to

use a port that is not monitored by Mail Protection for the connection. The ports monitored by Mail Protection can be configured in the configuration under **Mail Protection > Scan**.

- Is the Avira Mail Protection service active? If necessary, enable the service: In the taskbar, select **Start > Settings > Control Panel**. Start the configuration panel **Services** with a double-click (under Windows XP the services applet is located in the sub-directory *Administrative Tools*). Find the entry *Avira Mail Protection*. `Automatic` must be entered as the startup type and `Started` as the status. If necessary, start the service manually by selecting the relevant line and the button **Start**. If an error message appears, please check the event display. If this is not successful, you may have to completely uninstall the Avira product via **Start > Settings > Control Panel > Add or Remove Programs**, to restart the computer and then to reinstall your Avira product.

General

POP3 connections encrypted via SSL (Secure Sockets Layer, also frequently referred to as TLS (Transport Layer Security)) cannot currently be protected and are ignored.

Verification to the mail server is currently only supported via passwords. "Kerberos" and "RPA" are currently not supported.

Your Avira product does not check outgoing emails for viruses and unwanted programs.

> **Note**
> We recommend regularly installing Microsoft updates to close any gaps in security.

There is no network connection available in a virtual machine (e.g. VMWare, Virtual PC, ...) if Avira FireWall is installed on the host machine and the security level of Avira FireWall is set to *medium* or *high*.

If Avira FireWall is installed on a computer on which a virtual machine (for example VMWare, virtual PC, etc.) is also running, the Avira FireWall will block all network connections for the virtual machine when the security level of the Avira FireWall is set to *medium* or *high*. If the security level is set to *low*, the FireWall allows the network connections.

Reason: The virtual machine emulates a network card by means of software. This emulation encapsulates the data packages of the guest system in special packages (UDP packages) and routes them via the external gateway back to the host system. Avira FireWall rejects these packages coming from outside, starting from security level *medium*.

To avoid this behavior do the following:

- Go to Control Center and select the section *INTERNET PROTECTION* > **FireWall**.

- Click the **Configuration** button.

  The *Configuration* dialog box is displayed. You are in the configuration section *Application rules*.
- Select the configuration section **Adapter rules**.
- Click **add rule**.
- Select **UDP** in the section *Incoming rules*.
- Type the **name** of the rule in the Section Name of the rule.
- Click **OK**.
- Check if the rule is directly above the rule **Deny all IP packets**.

> **Warning**
> This rule is potentially dangerous because it will allow UDP packets without any filtering! After working with the virtual machine change to your previous security level.

Virtual Private Network (VPN) connection is blocked, if the security level of Avira FireWall is set to *medium* or *high*.

Reason: By default, all packets that do not comply with the pre-set rules are discarded. Packets dispatched by the VPN software (so-called GRE packets) do not fit into any of the other categories and are therefore filtered by these rules.

Add the rule **Allow VPN connections** in the **Adapter rules** of the Avira FireWall configuration. This rule will allow all VPN related packets.

An email sent via a TLS connection has been blocked by Mail Protection.

Reason: Transport Layer Security (TLS: encryption protocol for data transfers on the Internet) is not supported by Mail Protection at this time. The following options are available for sending the email:

- Use a port other than port 25, which is used by SMTP. This will bypass monitoring by Mail Protection.
- Turn off the TLS encrypted connection and disable TLS support in your email client.
- Disable (temporarily) the monitoring of outgoing emails by Mail Protection in the configuration under **Mail Protection > Scan**.

Webchat is not operational: Chat messages will not be displayed; data are being loaded in the browser.

This phenomenon may occur during chats, which are based on the HTTP protocol with 'transfer-encoding: chunked'.

Reason: Web Protection checks the sent data completely for viruses and undesired programs first, before the data are loaded into the web browser. During a data transfer with ‘transfer-encoding: chunked’, Web Protection cannot determine the message length or the data volume.

- Enter the configuration of the URL of the web chats as an exception (see Configuration: **Web Protection > Scan > Exceptions**).

12.2 Shortcuts

Keyboard commands - also called shortcuts - offer a fast possibility to navigate through the program, to retrieve individual modules and to start actions.

Below we provide you with an overview of the available keyboard commands. Please find further indications regarding the functionality in the corresponding chapter of the help.

12.2.1 In dialog boxes

Shortcut	Description
Ctrl + Tab **Ctrl + Page down**	Navigation in the Control Center Go to next section.
Ctrl + Shift + Tab **Ctrl + Page up**	Navigation in the Control Center Go to previous section.
←↑→↓	Navigation in the configuration sections First, use the mouse to set the focus on a configuration section. Change between the options in a marked drop-down list or between several options in a group of options.
Tab	Change to the next option or options group.
Shift + Tab	Change to the previous option or options group.
Space	Activate or deactivate a check box, if the active option is a check box.

Alt + underlined letter	Select option or start command.
Alt + ↓ **F4**	Open selected drop-down list.
Esc	Close selected drop-down list. Cancel command and close dialog.
Enter	Start command for the active option or button.

12.2.2 In the help

Shortcut	Description
Alt + Space	Display system menu.
Alt + Tab	Shift between the help and the other opened windows.
Alt + F4	Close help.
Shift + F10	Display context menu of the help.
Ctrl + Tab	Go to next section in the navigation window.
Ctrl + Shift + Tab	Go to previous section in the navigation window.
Page up	Change to the subject, which is displayed above in the contents, in the index or in the list of the search results.
Page down	Change to the subject, which is displayed below the current subject in the contents, in the index or in the list of the search results.

Page up **Page down**	Browse through a subject.

12.2.3 In the Control Center

General

Shortcut	Description
F1	Display help
Alt + F4	Close Control Center
F5	Refresh
F8	Open configuration
F9	Start update

Scan section

Shortcut	Description
F2	Rename selected profile
F3	Start scan with the selected profile
F4	Create desktop link for the selected profile
Ins	Create new profile

Del	Delete selected profile

FireWall section

Shortcut	Description
Return	Properties

Quarantine section

Shortcut	Description
F2	Rescan object
F3	Restore object
F4	Send object
F6	Restore object to...
Return	Properties
Ins	Add file
Del	Delete object

Scheduler section

Shortcut	Description
F2	Edit job
Return	Properties

Ins	Insert new job
Del	Delete job

Reports section

Shortcut	Description
F3	Display report file
F4	Print report file
Return	Display report
Del	Delete report(s)

Events section

Shortcut	Description
F3	Export event(s)
Return	Show event
Del	Delete event(s)

12.3 Windows Security Center

- Windows XP Service Pack 3 -

12.3.1 General

The Windows Security Center checks the status of a computer for important security aspects.

If a problem is detected with one of these important points (e.g. an outdated anti-virus program), the Security Center issues an alert and gives recommendations on how to protect your computer better.

12.3.2 The Windows Security Center and your Avira product

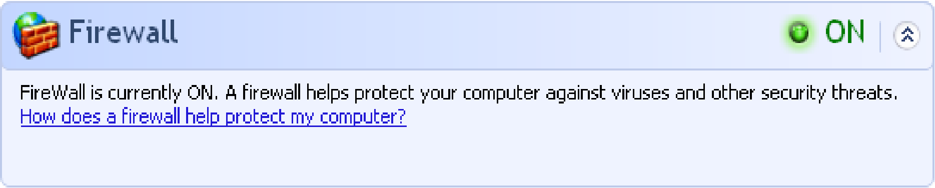
FireWall

You may receive the following information from the Security Center with regard to your firewall:

- Firewall ACTIVE / Firewall on
- Firewall INACTIVE / Firewall off

Firewall ACTIVE / Firewall on

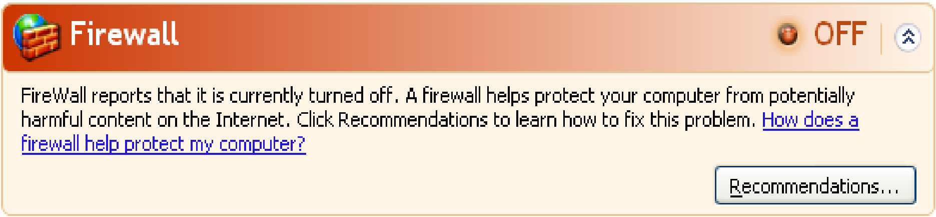
After installing your Avira product and turning off Windows Firewall, you will receive the following message:



FireWall is currently ON. A firewall helps protect your computer against viruses and other security threats.
How does a firewall help protect my computer?

Firewall INACTIVE / Firewall off

You will receive the following message as soon as you disable the Avira FireWall:



FireWall reports that it is currently turned off. A firewall helps protect your computer from potentially harmful content on the Internet. Click Recommendations to learn how to fix this problem. How does a firewall help protect my computer?

Note
You can enable or disable the Avira FireWall via the Status tab in the Control Center.

Warning
If you turn the Avira FireWall off, unauthorized users may gain access to your computer through a network or the Internet.

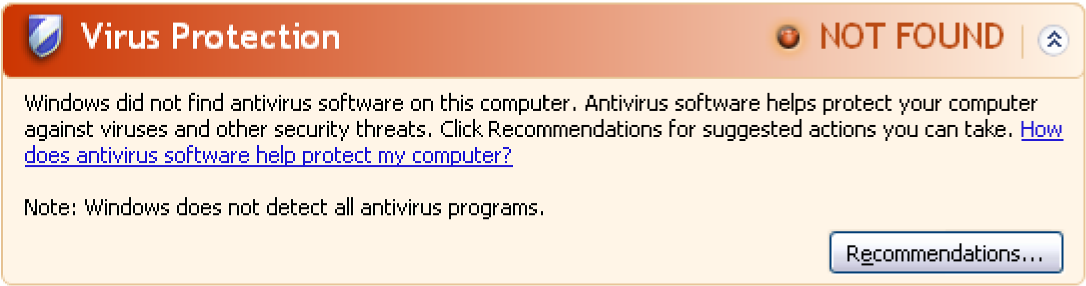
Virus protection software / Protection against malicious software

You may receive the following information from the Windows Security Center with regard to your virus protection:

- Virus protection NOT FOUND
- Virus protection OUT OF DATE
- Virus protection ON
- Virus protection OFF
- Virus protection NOT MONITORED

Virus protection NOT FOUND

This information of the Windows Security Center appears when the Windows Security Center has not found any anti-virus software on your computer.



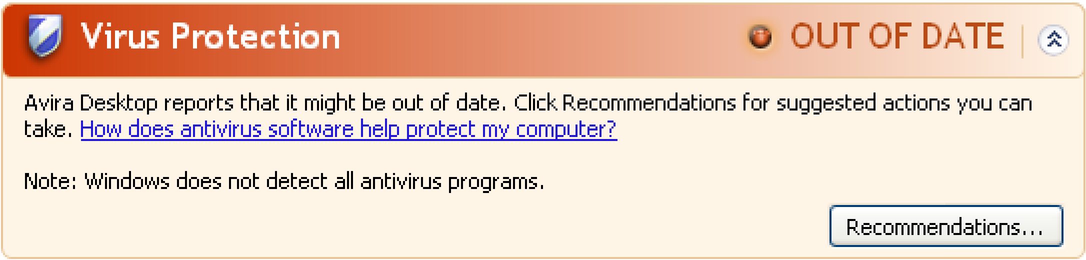
Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

Note
Install your Avira product on your computer to protect it against viruses and other unwanted programs!

Virus protection OUT OF DATE

If you have already installed Windows XP Service Pack 3 and then install your Avira product or you install Windows XP Service Pack 3 on a system on which your Avira product has already been installed, you will receive the following message:



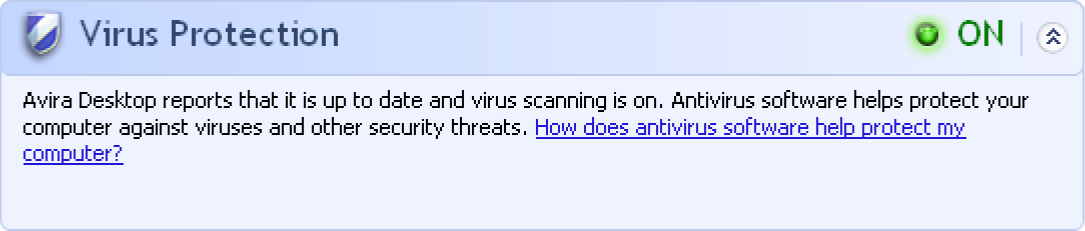
Avira Desktop reports that it might be out of date. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

Note
In order for the Windows Security Center to recognize your Avira product as up-to-date, an update must be performed after installation. Update your system by carrying out an update.

Virus protection ON

After installing your Avira product and performing a subsequent update, you will receive the following message:

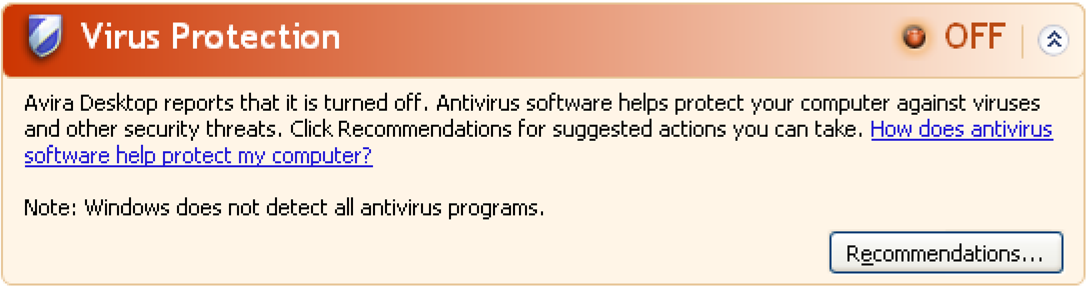


Avira Desktop reports that it is up to date and virus scanning is on. Antivirus software helps protect your computer against viruses and other security threats. How does antivirus software help protect my computer?

Your Avira product is now up-to-date and the Avira Real-Time Protection is enabled.

Virus protection OFF

You receive the following message if you disable the Avira Real-Time Protection or stop the Real-Time Protection service.



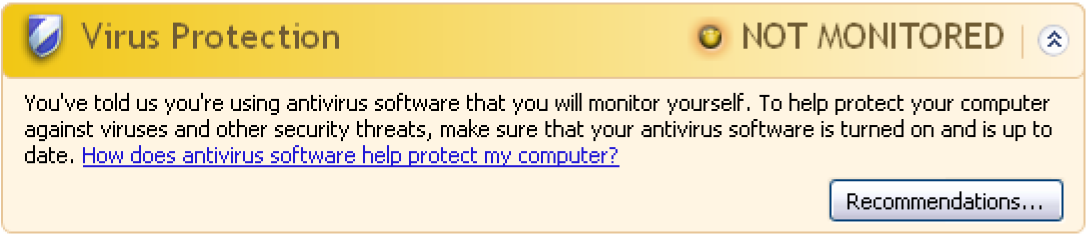
Avira Desktop reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

Note
You can enable or disable Avira Real-Time Protection in the Status section of the **Control Center**. You can also see that the Avira Real-Time Protection is enabled if the red umbrella in your taskbar is open.

Virus protection NOT MONITORED

If you receive the following message from the Windows Security Center, you have decided that you want to monitor your anti-virus software yourself.



Virus Protection

NOT MONITORED

You've told us you're using antivirus software that you will monitor yourself. To help protect your computer against viruses and other security threats, make sure that your antivirus software is turned on and is up to date. How does antivirus software help protect my computer?

Note
The Windows Security Center is supported by your Avira product. You can enable this option at any time via the **Recommendations** button.

Note
Even if you have installed Windows XP Service Pack 3, you still require a virus protection solution. Although Windows monitors your anti-virus software, it does not contain any anti-virus functions itself. Therefore you would not be protected against viruses and other malware without an additional anti-virus solution!

12.4 Windows Action Center

- Windows 7 and Windows 8 -

12.4.1 General

Note:
Starting from Windows 7 the **Windows Security Center** has been renamed to **Windows Action Center**. Under this section you will find the status of all your security options.

The Windows Action Center checks the status of a computer for important security aspects. You can access it directly by clicking the little flag in your taskbar or under **Control Panel > Action Center**.

If a problem is detected with one of these important points (e.g. an outdated anti-virus program), the Action Center issues an alert and gives recommendations on how to protect your computer better. This means, that if everything works correctly, you won't be bothered with messages. You still can have a look at the security status of your computer in the **Windows Action Center**, under the **Security** item.
The **Windows Action Center** also gives you the option of managing the installed programs and to choose between them (e.g. *View installed antispyware programs*).

You can even turn off the warning messages under **Change Action Center settings** (e.g. *Turn off messages about spyware and related protection*).

12.4.2 The Windows Action Center and your Avira product

Network firewall

You may receive the following information from the **Windows Action Center** with regard to your firewall:

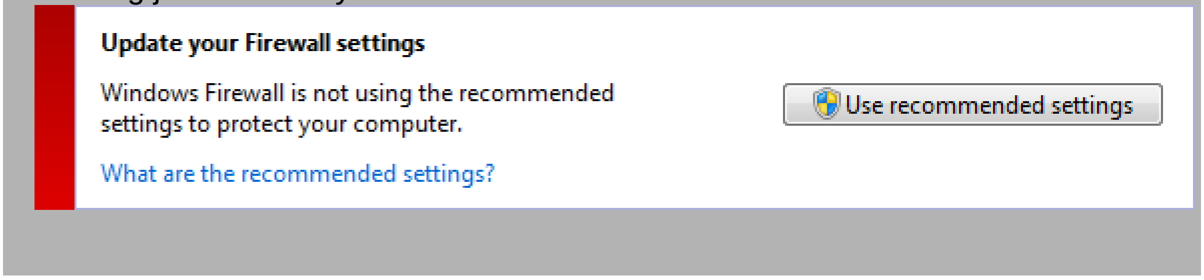
- Avira FireWall reports that it is turned on
- Windows Firewall and Avira FireWall both report that they are turned off.
- Windows Firewall is turned off or set up incorrectly

Avira FireWall reports that it is turned on

After installing your Avira product and turning off Windows Firewall, you will see the following message under **Action Center > Security > Network firewall**: *Avira FireWall reports that it is turned on*. This means that your have chosen Avira FireWall as your firewall solution. (Please notice the difference between Windows Firewall and Avira FireWall, with capital W).

Warning

Under the selection **Control Panel > Windows Firewall** the **only product referred to is Windows Firewall and not Avira FireWall**. That is the reason why everything will be marked in red with the message: *Update your Firewall settings* and ***Windows Firewall is not using the recommended settings to protect your computer***. You don't need to do anything, your Avira product is working just fine and your PC is secure.



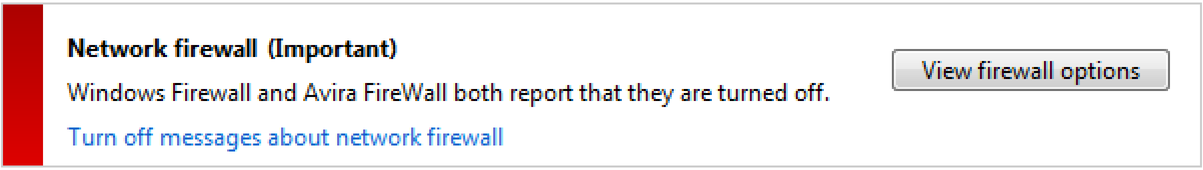
Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Windows Firewall and Avira FireWall both report that they are turned off

You will receive the following message as soon as you disable the Avira FireWall:



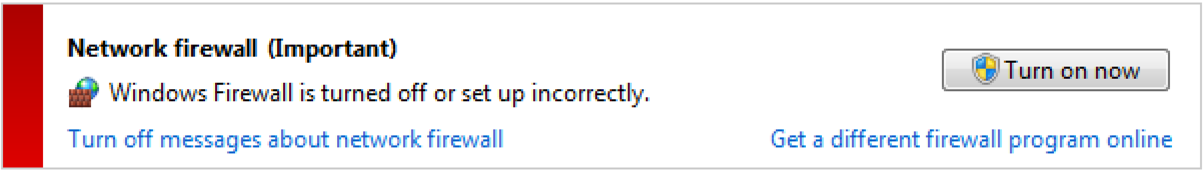
Network firewall (Important)

Windows Firewall and Avira FireWall both report that they are turned off.

Turn off messages about network firewall

> **Warning**
> If you turn the Avira FireWall off, unauthorized users may gain access to your computer through a network or the Internet.

Windows Firewall is turned off or set up incorrectly



Network firewall (Important)

Windows Firewall is turned off or set up incorrectly.

Turn on now
Turn off messages about network firewall
Get a different firewall program online

This means that neither the firewall from Windows nor the one from Avira are activated. You can receive this message in two different situations:

- **Avira FireWall installed**

  Avira FireWall is set up incorrectly or has not been installed correctly. Avira FireWall should be immediately detected by Windows Action Center. Please try rebooting your computer, and if this does not work, install Avira again.

- **Windows Firewall installed**

  Starting from Windows 7, Avira Professional Security gives you the option of directly managing the Windows Firewall from the Avira Control and Configuration Center.

Virus protection

You may receive the following information from the Windows Action Center with regard to your virus protection:

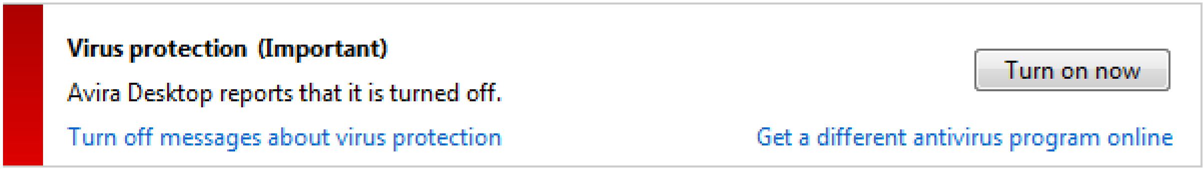
- Avira Desktop reports that it is up to date and virus scanning is on.
- Avira Desktop reports that it is turned off.
- Avira Desktop reports that it is out of date.
- Windows did not find antivirus software on this computer.
- Avira Desktop has expired.

Avira Desktop reports that it is up to date and virus scanning is on

After installation of your Avira product and a subsequent update, you will not receive any messages from the Windows Action Center. But if you go to **Action Center > Security** you can see: *Avira Desktop reports that it is up to date and virus scanning is on.* This means that your Avira product is now up-to-date and the Avira Real-Time Protection is enabled.

Avira Desktop reports that it is turned off

You receive the following message if you disable the Avira Real-Time Protection or stop the Real-Time Protection service.



Virus protection (Important)

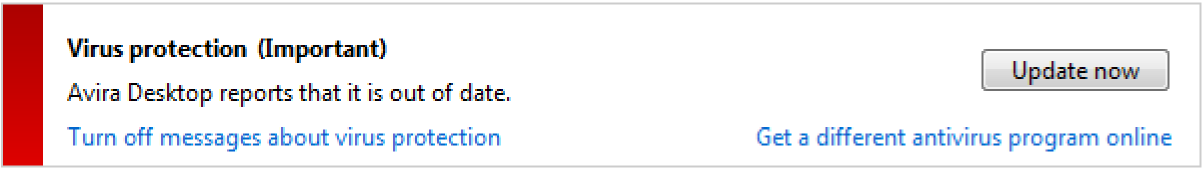
Avira Desktop reports that it is turned off.

Turn on now
Turn off messages about virus protection
Get a different antivirus program online

> **Note**
> You can enable or disable Avira Real-Time Protection in the **Status** section of the **Avira Control Center**. You can also notice that the Avira Real-Time Protection is enabled by the opened red umbrella in your taskbar. It is also possible to activate the Avira product by clicking the *Turn on now* button on the Windows Action Center message. You will receive a notification asking your permission to run Avira. Click on *Yes, I trust the publisher and want to run this program* and Real-Time Protection will be enabled again.

Avira Desktop reports that it is out of date

If you just installed Avira or if for some reason the virus definition file, the scan engine or the program files of your Avira product have not been updated automatically (e.g. if you have made an upgrade from an older Windows operating system, on which your Avira product is already installed), you will receive the following message:



Virus protection (Important)

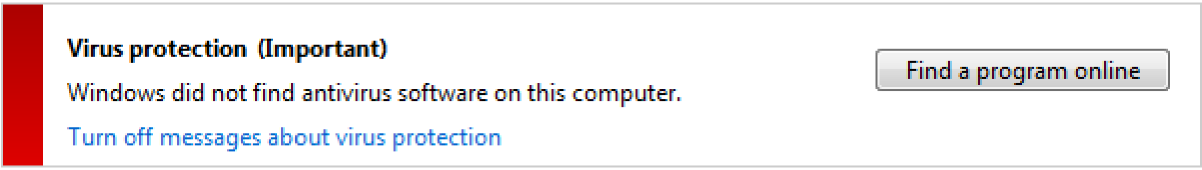
Avira Desktop reports that it is out of date.

Update now
Turn off messages about virus protection
Get a different antivirus program online

> **Note**
> In order for the Windows Action Center to recognize your Avira product as up-to-date, an update must be performed after installation. Update your Avira Product by carrying out an update.

Windows did not find antivirus software on this computer

This information of the Windows Action Center appears, when the Windows Action Center has not found any anti-virus software on your computer.



Virus protection (Important)

Windows did not find antivirus software on this computer.

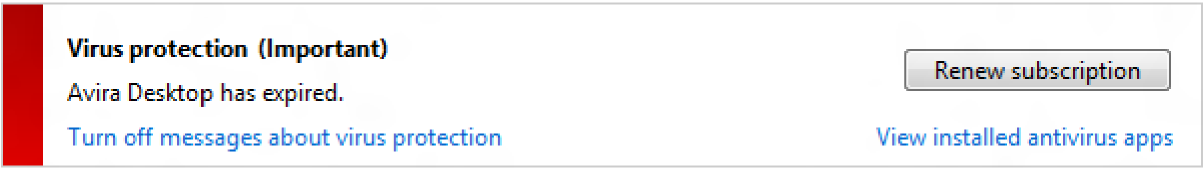
Turn off messages about virus protection

Note
Please note that this option will not appear in Windows 8, as Windows Defender is now also the pre-set virus protection function.

Note
Install your Avira product on your computer to protect it against viruses and other unwanted programs!

Avira Desktop has expired

This information of the Windows Action Center appears when the license of your Avira product has expired.
If you click on the button **Renew subscription**, you will be redirected to the website of Avira, where you can buy a new license.



Virus protection (Important)

Avira Desktop has expired.

Turn off messages about virus protection

Note
Please note that this option is only available for Windows 8.

Spyware and unwanted software protection

You may receive the following information from the Windows Action Center with regard to your spyware protection:

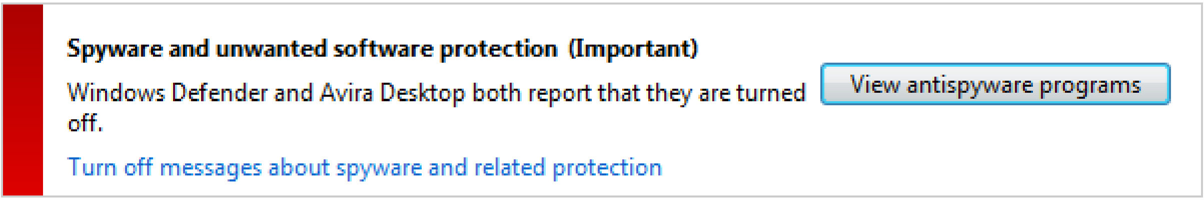
- Avira Desktop reports that it is turned on.
- Windows Defender and Avira Desktop both report that they are turned off.
- Avira Desktop reports that it is out of date.
- Windows Defender is out of date.
- Windows Defender is turned off.

Avira Desktop reports that it is turned on

After the installation of your Avira product and a subsequent update, you will not receive any messages from the Windows Action Center. But if you go to **Action Center > Security**, you can see: *Avira Desktop reports that it is turned on*. This means that your Avira product is now up-to-date and the Avira Real-Time Protection is enabled.

Windows Defender and Avira Desktop both report that they are turned off

You receive the following message if you disable the Avira Real-Time Protection or stop the Real-Time Protection service.



Spyware and unwanted software protection (Important)

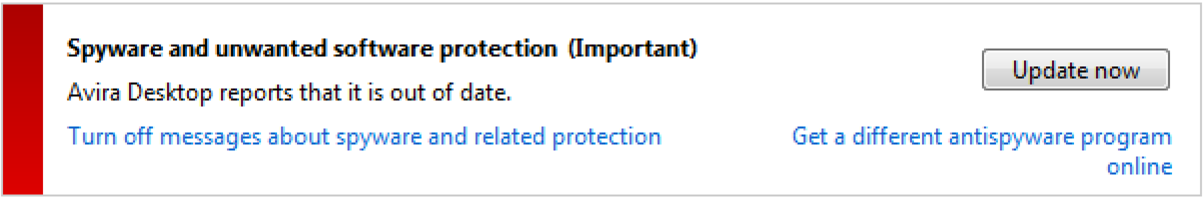
Windows Defender and Avira Desktop both report that they are turned off.

View antispyware programs
Turn off messages about spyware and related protection

Note
You can enable or disable Avira Real-Time Protection in the **Status** section of the **Avira Control Center**. You can also notice that the Avira Real-Time Protection is enabled by the opened red umbrella in your taskbar. It is also possible to activate the Avira product by clicking the *Turn on now* button on the Windows Action Center message. You will receive a notification asking your permission to run Avira. Click on *Yes, I trust the publisher and want to run this program* and Real-Time Protection will be enabled again.

Avira Desktop reports that it is out of date

If you just installed Avira or if for some reason the virus definition file, the scan engine or the program files of your Avira product have not been updated automatically (e.g. if you have made an upgrade from an older Windows operating system, on which your Avira product is already installed), you will receive the following message:



Spyware and unwanted software protection (Important)

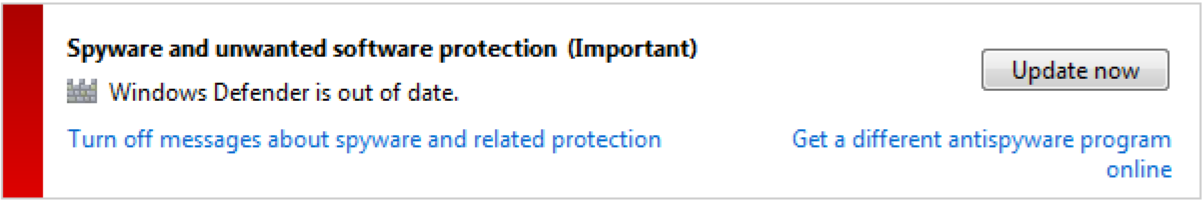
Avira Desktop reports that it is out of date.

Update now
Turn off messages about spyware and related protection
Get a different antispyware program online

Note
In order for the Windows Action Center to recognize your Avira product as up-to-date, an update must be performed after installation. Update your Avira Product by carrying out an update.

Windows Defender is out of date

You may receive the following message if Windows Defender is activated. If you have already installed the Avira product, this message should not appear. Please check if the installation went OK.



Spyware and unwanted software protection (Important)

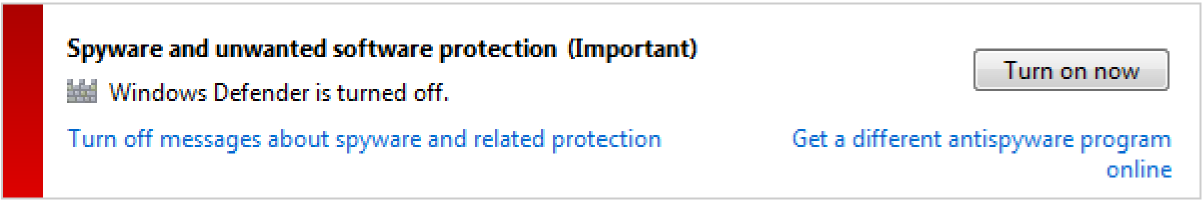
Windows Defender is out of date.

Update now
Turn off messages about spyware and related protection
Get a different antispyware program online

Note
Windows Defender is the pre-set spyware and virus protection solution from Windows.

Windows Defender is turned off

This information of the Windows Action Center appears when the Windows Action Center has not found any other anti-virus software on your computer than the one that the operating system integrates by default: Windows Defender. If you have had some anti-virus software installed on your computer before, this application has been disabled. If you have already installed the Avira product, this message should not appear: Avira should be automatically detected. Please check if the installation went OK.



Spyware and unwanted software protection (Important)

Windows Defender is turned off.

Turn on now
Turn off messages about spyware and related protection
Get a different antispyware program online

13. Viruses and more

Avira Professional Security not only detects viruses and malware, it can also protect you from other threats. In this chapter you can find an overview of different kinds of malware and other threats describing their background, behavior and the unpleasant surprises they have in store for you.

Related topics:

- Threat categories
- Viruses and other malware

13.1 Threat categories

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Your Avira product detects Adware. If the **Adware** option is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects adware.

Adware/Spyware

Software that displays advertising or software that sends the user's personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted.

Your Avira product recognizes "Adware/Spyware". If the option **Adware/Spyware** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects adware or spyware.

Application

The term APPL, respectively application, refers to an application which may involve a risk when used or is of dubious origin.

Your Avira product recognizes "Application (APPL)". If the option **Application** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such behavior.

Backdoor Clients

In order to steal data or manipulate computers, a backdoor server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the Internet or a network.

Your Avira product recognizes "Backdoor control software". If the **Backdoor control software** option is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such software.

Dialer

Certain services available in the Internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user’s computer subject to the user’s consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the Internet user’s default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask your telephone provider to block this number range directly for immediate protection against undesired dialers (0190/0900 dialers).

Your Avira product can detect the familiar dialers by default.

If the option **Dialers** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if a dialer is detected. You can now simply delete the potentially unwanted 0190/0900 dialer. However, if it is a wanted dial-up program, you can declare it an exceptional file and this file is then no longer scanned in future.

Double Extension Files

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Your Avira product recognizes "Double Extension Files". If the option **Double Extension files** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such files.

Fraudulent software

Also known as "scareware" or "rogueware", it is a fraudulent software that pretends that your computer is infected by viruses or malware. This software looks deceptively similar to professional antivirus software but is meant to raise uncertainty or to scare the user. Its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it. There are also cases when the victims are lead to believe they were attacked and they are instructed to carry out an action, which in reality is the real attack.

Your Avira product detects scareware. If the option **Fraudulent software** is enabled with a check mark in the configuration Threat categories, you receive a corresponding alert if your Avira product detects such files.

Games

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the Internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Your Avira product recognizes computer games. If the **Games** option is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects a game. The game is now over in the truest sense of the word, because you can simply delete it.

Jokes

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Thanks to the extension of its scanning and identification routines, your Avira product is able to detect joke programs and eliminate them as unwanted programs if required. If the option **Jokes** is enabled with a check mark in the configuration under Threat categories, a corresponding alert is issued if a joke program is detected.

Phishing

Phishing, also known as "brand spoofing" is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.
When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

Your Avira product recognizes "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such behavior.

Programs that violate the private domain

Software that may be able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy on your user behavior and could therefore be unwanted.

Your Avira product detects "Security Privacy Risk" software. If the option **Programs that violate the private domain** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such software.

Unusual Runtime Packers

Files that have been compressed with an unusual runtime packer and that can therefore be classified as potentially suspicious.

Your Avira product recognizes "Unusual runtime packers". If the option **Unusual runtime packers** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such packers.

13.2 Viruses and other malware

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Backdoors

A backdoor can gain access to a computer by bypassing the computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help. But are mainly used to install further computer viruses or worms on the relevant system.

Boot viruses

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more…

Bot-Net

A bot-net is defined as a remote network of PCs (on the Internet) that is composed of bots that communicate with each other. A bot-net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-nets serve various purposes, including denial-of-service attacks etc., usually without the affected PC user's knowledge. The main potential of bot-nets is that the networks can achieve grow to thousands of computers and their total bandwidth exceeds most conventional Internet accesses.

Exploit

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. One form of exploitation for example is an attack from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

Fraudulent software

Also known as "scareware" or "rogueware", it is a fraudulent software that pretends that your computer is infected by viruses or malware. This software looks deceptively similar to professional Antivirus software but is meant to raise uncertainty or to scare the user. Its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it. There are also cases when the victims are lead to believe they were attacked and they are instructed to carry out an action, which in reality is the real attack.

Hoaxes

For several years, Internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread via email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

Honeypot

A honeypot is a service (program or server) installed in a network. Its function is to monitor a network and log attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a honeypot, it is logged and an alert is triggered.

Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses consequently do not attack executable files but they do attack the documents of the corresponding host application.

Pharming

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

Phishing

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that: banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

Polymorph viruses

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

Program viruses

A computer virus is a program that is capable of attaching itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits its virulent code. The program execution of the host itself is not changed as a rule.

Rootkits

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

Script viruses and worms

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms cannot consequently form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

Spyware

Spyware are so called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

Trojan horses (short Trojans)

Trojans are pretty common nowadays. Trojans include programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

Zombie

A zombie PC is a computer that is infected with malware programs and that enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

14. Info and Service

This chapter contains information on how to contact us.

- see Chapter Contact address
- see Chapter Technical support
- see Chapter Suspicious files
- see Chapter Reporting false positives
- see Chapter Your feedback for more security

14.1 Contact address

If you have any questions or requests concerning the Avira product range, we will be pleased to help you. For our contact addresses, please refer to the Control Center under **Help > About Avira Professional Security**.

14.2 Technical support

Avira support provides reliable assistance in answering your questions or solving a technical problem.

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

http://www.avira.com/professional-support

So that we can provide you with fast, reliable help, you should have the following information ready:

- **License information**. You can find this information in the program interface under the menu item **Help > About Avira Professional Security > License information**. See License information.
- **Version information**. You can find this information in the program interface under the menu item **Help > About Avira Professional Security > Version information**. See Version information.
- **Operating system version** and any Service Packs installed.
- **Installed software packages**, e.g. anti-virus software of other vendors.
- **Exact messages** of the program or of the report file.

14.3 Suspicious files

Suspect files or viruses that may not yet be detected or removed by our products can be sent to us. We provide you with several ways of doing this.

- Identify the file in the quarantine manager of the Control Center and select the item **Send file** via the context menu or the corresponding button.
- Send the required file packed (WinZIP, PKZip, Arj, etc.) in the attachment of an email to the following address:
  virus-professional@avira.com
  As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).
- You can also send us the suspicious file via our website: http://www.avira.com/sample-upload

14.4 Reporting false positives

If you believe that your Avira product is reporting a detection in a file that is most likely "clean", send the relevant file packed (WinZIP, PKZip, Arj, etc.) as an email attachment to the following address:

virus-professional@avira.com

As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

14.5 Your feedback for more security

At Avira, our customers' security is paramount. For this reason, we don't just have an in-house expert team that tests the quality and security of every Avira solution before the product is released. We also attach great importance to the indications regarding security relevant gaps that could develop and we treat those seriously.

If you think you have detected a security gap in one of our products, please send us an email to the following address:

vulnerabilities-professional@avira.com

Avira

Issued Q4-2013

Avira | Kaplaneiweg 1 | 88069 Tettnang | Germany | Telephone: +49 7542-500 0
www.avira.com