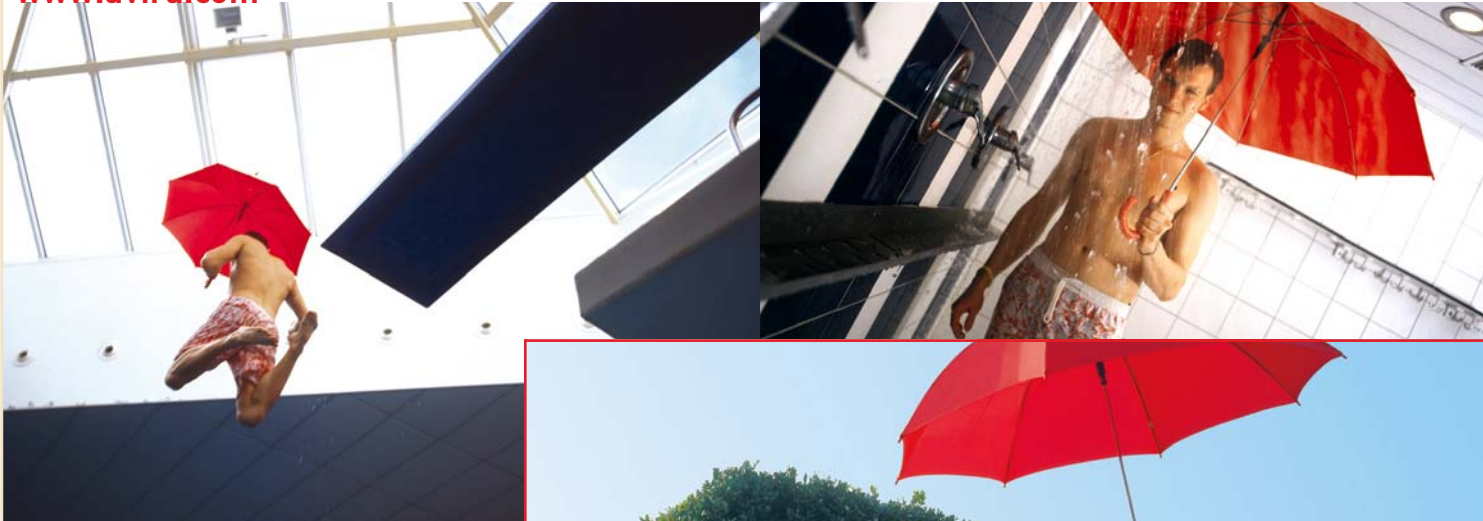


www.avira.com



User Manual

Avira AntiVir

PersonalEdition Classic

Trademarks

AntiVir is a registered trademark of the Avira GmbH.

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

The purpose of this information is to acknowledge and recognize the code from third-party suppliers used for Avira AntiVir PersonalEdition Classic. We would like to thank the copyright owners for allowing us to use their code.

MD5 code

The MD5 code used for security reasons was written by the Information Science Institute of the University of Southern California and derived from the Message-Digest algorithm from RSA Data Security, Inc.

Copyright (C) 1991-2, RSA Data Security, Inc., Created in 1991.

All rights reserved.

The license to copy and use this software is distributed with the stipulation that it is designated as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all materials mentioned by this software or which refer to this software or these functions.

The license is also granted for the creation of works deriving from this, with the stipulation that these works are designated as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all materials which mention the derived work or refer to it.

RSA Data Security, Inc. provides no warranty whatsoever regarding the marketability of this software or the suitability of this software for a particular purpose. It is provided without any guarantee in its present form. This applies to expressed or implied guarantees.

This information must be contained in every copy of each part of this documentation and/or software.

Expat

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

ScewXML

Copyright (C) 2002, 2003 Aleix Conchillo Flaque: SCEW is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version: <http://www.gnu.org/copyleft/lesser.html>

Publisher

Avira GmbH

D-88069 Tettnang, Lindauer Str. 21

Phone: +49 (0) 7542 - 500 0

Fax: +49 (0) 7542 - 525 10

Email: info@avira.com

Internet: <http://www.free-av.com>

Production

Avira GmbH

D-88069 Tettnang, Lindauer Str. 21

Copyright © 2007 Avira GmbH

This manual was created with great care. However, errors in design and contents cannot be excluded.

All rights reserved. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued: April 2007

Table of Contents

1	Introduction	5
2	Symbols, emphases and terms	6
3	Product information.....	8
3.1	Delivery scope	8
3.2	System requirements.....	9
4	Installation and deinstallation	10
4.1	Installation.....	10
4.1.1	Requirements for an installation	10
4.1.2	Installation	10
4.2	Deinstallation	13
5	Configuration.....	14
5.1	Configuring basic settings.....	15
5.1.1	Configuring working directories	15
5.1.2	Protecting configuration file and jobs	16
5.1.3	Configuring update alert	17
5.2	Configuring AntiVir Guard	18
5.2.1	Configuring scan mode of on-access scan.....	18
5.2.2	Configuring check of drives during on-access scan.....	19
5.2.3	Selecting file types for on-access scan.....	19
5.2.4	Selecting check of runtime-compressed files for on-access scan.....	21
5.2.5	Configuring exceptions from on-access scan.....	21
5.2.6	Configuring heuristic for on-access scan	22
5.2.7	Configuring actions of on-access scan in case of a detection	23
5.2.8	Configuring report of on-access scan.....	23
5.3	Configuring AntiVir Scanner	25
5.3.1	Configuring check of boot sectors and memory during on-demand scan	25
5.3.2	Configuring rootkit scan during on-deman-scan	26
5.3.3	Configuring priority of on-demand scan	26
5.3.4	Allowing stops during on-demand scan.....	27
5.3.5	Selecting file types for on-demand scan	27
5.3.6	Configuring check of archives during on-demand scan	28
5.3.7	Configuring exceptions from on-demand scan	29
5.3.8	Configuring heuristic for on-demand scan.....	30
5.3.9	Configuring actions of on-demand scan in case of a detection	31
5.3.10	Configuring report of on-demand scan	32
5.4	Configuring scan for extended threat categories.....	33
5.5	Configuring email settings.....	33
5.6	Configuring Avira AntiVir PersonalEdition Classic Updater.....	34
5.6.1	Configuring update via a web server.....	34
5.7	Configuring events	36
5.7.1	Selecting program module for displaying events	36
5.7.2	Selecting filters for specific events.....	36
5.7.3	Limiting the size of the event data	37

6	Scanning	38
6.1	Checking active files (on-access scan)	38
6.2	Targeted scan for viruses and malware (on-demand scan)	38
6.2.1	Scanning for viruses and malware via a scan profile.....	39
6.2.2	Scanning for viruses and malware via drag&drop.....	41
6.2.3	Scanning for viruses and malware via the pop-up menu	42
6.2.4	Scanning for viruses and malware automatically.....	42
6.3	Targeted scan for active rootkits (on-demand scan).....	43
6.4	Reacting to found viruses and malware	44
6.4.1	Reacting to viruses and malware in an archive file	45
6.5	Handling files in quarantine	45
6.5.1	Handling files in quarantine (*.qua)	45
6.5.2	Restoring files in quarantine	46
6.6	Moving suspicious file to quarantine	47
7	Updating	48
7.1	Updating Avira AntiVir PersonalEdition Classic automatically	48
7.2	Updating Avira AntiVir PersonalEdition Classic manually	50
8	Service	51
8.1	Frequently Asked Questions (FAQ).....	51
8.2	Help in case of a problem	53
8.3	Forum.....	55
8.4	Service hotline	55
8.4.1	Preparing your request	55
8.5	Online shop.....	55

1 Introduction

Avira AntiVir PersonalEdition Classic from Avira GmbH protects your computer from viruses, malware, adware and spyware, undesired programs and other dangers. These will be referred to as viruses and malware in this manual .

The manual describes the installation and use of the program.



On our website, <http://www.free-av.com>, you can download the manual for Avira AntiVir PersonalEdition Classic as a PDF file, update Avira AntiVir PersonalEdition Classic or find more information on the pay version Avira AntiVir PersonalEdition Premium that offers even more functionality.

Our website also contains information such as the telephone number for technical support and our newsletter, for which you can sign up there.

Your Avira GmbH team

2 Symbols, emphases and terms

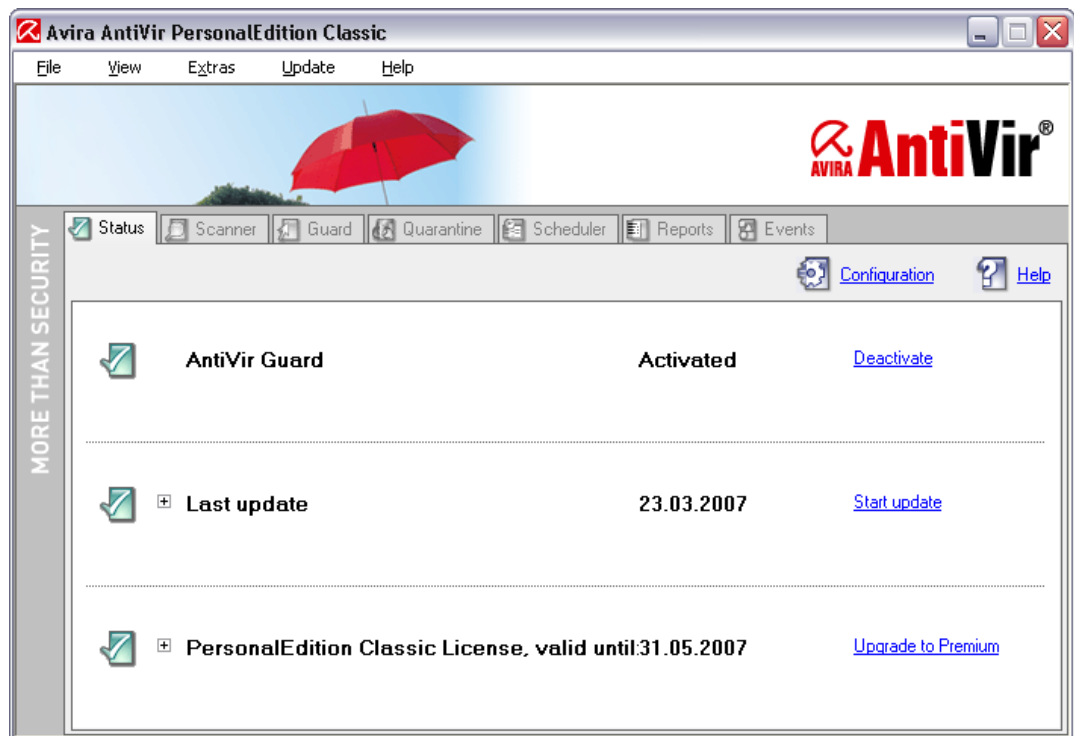
The following symbols are used:

Symbol	Explanation
✓	Appears before a condition which must be met before an action is carried out.
▶	Appears before a step you carry out.
→	Appears before a result that follows the preceding action.
	Appears before a warning of the danger of critical data loss.
	Appears before a note with especially important information or a tip which makes it easier to understand and use the Avira AntiVir PersonalEdition Classic.

The following emphases are used:

Emphasis	Explanation
<i>Italic</i>	File name or path.
	Elements of the software interface which are displayed (e.g., window title, window area or option).
Bold	Elements of the software interface which are clicked (e.g., menu item, tab or button).

The window which opens when the program is started; referred to as *Control Center* in the following (see figure).



3 Product information

Avira AntiVir PersonalEdition Classic is a comprehensive and flexible tool for reliable protection of your computer from viruses, malware, undesired programs and other dangers.

► Note the following:



The loss of valuable data usually has serious consequences. Even the best anti-virus program cannot provide 100% protection against data loss.

► Back-up your data on a regular basis.



A program which protects against viruses, malware, undesired programs and other dangers is only reliable and effective when it is kept up-to-date.

► Ensure that Avira AntiVir PersonalEdition Classic is always up-to-date with automatic updates. Configure the program accordingly.

3.1 Delivery scope

- Control Center for monitoring, administration and control of the entire program
- Central configuration with user-friendly standard and expert configurations and context-sensitive help
- Integration with the Windows Vista User Account Control in order to be able to perform tasks which require administrator rights.
- Scanner (on-demand scan) with profile-based and configurable scans for all known virus and malware types
- Guard (on-access scan) for constant monitoring of all file accesses
- Rootkit Detection for detecting malware which was installed secretly in the computer's system (so-called Rootkits)
- Integrated quarantine management for containment and handling of suspicious files
- Direct access to detailed information on found viruses and malware via the Internet
- Quick and easy updating of the program and virus definitions (VDF), of the search engine via Single File Update and incremental VDF update via a web server on the Internet
- Integrated Scheduler for the scheduling of single or recurring tasks such as updates and test runs
- Extremely high rate of virus and malware detection thanks to innovative scanning technologies (search engine) with heuristic scanning
- Detection of all common archive types including detection of nested archives and smart extension detection
- High performance via multi-threading capability (simultaneous scanning of many files at high speed)

3.2 System requirements

In order for Avira AntiVir PersonalEdition Classic to run properly, the computer system must fulfill the following requirements:

- Computer: Pentium or higher, at least 133 MHz
- Operating system
 - Microsoft Windows Vista (32 bit), or
 - Microsoft Windows XP, or
 - Microsoft Windows 2000, SP 4 recommended



Avira AntiVir PersonalEdition Classic also supports the Microsoft Windows XP x64 Edition.



The display of the program interfaces can differ, depending on the operating system used.

- RAM
 - 196 MB RAM (Windows XP and Windows 2000)
 - 512 MB RAM (Windows Vista (32 bit))
- 50 MB free memory on the hard disk (more if quarantine is used)
- 100 MB temporary memory on the hard disk
- 25 MB of free main memory
- For all installations: Internet Explorer 5.0 or higher
- For the installation of Avira AntiVir PersonalEdition Classic: administrator rights



When installing under Microsoft Windows Vista, the User Account Control of Microsoft Windows Vista separately asks for and approves the required administrator rights, which are needed for certain actions (e.g., installation or search runs).

You will get further information on the Windows User Account Control and the approval of administrator rights in the operating system manual.

4 Installation and deinstallation

4.1 Installation

4.1.1 Requirements for an installation

- ▶ Ensure that the following requirements are fulfilled so that Avira AntiVir PersonalEdition Classic works properly on your computer:
 - ✓ System requirements fulfilled
 - ✓ No other virus protection programs installed
 - ✓ Installer has administrator rights
 - ✓ All running programs on the computer exited

4.1.2 Installation



Danger of data loss and damage to the operating system of the computer!

- ▶ Do not install any other virus protection programs or comparable services on the computer on which Avira AntiVir PersonalEdition Classic is installed.
- ▶ If necessary, deinstall any such programs or services.
- ▶ Close all running programs before installation.

-
- ▶ Go to the website <http://www.free-av.com>.
 - ▶ Follow the instructions to download Avira AntiVir PersonalEdition Classic.
 - ▶ Double-click the program file *.exe.



Under Windows Vista the dialog box *User account control* is displayed.

- ▶ If applicable, sign on as administrator.
- ▶ Click on **Continue**.

-
- ↳ The dialog box of the setup program is displayed after a safety prompt confirming the publisher of the software.
 - ▶ Click **Accept**.
 - ↳ The setup program for Avira AntiVir PersonalEdition Classic starts.
 - ▶ Click **Next**.
 - ↳ The *Welcome* dialog box is displayed.
 - ▶ Click **Next**.
 - ↳ The *More threat categories* dialog box containing information on basic and advanced protection is displayed.
 - ▶ Click **Next**.
 - ↳ The dialog box with the license agreement is displayed.

- ▶ Confirm that you accept the license agreement and click **Next**.
 - ↳ The *Private Use* dialog box is displayed.
- ▶ Confirm that you will use Avira AntiVir PersonalEdition Classic solely for private purposes and not for commercial reasons and click **Next**.
 - ↳ The *Generate Serial Number* dialog box is displayed.
- ▶ If appropriate, confirm that a random serial number is to be generated and transferred with an update and click **Next**.
 - ↳ The *Choose Installation Type* dialog box is displayed.
- ▶ Decide whether you would like a complete or custom installation.
- ▶ Activate the **Complete** or **Custom** option and confirm with **Next**.
- ▶ For a complete installation: Skip the next two steps.

For a custom installation:

- ↳ The *Choose Destination Folder* dialog box is displayed.
- ▶ Confirm the specified destination folder with **Next**.
 - OR -
 - Select another destination folder with **Browse** and confirm with **Next**.
 - ↳ The *Install Components* dialog box is displayed:
 - The components have the following functions:
 - *AntiVir PersonalEdition Classic*: AntiVir Scanner. Always installed
 - *AntiVir Guard*: Constant monitoring of all file accesses in real-time (on-access scanner)
 - *AntiVir Rootkit Protection*: module for detecting secretly installed malware
 - *Shell Extension*: Direct checking of files in Windows Explorer
- ▶ Activate or deactivate the desired components and confirm with **Next**.
 - ↳ In the following dialog box, you can specify whether to activate Win32 file heuristic.
- ▶ Click **Next**.
 - ↳ In the following dialog box, you can specify whether a link is to be created on your desktop and/or a program group in the Start menu.
- ▶ Click **Next**.

Complete and custom installations continued:

- ↳ The set-up program asks whether the *readme.txt* file with current information on Avira AntiVir PersonalEdition Classic is to be displayed.
- ▶ Agree, if appropriate, and click **Finish**.
 - ↳ The setup program completes the installation and places a shortcut on the desktop, if appropriate.
 - ↳ The file *readme.txt* is displayed, if appropriate.
 - ↳ You are asked if you want to perform an update.



Only the latest version of Avira AntiVir PersonalEdition Classic can reliably protect you against continuous new threats from viruses and malware.

- ▶ Perform an update immediately after installation.
 - ↳ The Windows Security Center (XP and Vista) indicates that Avira AntiVir PersonalEdition Classic is *ACTIVE* after this initial update.

- OR -

- ↳ You are asked whether the computer is to be restarted.

If you would like to perform an update:

- ▶ Confirm with **Yes**.
 - ↳ An update for the Avira AntiVir PersonalEdition Classic is sought via an existing web server connection.
 - ↳ The Avira AntiVir PersonalEdition Classic then automatically starts by scanning the Windows system directories.



The first scan is particularly important in order to ensure that your system is free of viruses and malware.

- ▶ Do not abort the first scan.

If you would like to restart the computer:

- ▶ Confirm with **Yes**.
 - ↳ The computer is restarted.

4.2 Deinstallation

To deinstall Avira AntiVir PersonalEdition Classic (using Windows XP and Windows Vista for the example):

- ▶ Open the **Control Panel** via the Windows **Start** menu.
- ▶ Double-click **Add or Remove Programs** (Windows Vista: **Programs**).
- ▶ Select **Avira AntiVir PersonalEdition Classic** and click **Remove** (Windows Vista: **Uninstall**).



Under Windows Vista the dialog box *User account control* is displayed.

- ▶ If applicable, sign on as administrator.
- ▶ Click on **Continue**.

-
- ↳ You are asked whether you do indeed want to remove the program.
 - ▶ Confirm with **Yes**.
 - ↳ All components of the program are removed.
 - ▶ Click **Finish** to complete the deinstallation.
 - ↳ A dialog box suggesting that you restart the computer may be displayed.
 - ▶ Confirm with **Yes**.
 - ↳ Avira AntiVir PersonalEdition Classic is deinstalled, your computer is restarted, if necessary, and all directories, files and registry entries from Avira AntiVir PersonalEdition Classic are deleted.

5 Configuration

As standard, Avira AntiVir PersonalEdition Classic is configured with sensible settings which are commonly used.

Avira AntiVir PersonalEdition Classic offers a large number of options for configuring protection against viruses and malware and for configuring the responses of the components in case of a detection and adapting them to your needs. The basic functions can be configured in Standard mode, and additional functions are available in Expert mode.

With the AntiVir Guard, your computer is continually protected and all data are checked as soon as they are accessed while you are working (on-access).

- See Chapter: Configuring AntiVir Guard

With the AntiVir Scanner, your computer can be scanned directly for viruses and malware and individual files or whole directories of your computer can be checked as desired (on-demand).

- See Chapter: Configuring AntiVir Scanner

With all modules, you can configure whether extended threats are to be scanned for as well:

- See Chapter: Configuring scan for extended threat categories

Suspicious files can be sent for analysis to Avira Malware Research Center. Therefore it is necessary to specify the email settings.

- See Chapter: Configuring email settings

The working directories and security settings of Avira AntiVir PersonalEdition Classic can be adapted to your needs if necessary:

- See Chapter: Configuring basic settings

To ensure regular updating of Avira AntiVir PersonalEdition Classic, you can configure the Avira AntiVir PersonalEdition Classic Updater:

- See Chapter: Configuring Avira AntiVir PersonalEdition Classic Updater

If necessary, you can adapt the display of events generated by the modules of Avira AntiVir PersonalEdition Classic to your requirements (in the same way as the events display of your Windows operating system):

- See Chapter: Configuring events

5.1 Configuring basic settings

You can adapt the default working directory of Avira AntiVir PersonalEdition Classic created during installation to your needs:

- See Chapter: Configuring working directory

You can protect the configuration file from undesired modifications:

- See Chapter: Protecting configuration file and jobs

In the Control Center and the Windows XP Security Center (WSC), you can have an alert displayed if a certain number of days have passed since the last update of Avira AntiVir PersonalEdition Classic.

- See Chapter: Configuring update alert

5.1.1 Configuring working directories




Data loss!

Data in existing working directories are not copied to the new working directories.

The working directories must only be changed by experienced persons.

To set the working directories of Avira AntiVir PersonalEdition Classic:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **General** tab and then **Directories**.
- ▶ Select the directory in the *Temporary path* section:
 - Activate the **Use default system settings** option.
 - ↳ The Windows TEMP directory is used as temporary directory.
 - OR -
 - Activate the **Use following directory** option and enter a directory.
 - OR -
 - Click  to select the directory.

If you would like to restore the default directories:

- ▶ Click **Default** in the respective section.

5.1.2 Protecting configuration file and jobs

To specify whether the configuration file of the Avira AntiVir PersonalEdition Classic is to be protected:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **General** tab and then **Security**.
- ▶ Activate the **Protect configuration** option in the *Protect configuration file against unwanted modifications* section.
 - ↳ If the option is activated, the configuration file can only be saved if the user has administrator rights. Users with limited access to the computer thus cannot modify and save the configuration.



This option is only available if Avira AntiVir PersonalEdition Classic is installed on a NTFS partition.

To specify that scan and update jobs are to be protected:

- ▶ Activate the **Protect job files** option in the *Protect configuration file against unwanted modifications* section.



Under Windows Vista: After confirming with **OK** the dialog box *User account control* is displayed.

- ▶ If applicable, sign on as administrator.
 - ▶ Click on **Continue**.
-

- ↳ If the option is activated, only a user with administrator rights can change, create and delete update and scan jobs. Users with limited access to the computer do not have access.



If the option is deactivated, all users can change, create and delete update and scan jobs, regardless of their user rights.

5.1.3 Configuring update alert

To specify the number of days after which an alert is to appear in the Control Center and Security Center of Windows XP if Avira AntiVir PersonalEdition Classic has not been updated:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **General** tab and then **Security**.
- ▶ Select the number of days in the list field of the *Update* section.

The program accepts values between 1 and 30.

If a dialog box with a security warning is also to be displayed once the time specified above elapses:

- ▶ Activate the **Show notice if the virus definition file is out of date** option.

5.2 Configuring AntiVir Guard

Normally, you would want to monitor your system constantly. The on-access scanner of the AntiVir Guard is used for this purpose. In this way, all files on the computer are scanned for viruses and malware as soon as they are opened, read, executed or written to.

You can configure the following settings in Standard mode:

- See Chapter: Configuring scan mode of on-access scan
- See Chapter: Configuring check of drives during on-access scan
- See Chapter: Selecting file types for on-access scan

You can configure the following additional settings in Expert mode:

- See Chapter: Selecting check of runtime compressed files for the on-access scan (additional details)
- See Chapter: Selecting file types for on-access scan (additional details)
- See Chapter: Configuring exceptions from on-access scan
- See Chapter: Configuring heuristic for on-access scan
- See Chapter: Configuring actions of on-access scan in case of a detection
- See Chapter: Configuring report of on-access scan

In addition, you can configure whether the AntiVir Guard scans for extended threat categories in case of a detection.

- See Chapter: Configuring scan for extended threat categories

5.2.1 Configuring scan mode of on-access scan

To specify the situations in which AntiVir Guard is to scan files and programs:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ In the *Scan* section, specify the situation in which files and programs are scanned.
 - **Scan when reading**
Files and programs are scanned before they are read or executed by an application or the operating system.
 - **Scan when writing**
Files and programs are checked upon writing. The file cannot be accessed until this process is completed.

- **Scan when reading and writing**

Files and programs are scanned before opening, reading and executing and after writing. This setting is activated by default.



We recommend activating the *Scan when reading and writing* option. This provides maximum security.

An internal cache ensures that the files are checked only once. This guarantees maximum performance.

5.2.2 Configuring check of drives during on-access scan

To specify the drives to be scanned by the AntiVir Guard:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Specify the drives to be scanned in the *Drives* section:
 - **Local drives**
E.g., hard disks, CD drives, floppy drives, MO drives, ZIP drives
This setting is activated by default.



We recommend activating the *Local drives* option.

5.2.3 Selecting file types for on-access scan

Selecting file types for on-access scan

To specify the file types to be scanned by the AntiVir Guard:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Specify the file types to be scanned in the *Files* section:
 - **All files**
All files and programs are scanned. (If *All files* is active, the *File Extensions* button cannot be clicked.)
 - **Use smart extensions**
Avira AntiVir PersonalEdition Classic selects the file types itself using the content. This process is slightly slower than using the file extension list, but is more secure, since files are not only checked or not checked depending on their extension. (If *Use smart extensions* is active, the *File Extensions* button cannot be clicked.)

– Use file extension list

Only certain file types are scanned. By default, all the file types which can contain viruses and malware are set.



▶ Please note that the file extension list can vary from version to version.

If you activate the *Use file extension list* option, we recommend using all file types which are set by default.

The file extension list can be edited via the **File extensions** button:

- See Chapter: Configuring list of file types for on-access scan

Configuring list of file types for on-access scan

To edit the file extension list:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Activate the **Use file extension list** option in the *Files* section.
- ▶ Click **File extensions**.
 - ↳ The *File extensions* dialog box is displayed.

If you want to insert a new file extension:

- ▶ Click **Insert [Ins]**.
 - You can enter a maximum of 10 characters (without preceding dot). Wildcards (* and ?) are acceptable.
 - ↳ The *Insert extension* dialog box is displayed.
- ▶ Enter a new file extension and confirm with **OK**.
 - ↳ The *Insert extension* dialog box is closed.
- ▶ Confirm with **OK**.
 - ↳ The *File Extensions* dialog box is closed.
 - ↳ The new file extension is included in the list.

If you want to remove a file extension from the list:

- ▶ Select the extension to be deleted in the *File extensions* dialog box and click **Delete [Del]** and confirm with **OK**.
 - ↳ The file extension is deleted from the list.

If you want to reset the list to the default:

- ▶ Click in the *File extensions* dialog box on **Default** and confirm with **OK**.
 - ↳ The default settings are restored.

5.2.4 Selecting check of runtime-compressed files for on-access scan

To specify whether the AntiVir Guard is to check runtime-compressed files:

This option is activated by default.

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Activate the **Unpack runtime compressed files** option in the *Archive* section.
 - ↳ Runtime compressed files are unpacked and checked during the on-access scan.

5.2.5 Configuring exceptions from on-access scan

Certain processes (*.exe files) and file objects can be omitted from the on-access scan in order to avoid collisions during parallel file accessing, e.g., during database queries or backup processes. In this case, all the files which are accessed by one of the specified processes are not checked.



Danger of data loss and damage to the operating system of the computer!

Processes and file objects to be omitted and all files accessed by such processes are not checked for viruses and malware.

- ▶ Check file objects for viruses and malware before adding them to the list of file objects to be omitted.



A long list of entries can affect the performance of your system.

- ▶ Keep the list as short as possible.

To specify which processes and file objects of the AntiVir Guard are to be omitted from the scan:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Exceptions** tab.



- ▶ Observe the information in the online help texts of the Avira AntiVir PersonalEdition Classic when entering processes and files to be omitted.

If you want to add a process to be omitted:

- ▶ Enter the name of the process in the input field of the *Processes to be omitted for the Guard* section.

You can specify up to 12 processes. The exact names of the processes are found in the Windows Task Manager. Windows Explorer and the operating system cannot be omitted from the on-access scan. A corresponding entry will be ignored.

Only the first 16 characters of the process name (inclusive file extension) are considered. If there exist 2 processes whose names match the first 16 characters, Guard excludes both processes from the monitoring.

- ▶ Click **Add**.
 - ↳ The name of the process is listed in the display window.

If you want to add a file object to be omitted:

- ▶ Enter the name of the file object in the input field of the *File objects to be omitted for the Guard* section.

All entries together must not exceed 6,000 characters.

Wildcards (* and ?) are only allowed in file names. Directory names must be concluded with "\". File names may not be concluded with "\".

Example for file name: c:\temp\program*.exe

Example for directory name: c:\temp\program_test\

- ▶ Click **Add**.
 - ↳ Select the file object or process in the appropriate display window.

If you want to include a file object or a process in the on-access scan again:

- ▶ Select the file object or process in the appropriate display window.
- ▶ Click **Delete**.
 - ↳ The name of the file object or process is removed from the display window.

5.2.6 Configuring heuristic for on-access scan

The macrovirus heuristic can also detect unknown (new) macroviruses and other malware (e.g., in Microsoft Office documents such as Word or Excel). For this purpose, the code of the macro is examined for functions typical for viruses. If a macro fulfills characteristic features, it is reported as suspicious.

The Win32 file heuristic can also detect unknown file viruses, worms and trojans in executable files (*.exe, *.dll) of Windows.

To specify the heuristic to be used by the AntiVir Guard:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Heuristic** tab.
- ▶ Activate the **Macrovirus heuristic** option in the *Macrovirus heuristic* section.

- ▶ Activate the **Win32 file heuristic** option in the *Win32 file heuristic* section.
- ▶ Select the detection level for the file heuristic:
 - **Low detection level**
The heuristic detects slightly fewer viruses, worms, trojans and other malware. This means that the risk of false alarms is very low.
 - **Medium detection level**
Default setting.
 - **High detection level**
The heuristic detects most unknown viruses, worms, trojans and other malware. Thus false alarms are also possible.

5.2.7 Configuring actions of on-access scan in case of a detection

To specify how the AntiVir Guard is to act if viruses and malware are found:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Action for concerning files** tab.
- ▶ Select the action to be carried out in the *Action for concerning files* section:
 - **Interactive**
A dialog box is displayed and allows you to select further actions yourself in case of a detection.



In the Avira AntiVir PersonalEdition Classic this option is enabled as the default setting and is not changeable.

Information on how you can respond to a detection and configure other measures is contained in the following chapters:

- See Chapter: Reacting to found viruses and malware

5.2.8 Configuring report of on-access scan

To specify how the AntiVir Guard is to report the results of the on-access scan:

- ▶ Select the **Guard** tab in the Control Center.
- ▶ Click the **Configuration** link.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *Guard / Scan* tab.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Report** tab.

- ▶ Select the scope of the entries in the report file in the *Reporting* section:
 - **Off**
No report file is generated.
 - **Default**
Only important information (on finds, alerts and errors) is recorded in the report file.
 - **Extended**
Additional information is recorded in the report file.
 - **Complete**
All information is recorded in the report file (including file size, file type date etc.).



With the option *Complete*, the size of the report file grows large very quickly and can take up great amounts of memory on your computer.

- ▶ Activate this option **only if instructed to do so by our technical support** and not for a longer period of time.
-

- ▶ Select the size of the report file in the *Limit report file* section.
By default, the report file is limited to 1 MB. You can enter a value up to 100 MB.
- ▶ Activate additional desired options for the report file in the *Limit report file* section.
 - **Backup report file before shortening**
The report file is backed up before being shortened in the report directory.
 - **Write configuration in report file**
The configuration of the on-access scan is added to the report file.

5.3 Configuring AntiVir Scanner

The on-demand scan with the AntiVir Scanner is used to specifically check one or more files and programs, but also directories and archives, drives and boot sectors, even if you are not currently accessing them.

You can configure the following settings in Standard mode:

- See Chapter: Configuring check of boot sectors and memory during on-demand scan
- See Chapter: Configuring rootkit scan during on-demand scan
- See Chapter: Selecting file types for on-demand scan
- See Chapter: Configuring check of archives during on-demand scan

You can configure the following additional settings in Expert mode:

- See Chapter: Configuring priority of on-demand scan
- See Chapter: Allowing stops during on-demand scan
- See Chapter: Configuring details for checking of archives during on-demand scan
- See Chapter: Configuring exceptions from on-demand scanning
- See Chapter: Configuring heuristic for on-demand scan
- See Chapter: Configuring actions of on-demand scan in case of a detection
- See Chapter: Configuring report of on-demand scan

In addition, you can configure whether the AntiVir Scanner scans for extended threat categories:

- See Chapter: Configuring scan for extended threat categories

5.3.1 Configuring check of boot sectors and memory during on-demand scan

To specify whether only boot sectors and memory are to be checked during on-demand scan:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Select the **Scanner** tab and then **Scan**.

If only the boot sectors of the drives selected for the on-demand scan are to be checked:

- ▶ Activate the **Scan boot sectors of selected drives** option in the *Additional settings* section.

This setting is activated as default and is recommended.

If the boot sectors of all drives are to be checked:

- ▶ Deactivate the **Scan boot sectors of selected drives** option in the *Additional settings* section.

If the memory of the computer is to be checked during each on-demand scan:

- ▶ Activate the **Scan memory** option in the *Additional settings* section.



If viruses and malware are active in memory, all files which are checked can be infected.

We recommend activating the *Scan memory* option.

If offline files are not to be scanned for viruses and malware

(files that have been physically moved from the hard disc to a tape, for example, via a so-called hierarchical storage management system (HSMS)):

- ▶ Activate the **Ignore offline files** option in the *Additional settings* section.

5.3.2 Configuring rootkit scan during on-demand scan

To specify whether active rootkits are scanned during on-demand scan:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Select the **Scanner** tab and then **Scan**.
- ▶ In the area *Additional settings* activate the option **Rootkit search on search start**.

5.3.3 Configuring priority of on-demand scan

To specify the priority with which the AntiVir Scanner is to perform the on-demand scan:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab and then **Scan**.
- ▶ Select the priority with which the on-demand scan is to be performed in the *Scan process* section.

- **Low**

The on-demand scan is only allocated processor time by the operating system if no other process requires computation time, i.e. as long as only the on-demand scan 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 on-demand scan continues running in the background.

This setting is activated as default and is recommended.

- **Normal**

The on-demand scan is performed with normal priority. All processes are allocated the same amount of processor time by the operating system. Under certain circumstances, work with other applications may be affected.

- **High**

The on-demand scan has the highest priority. Simultaneous work with other applications is almost impossible. The on-demand scan completes its scan at maximum speed, however.

5.3.4 Allowing stops during on-demand scan

To specify whether a running on-demand scan can be stopped:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab and then **Scan**.

If you would like to stop a running on-demand scan at any time:

- ▶ Activate the **Allow stopping the scanner** option in the *Scan process* section.
 - ↳ You can stop the on-demand scan via the **Stop** button in the *Luke Filewalker* dialog box at any time.

If it should not be possible to stop a running on-demand scan:

- ▶ Deactivate the **Allow stopping scanner** option in the *Scan process* section.
 - ↳ The **Stop** button is displayed grayed out in the *Luke Filewalker* dialog box. The running on-demand scan cannot be stopped.

5.3.5 Selecting file types for on-demand scan

Selecting file types for on-demand scan

To specify the file types to be scanned by the AntiVir Scanner:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Select the **Scanner** tab and then **Scan**.
- ▶ Specify the file types to be scanned in the *Files* section.
 - **All files**

All files and programs are scanned. (If *All files* is active, the *File Extensions* button cannot be clicked.)
 - **Use smart extensions**

The Avira AntiVir PersonalEdition Classic selects the file types itself using the content. This process is somewhat slower than using the file extension list, but is more secure, since files are not only checked or not checked depending on their extension. This setting is activated as default and is recommended. (If *Use smart extensions* is active, the *File Extensions* button cannot be clicked.)
 - **Use file extension list**

Only certain file types are scanned. By default, all the file types which can contain viruses and malware are set.



- ▶ Please note that the file extension list can vary from version to version.

If you activate the *Use file extension list* option, we recommend using all file types which are set by default.

The list can be edited via the **File extensions** button:

- See Chapter: Configuring list of file types for on-demand scan

Configuring list of file types for on-demand scan

To edit the file extension list:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Select the **Scanner** tab and then **Scan**.
- ▶ Activate the **Use file extension list** option in the *Files* section.
 - ↳ The *File extensions* dialog box is displayed.

If you want to insert a new file extension:

- ▶ Click **Insert [Ins]**.

You can enter a maximum of 10 characters (without preceding dot). Wildcards (* and ?) are acceptable.

 - ↳ The *Insert extension* dialog box is displayed.
- ▶ Enter a new file extension and confirm with **OK**.
 - ↳ The *Insert extension* dialog box is closed.
- ▶ Confirm with **OK**.
 - ↳ The *File extensions* dialog box is closed.
 - ↳ The new file extension is included in the list.

If you want to remove a file extension from the list:

- ▶ Select the extension to be deleted in the *File extensions* dialog box and click **Delete [Del]** and confirm with **OK**.
 - ↳ The file extension is deleted from the list.

If you want to reset the list to the default:

- ▶ Click in the *File extensions* dialog box on **Default** and confirm with **OK**.
 - ↳ The default settings are restored.

5.3.6 Configuring check of archives during on-demand scan

Configuring check of archives during on-demand scan

Archives which can be checked by the AntiVir Scanner are files compressed with WinZip, WinRar or similar programs.

To specify whether the AntiVir Scanner is to scan archives:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Select the **Scanner** tab, then select **Scan** and **Archives**.
- ▶ Activate the option **Scan archives**.
 - ↳ All archive types selected in the archive list are checked during on-demand scan.

The list of archive types can also be edited in Expert mode, and the type of archive check can be configured more precisely:

- See Chapter: Configuring details for checking of archives during on-demand scan

Configuring details for checking of archives during on-demand scan

To specify which archives are checked to which depth by the AntiVir Scanner during the on-demand scan:

- ✓ *Scan archives* option is activated.
- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab, then select **Scan** and **Archives**.
- ▶ Select the archives to be checked during the on-demand scan:
 - **All archive types**
All archive types in the archive list are selected and checked.
 - **Smart Extensions**
The AntiVir Scanner detects whether a file is a compressed archive, even if the file extension deviates from the usual form.
- ▶ Click **Limit recursion depth** and select the value for the maximum recursion depth. The program accepts values from 1 to 99. 20 is set by default.



The limitation of recursion depth is recommend to save computer resources.

- ▶ Select the archive types to be checked in the archive list.
Activate or remove the check mark by clicking the box next to the archive type.

If you would like to restore the default settings for checking archives:

- ▶ Click **Default values**.
 - ↳ The predefined values for checking archives are restored.

5.3.7 Configuring exceptions from on-demand scan

Specific files and directories can be omitted from the on-demand scan. The files and directories entered in the list are listed in the report file.



File objects to be omitted are not checked for viruses and malware.

- ▶ Only omit files and directories from on-demand scan which have already been checked for viruses and malware once.
 - ▶ Check file objects for viruses and malware before adding them to the list of file objects to be omitted.
 - ▶ Check the list of files and directories regularly.
-

To specify which file objects are to be omitted by the AntiVir Scanner during scan:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab and then **Scan** and **Exceptions**.



A long list of entries can affect the performance of your system and network.

- ▶ Keep the list as short as possible.
-

If you want to add a file object to be omitted:

- ▶ Enter the name of the file object in the input field of the *File objects to be omitted for the scanner* section.

All entries together must not exceed 6,000 characters.
- ▶ Click **Add**.
 - ↳ The name of the file object is listed in the display window.

If you want to include a file object in the on-demand scan again:

- ▶ Select the file object in the corresponding display window again.
- ▶ Click **Delete**.
 - ↳ The name of the file object is removed from the display window.

5.3.8 Configuring heuristic for on-demand scan

The macrovirus heuristic can also detect unknown (new) macroviruses and other malware (e.g., in Microsoft Office documents such as Word or Excel). For this purpose, the code of the macro is examined for functions typical for viruses. If a macro fulfills characteristic features, it is reported as suspicious.

The Win32 file heuristic can also detect unknown file viruses, worms and trojans in executable files (*.exe, *.dll).

To specify the heuristic to be used by the AntiVir Scanner:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab, then select **Scan** and **Heuristic**.
- ▶ Activate the **Macrovirus heuristic** option in the *Macrovirus heuristic* section.
- ▶ Activate the **Win32 file heuristic** option in the *Win32 file heuristic* section.
- ▶ Select the detection level for the file heuristic:

- **Low detection level**

The heuristic detects slightly fewer viruses, worms, trojans and other malware. This means that the risk of false alarms is very low.

- **Medium detection level**
Default setting.
- **High detection level**
The heuristic detects most unknown viruses, worms, trojans and other malware. Thus false alarms are also possible.

5.3.9 Configuring actions of on-demand scan in case of a detection

To specify how the AntiVir Scanner is to act if viruses and malware are found:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab, then **Scan** and **Action for concerning files**.
- ▶ Select the action to be carried out in the *Action for concerning files* section:
 - **Interactive**
A dialog box is displayed and allows you to select further actions in case of a detection.
 - **Automatic**
The configured actions are carried out automatically in case of a detection.

If you select **Automatic** in the *Action for concerning files* section:

- ▶ Select the automatic actions to be carried out:
 - **Copy file to quarantine before action**
The file is copied to quarantine before the automatic actions are carried out.
 - **Primary action**
The action carried out in case of a detection.
 - **Secondary action**
The secondary action can only be selected if *Repair* was selected as the primary action. The secondary action is only carried out if the file cannot be repaired.
- ▶ Select one of the following actions:
 - **Repair**
(Can only be selected as primary action.) The file is repaired automatically.
 - **Rename**
The file is renamed.
 - **Quarantine**
The file is moved to quarantine.
 - **Delete**
The file is deleted, but can be restored.

- **Ignore**

No action is performed. The file can be accessed.



Danger of data loss and damage to the operating system of the computer!

Affected files remain on your computer if the *Ignore* option is active.

- ▶ Use the *Ignore* option in exceptional cases only.
-

If a warning sound is to be emitted when viruses and malware are found:

- ▶ Activate the **Acoustic alert** option in the *Acoustic alert* section.
 - ↳ A standard warning sound is emitted in case of a detection.
- ▶ Select any *Wave file* if you do not want to hear the standard sound.



opens the *Open* dialog box, in which you can search for the file on your computer.

- ▶ Click **Test acoustic alert** to test the warning sound.

Information on how you can respond to a detection and configure other measures is contained in the following chapters:

- See Chapter: Reacting to found viruses and malware

5.3.10 Configuring report of on-demand scan

To specify how the AntiVir Scanner is to report the results of the on-demand scan:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **Scanner** tab and then **Report**.
- ▶ Select the scope of the entries in the report file in the *Reporting* section:
 - **Off**
 - No report file is generated.
 - **Default**
 - The name of the affected file including the path is reported.
 - **Extended**
 - The name of the affected file, including path, alerts and information are reported.
 - **Complete**
 - All checked files, the affected files, including path, alerts and information are reported.

5.4 Configuring scan for extended threat categories

To specify the extended threat categories to be scanned for by the Avira AntiVir PersonalEdition Classic:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **General** tab and then **Extended threat categories**.

If the Avira AntiVir PersonalEdition Classic is to scan for all extended threat categories:

- ▶ Activate the **Select all** option in the *Selection of extended threat categories* section.
 - ↳ All threat categories in the list are selected.

If the Avira AntiVir PersonalEdition Classic is to scan for specific extended threat categories:

- ▶ Select the desired threat categories in the list.
 - Activate or remove the check mark by clicking the box next to the threat category.

5.5 Configuring email settings

To specify how the Avira AntiVir PersonalEdition Classic sends messages via email:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **General** tab and then **Email**.
- ▶ Enter the sender data in the *Email messages* section.
 - **SMTP Server**: The host name may have a maximum length of 127 characters.
Example: 192.168.1.100 or mail.testcompany.com
 - **Sender address**: Example: name@testcompany.com

If authentication at the mail server is required:

- ▶ Activate the **Use authentication** option in the *Authentication* section.
- ▶ Enter the data for logging in at the mail server in the *Authentication* section.
 - **Login name**
Name for logging in at the mail server
 - **Password**
The password is saved encrypted. Only * are displayed in the field.

5.6 Configuring Avira AntiVir PersonalEdition Classic Updater

Depending on the system environment, you can configure the Avira AntiVir PersonalEdition Classic Updater of the Avira AntiVir PersonalEdition Classic for a variety of updating procedures.

The Avira AntiVir PersonalEdition Classic Updater can perform the update directly via a web server on the Internet:

- See Chapter: Configuring update via a web server

You can also be notified when an update is past-due in the Control Center:

- See Chapter: Configuring update alert

5.6.1 Configuring update via a web server

To configure the Avira AntiVir PersonalEdition Classic Updater for updating via the Internet:

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed.
- ▶ Activate the **Expert mode** option.
 - ↳ Additional tabs and options are displayed.
- ▶ Select the **General** tab and then **Update**.
- ▶ Select the option which you would like to use for accessing the web server in the *Web server connection* section:
 - **Use existing connection (network)**
If you would like to use a network connection.
 - **Use the following connection**
If you would like to establish the connection to the web server via one of the specified connection options. The Avira AntiVir PersonalEdition Classic Updater automatically detects which connection options are available. Connection options which 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.

If you do not establish access to the web server via a network connection:

- ▶ Activate the **Use the following connection** option.
- ▶ Select a connection in the list field.
- ▶ Enter the *User name* and *Password* for the web server connection.
The password is saved encrypted. Only * are displayed in the field.

If you are using a dial-up connection for accessing the web server and want to terminate it immediately after the update:

- ▶ Activate the option **Terminate a dial-up connection that was set up for the update**.

If access to the web server is provided by a proxy server:

- ▶ Select the **Proxy** tab.
- ▶ Activate the **Use this proxy server** option in the *Proxy server* section.
- ▶ Enter the data on the proxy server (optional; if required by the proxy server):
 - **Address**
URL or IP address of the proxy server
Example: proxy.domain.com or 192.168.1.100
 - **Port**
Port number of the proxy server
Example: 8080
 - **Login name**
Name for logging in at the proxy server
 - **Login password**
Password for logging in at the proxy server. The password is saved encrypted.
Only * are displayed in the field.

5.7 Configuring events

5.7.1 Selecting program module for displaying events

You can display events generated by the modules of the Avira AntiVir PersonalEdition Classic (analogous to the event display of your Windows operating system). Modules include:

- Updater
- Guard
- Scanner
- Scheduler

- ▶ Select the **Events** tab in the Control Center.
- ▶ Activate the checkboxes of the desired modules.

- OR -

Activate the checkbox **All**  to display the events of all available modules.

- ▶ To display a selected event: Click 

- OR -

Double-click the event.

↳ A *Properties* window with the results of an action, e.g. the results of a scan, is displayed.

- ▶ To scroll through all events: Open the *Properties* window of any desired event and navigate through the events with the arrow buttons.

- ▶ To export an event: Select the event and click  .

5.7.2 Selecting filters for specific events

- ▶ Specify the event types to be displayed: information, warning, error, detection

5.7.3 Limiting the size of the event data

- ▶ Click the **Configuration** link in the Control Center.
 - ↳ The *Avira AntiVir PersonalEdition Classic Configuration* dialog box is displayed. You are presented with the *General / Events*.
 - ↳ You are asked whether Expert mode is to be activated (this option is not available in Standard mode).
- ▶ Click **Yes**.
- ▶ Specify whether the size of the event database is to be limited:
 - **Limit maximum number of events to n entries**
Values from 100 to 10,000 are possible. If the specified number of entries is exceeded, the oldest entries are deleted.
 - **Delete events older than n day(s)**
Values from 1 to 90 days are possible (default setting: 30 days).
 - **Do not limit size of event database (delete events manually)**

6 Scanning

Avira AntiVir PersonalEdition Classic offers two options for finding viruses and malware:

- See Chapter: Checking active files (on-access scan)
- See Chapter: Targeted scan for viruses and malware (on-demand scan)
- See Chapter: Targeted scan for active rootkits (on-demand scan)

In addition, you can manually move files which seem suspicious to the quarantine of the Avira AntiVir PersonalEdition Classic.

- See Chapter: Moving suspicious file to quarantine

6.1 Checking active files (on-access scan)

By default, the AntiVir Guard scans files for viruses and malware on access before they are opened, read, executed or after they have been written to.

The AntiVir Guard should be active continuously for effective protection of your computer from viruses and malware.

To check whether the AntiVir Guard is active:

- ▶ Select the **Status** tab in the Control Center.
- ▶ Check whether the AntiVir Guard is activated.
- ▶ Activate the AntiVir Guard, if necessary.

6.2 Targeted scan for viruses and malware (on-demand scan)

You have the following options for a targeted (on-demand) virus and malware scan:

- Via a scan profile
If you want to check a specific selection of drives.
- Via drag&drop
If you want to check individual files which you have placed on your desktop, for example.
- Via the pop-up menu
If, for example, you want to check individual files in Windows Explorer and do not want to start the Control Center first.
- Automated
If you want drives to be checked automatically on a regular basis.

6.2.1 Scanning for viruses and malware via a scan profile

A scan profile is a list of drives and directories which are to be scanned.

You have the following option for scanning via a scan profile:

- Using a predefined scan profile
If the predefined scan profiles meet your needs.
- Customizing and using a scan profile (manual selection)
If you would like to scan with a customized scan profile.

Depending on the operating system, there are different symbols for starting a scan profile:

- Under Windows XP and 2000:



With this symbol you start the scan using a scan profile.

- Under Windows Vista:

Under Microsoft Windows Vista the Control Center initially has restricted rights e.g., for accessing folders and files. The Control Center can only execute certain actions and file accesses if it possesses extended administrator rights. These extended administrator rights have to be issued at each start using a scan profile.



With this symbol you start the restricted scan using a scan profile. Only those folders and files are scanned for which Windows Vista has assigned the access rights.



With this symbol you start the scan with extended administrator rights. After a confirmation, all folders and files are scanned in the chosen scan profile.



Information on using scan profiles is also found in the following chapters:



- Creating a desktop link for a scan profile
- Adding or removing file type in a scan profile

Scanning for viruses and malware with a predefined scan profile

To scan for viruses and malware with a predefined scan profile:

- ▶ Select the **Scanner** tab in the Control Center.
 - ↳ Predefined scan profiles are displayed.

- ▶ Select one of the predefined scan profiles and click the symbol (Windows XP:  or Windows Vista: ).



-
-  Under Windows Vista: If you have clicked :
The dialog box *User account control* is displayed.
 - ▶ If applicable, sign on as administrator.
 - ▶ Click on **Continue**.
-



- ▶ The *Luke Filewalker* dialog box is displayed and the on-demand scan starts.
 - ↳ The results are displayed once the scanning process is complete.

Scanning for viruses and malware with customized scan profiles

You can start a scan based on your needs very quickly with a customized scan profile (manual selection) without having to create a new scan profile.

To customize a scan profile and use it to scan for viruses and malware:

- ▶ Select the **Scanner** tab in the Control Center.
 - ↳ Scan profiles appear.
- ▶ Open the file tree in the **Manual Selection** scan profile until all drives to be scanned are open:
- ▶ Select the nodes to be scanned by clicking the box:
- ▶ Click the symbol (Windows XP:  or Windows Vista: .

-
-  Under Windows Vista: If you have clicked :
The dialog box *User account control* is displayed.
 - ▶ If applicable, sign on as administrator.
 - ▶ Click on **Continue**.
-

- ▶ The *Luke Filewalker* dialog box is displayed and the on-demand scan starts.
 - ↳ The results are displayed once the scanning process is complete.


Information on using scan profiles is also found in the following chapters:

- Creating a desktop link for a scan profile

Creating a desktop link for a scan profile

You can start a on-demand scan directly from your desktop via a desktop link without calling up the Control Center of the Avira AntiVir PersonalEdition Classic.

To create a link to the scan profile on the desktop:

- ✓ You are in the Control Center, on the *Scanner* tab.
- ▶ Select the scan profile to which you would like to create a link.
- ▶ Click the  symbol.
 - ↳ The desktop link is created.

Adding or removing file type in a scan profile

To specify in a scan profile that additional file types are to be scanned or certain file types are to be omitted from the scan (only possible with manual selection):

- ✓ You are in the Control Center, on the *Scanner* tab.
- ▶ Right-click the scan profile you would like to edit.
 - ↳ A pop-up menu is opened.
- ▶ Select the **File filter** item.
- ▶ Open the pop-up menu further by clicking the small triangle on the right-hand side of the pop-up menu.
 - ↳ The items *Default*, *Scan all files* and *User-defined* are displayed.
- ▶ Select the **User-defined** item.
 - ↳ The *File extensions* dialog box is displayed and shows a list of all file types to be scanned in the scan profile.

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

- ▶ Select the file type and click **Delete**.

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

- ▶ Select the file type.
- ▶ Click **Insert** and enter the file extension of the file type in the input field.

Enter no more than 10 characters and do not include the leading dot. Wildcards (* and ?) are acceptable placeholders.

6.2.2 Scanning for viruses and malware via drag&drop

To scan for viruses and malware in a targeted way via drag&drop:

- ✓ The Control Center of Avira AntiVir PersonalEdition Classic is open.
- ▶ Select the file to be checked.
- ▶ Drag the selected file to the *Control Center* with the left mouse button.
 - ↳ The *Luke Filewalker* dialog box is displayed and the on-demand scan starts.
 - ↳ The results are displayed once the scanning process is complete.


6.2.3 Scanning for viruses and malware via the pop-up menu

To scan for viruses and malware in a targeted way via the pop-up menu:

- ▶ Right-click the file to be checked (e.g., in Windows Explorer, on the desktop or in an opened Windows directory).
 - ↳ The pop-up menu of Windows Explorer is displayed.
- ▶ Select **Scan selected files with AntiVir** in the pop-up menu.
 - ↳ The *Luke Filewalker* dialog box is displayed and the on-demand scan starts.
 - ↳ The results are displayed once the scanning process is complete.

6.2.4 Scanning for viruses and malware automatically

To create a job which scans for viruses and malware automatically:

- ▶ Select the **Scheduler** tab in the Control Center.
- ▶ Click the  symbol.
 - ↳ The *Name and description of the job* dialog box is displayed.
- ▶ Name the job and describe it, if necessary.
- ▶ Click **Next**.
 - ↳ The *Type of job* dialog box is displayed.
- ▶ Select the **Scan job**.
- ▶ Click **Next**.
 - ↳ The *Time of the job* dialog box is displayed.
- ▶ Select the time at which the scan is to be performed:
 - **Immediately**
 - **Daily**
 - **Weekly**
 - **Interval**
 - **Single**
 - **Login**
- ▶ Enter the date, if appropriate, for your selection.
- ▶ Select the following additional option, if applicable (availability depends on job type):
 - **Repeat job if time has expired**
 - Jobs from the past which could not be performed at the desired time, e.g. because the computer was switched off, are performed.
- ▶ Click **Next**.
 - ↳ The *Selection of the profile* dialog box is displayed.
- ▶ Select the profile to be scanned.
- ▶ Click **Next**.
 - ↳ The *Selection of the display mode* dialog box is displayed.

- ▶ Select the display mode of the job window:
 - **Minimized**: progress indicator only
 - **Maximized**: entire job window
 - **Invisible**: no job window
- ▶ Click **Finish**.
 - ↳ Your new job is displayed as active (with a check mark) on the start page of the *Scheduler* tab.
- ▶ Deactivate the orders which are not to be performed, if applicable.

You can edit jobs further via the following symbols:



View properties of a job



Modify job



Delete job



6.3 Targeted scan for active rootkits (on-demand scan)

To scan for active rootkits using the predefined scan profile:



Under Windows XP your user account has to possess administrator jobs.

- ▶ If applicable, sign on as administrator or assign administrator rights to your user account.

- ▶ Select the **Scanner** tab in the Control Center.
 - ↳ Predefined scan profiles are displayed.
- ▶ Select the predefined scan profile **Rootkit search** and click (Windows XP:  or Windows Vista: ).
 - ▶ Select the nodes and folders to be scanned by clicking the checkbox of the folder level.



Under Windows Vista the dialog box *User account control* is displayed.

- ▶ If applicable, sign on as administrator.
- ▶ Click on **Continue**.

- ↳ The window *Luke Filewalker* is displayed and the scan-on-demand is started.
- ↳ As soon as the scan process is completed, the results are displayed.

If something was detected, Avira Premium Security Suite offers several possibilities to react, see chapter: Reacting to found viruses and malware.

6.4 Reacting to found viruses and malware

If viruses or malware are found by the Avira AntiVir PersonalEdition Classic, the Avira AntiVir PersonalEdition Classic offers the following options for reacting to this:



The displayed options depend on the operating system and on the module which reports the find (AntiVir Guard, AntiVir Scanner).

- **Repair**

The file is repaired.

This option can only be activated if the found file can be repaired.

- **Move to quarantine**

The file is moved to the *INFECTED* quarantine directory of your hard disk in a special format (*.qua) so that access is no longer possible. Files in this directory can be repaired later in quarantine or, if necessary, sent to Avira GmbH.

- **Delete**

The file is deleted, but can be restored by using corresponding tools (e.g., *Avira UnErase*). This means that the virus signature can be recovered.

- **Rename**

The file is renamed *.vir. Direct access to these files (e.g., via double-clicking) is no longer possible. Files can be repaired and named by to the original later.

- **Deny access**

The detection is only entered in the report file (if activated).

- **Ignore**

The Avira AntiVir PersonalEdition Classic does not carry out further actions. The affected file remains active on your computer.



Danger of data loss and damage to the operating system!

► Use the *Ignore* option in exceptional cases only.

- **Backup to quarantine**

This option can only be activated, if one of the Options Repair, Delete has been selected.

- **Apply selection to all following detections**

The selected action on this detection is applied to all following detections.



We recommend moving a suspicious file which cannot be repaired to quarantine.

Information on handling affected files is also found in the following Chapters:

- Reacting to viruses and malware in an archive file
- Handling files in quarantine (*.qua)

6.4.1 Reacting to viruses and malware in an archive file

If viruses or malware have been found in an archive file, you have the following options:

- Delete entire archive
- Rename archive
- Move archive to quarantine



It is not possible to delete individual files which have been affected from the archive.


6.5 Handling files in quarantine

6.5.1 Handling files in quarantine (*.qua)

To handle files in quarantine:


- ▶ Select the **Quarantine** tab in the Control Center.
- ▶ Check which files are affected so that you can reload the originals back onto your computer from another source, if necessary.

If you would like to view more detailed information on a file:


- ▶ Select the file and click .
 - ↳ The *Properties* dialog box with additional information on the file is displayed.

If you would like to check a file again:

Checking a file is recommended if the virus definition file of the Avira AntiVir PersonalEdition Classic has been updated and a false alarm is suspected. In this way, you can confirm a false alarm by repeating the check and restore the file.

- ▶ Select the file and click .
 - ↳ The file is checked for viruses and malware using the settings of the on-demand scan.
 - ↳ After checking, the *Scan statistics* dialog box appears, which shows statistics on the status of a file before and after the repeated check.

If you would like to delete a file:

- ▶ Select the file and click .

If you are not sure if you can delete the files safely:

- ✓ Email settings configured (see Chapter: Configuring email settings)

- ▶ Send the files to Avira GmbH for analysis. Click .

You can also restore files in quarantine:

- See Chapter: Restoring files in quarantine

6.5.2 Restoring files in quarantine

Depending on the operating system, there are several symbols for restoring:

- Under Windows XP und 2000:



With this symbol you restore the files in the original folder.



With this symbol you restore the files in a folder of your choice.

- Under Windows Vista:

Under Microsoft Windows Vista the Control Center initially has restricted rights e.g., for accessing folders and files. The Control Center can only execute certain actions and file accesses if it possesses extended administrator rights. These extended administrator rights have to be issued at each start using a scan profile



With this symbol you restore the files in a folder of your choice.



With this symbol you restore the files in the original folder. If extended administrator rights are required for accessing, a corresponding enquiry is displayed.

To restore files in quarantine:




Danger of data loss and damage to the operating system of the computer!

- ▶ Use the *Restore selected object* function only in exceptional cases.
 - ▶ Only restore files which could be repaired by a repeated scan.
-



- ✓ File re-scanned and repaired.

- ▶ Select the **Quarantine** tab in the Control Center.
-



Emails and attachments of emails can only be restored with the  option and with the extension **.eml*.

If you would like to restore a file at its original location:

- ▶ Select the file and click the symbol (Windows 2000/XP: , Windows Vista: ).
- This option is not available for emails.



Unter Windows Vista erscheint das Dialogfenster *User account control*.


- ▶ Melden Sie sich ggf. als Administrator an.
- ▶ Klicken Sie auf **Continue**.

↳ You are asked whether you want to restore the file.

- ▶ Click **Yes**.


↳ This file is restored to the directory from which it was moved into quarantine.

If you would like to restore a file to a specific directory:

- ▶ Select the file and click .
- ↳ You are asked whether you want to restore the file.
- ▶ Click **Yes**.
- ↳ The default Windows dialog box for selection of the directory is displayed.
- ▶ Select the directory in which the file is to be restored and confirm.
- ↳ The file is restored in the selected directory.

6.6 Moving suspicious file to quarantine

To move a suspicious file to quarantine manually:

- ▶ Select the **Quarantine** tab in the Control Center.
- ▶ Click .
- ↳ The default Windows dialog box for selection of the file is displayed.
- ▶ Select the file and confirm.
- ↳ The file is moved to quarantine.

Files in quarantine can be checked with the AntiVir Scanner:

- See Chapter: Handling files in quarantine (*.qua)

7 Updating

The effectiveness of the Avira AntiVir PersonalEdition Classic depends on how up-to-date the program files and virus definitions are. For this reason, regularly download updates for the Avira AntiVir PersonalEdition Classic from our download servers.

During download, your computer establishes a connection, to the web server, to which you have previously downloaded the current program packages and virus definitions. It searches for updates for all components of the program packages and loads and installs them on your computer.

You have the following options for performing an update:

- See Chapter: Updating Avira AntiVir PersonalEdition Classic automatically
- See Chapter: Updating Avira AntiVir PersonalEdition Classic manually

You can see whether an update is overdue in the Control Center and the Security Center of Windows XP and Windows Vista:


- See also Chapter: Configuring update alert

7.1 Updating Avira AntiVir PersonalEdition Classic automatically



An update job is preinstalled, which updates the Avira AntiVir PersonalEdition Classic every 24 hours with an available Internet connection and also when an Internet connection is established.

To create a job using the AntiVir Scheduler which updates the Avira AntiVir PersonalEdition Classic automatically:

- ▶ Select the **Scheduler** tab in the Control Center.
- ▶ Click the  *Insert new job with the assistant* symbol.
 - ↳ The *Name and description of the job* dialog box is displayed.
- ▶ Name the job and describe it, if necessary.
- ▶ Click **Next**.
 - ↳ The *Type of job* dialog box is displayed.
- ▶ Select **Update job** from the selection list.
- ▶ Click **Next**.
 - ↳ The *Time of the job* dialog box is displayed.
- ▶ Select the time at which the update is to be performed:
 - **Immediately**
 - **Daily**
 - **Weekly**
 - **Interval**
 - **Single**
 - **Login**



We recommend updating the Avira AntiVir PersonalEdition Classic regularly and often, e.g. every 24 hours.

- ▶ Enter the date, if appropriate, for your selection.
- ▶ Select the additional option, if applicable (availability depends on job type):
 - **Start job while connecting to the Internet**
In addition to the specified frequency, the job is also performed each time a connection to the Internet is established.
 - **Repeat job if time has expired**
Jobs from the past which could not be performed at the desired time, e.g., because the computer was switched off, are performed.
- ▶ Click **Next**.
 - ↳ The *Selection of the display mode* dialog box is displayed.
- ▶ Select the display mode of the job window:
 - **Minimized**: progress indicator only
 - **Maximized**: entire job window
 - **Invisible**: no job window
- ▶ Click **Finish**.
 - ↳ Your new job is displayed as active (with a check mark) on the start page of the *Scanner* tab.
- ▶ Deactivate the jobs which are not to be performed, if applicable.

You can edit jobs further via the following symbols:



View properties of a job



Modify job



Delete job

7.2 Updating Avira AntiVir PersonalEdition Classic manually

To update the Avira AntiVir PersonalEdition Classic manually:

- ▶ Right-click the Avira AntiVir PersonalEdition Classic Tray Icon in the taskbar.
 - ↳ A pop-up menu is opened.
- ▶ Select **Start update**.
 - ↳ The *Avira AntiVir PersonalEdition Classic Updater* dialog box is displayed.
 - OR -
- ▶ Select the **Status** tab in the Control Center.
- ▶ Click the link **Start update** in the *Last update* area.
 - ↳ The Avira AntiVir PersonalEdition Classic Updater dialog box is displayed.



We strongly recommend regularly updating the Avira AntiVir PersonalEdition Classic, e.g., every 24 hours.



You can also perform a manual update directly via the Windows Security Center.

8 Service

Help and additional information can be found here:

- See Chapter: Frequently Asked Questions (FAQ)
- See Chapter: Help in case of a problem
- See Chapter: Forum
- See Chapter: Service hotline
- See Chapter: Online shop

8.1 Frequently Asked Questions (FAQ)

Here are the answers to frequently asked questions.

Where can I get the Avira AntiVir PersonalEdition Classic?

Download the program from the website <http://www.free-av.com>.

Do I get a CD of the Avira AntiVir PersonalEdition Classic?

The program is only available for download on our website <http://www.free-av.com>.

Where can I find detailed version information?

Detailed version information is found in the menu item **Help / About AntiVir PersonalEdition Classic... / Version information** of the Control Center.

Which settings should I make for the Avira AntiVir PersonalEdition Classic?

The Avira AntiVir PersonalEdition Classic is preconfigured with practical settings after installation. You can adapt these settings, depending on the desired level of security (e.g., heuristic detection or expanding the scan to all file and archive types).

How can I check whether the Avira AntiVir PersonalEdition Classic is up-to-date?

The Avira AntiVir PersonalEdition Classic is up-to-date when you have the most current virus definition file. This file is usually updated several times a day.

To check whether you have the up-to-date virus definition file:

- ▶ Perform an update.
- OR -
- ▶ Visit the website <http://www.free-av.com> and read the following information there:
 - Current VDF version number
 - Date and time of publication of the current VDF
- ▶ Select the **Status** tab in the Control Center.
- ▶ Compare this information to the information on the website.

If the information is identical: The Avira AntiVir PersonalEdition Classic is up-to-date.

If the information is not identical: The Avira AntiVir PersonalEdition Classic is not up-to-date. Perform an update.

What is the difference between on-access scan and direct scan?

The on-access scan is carried out automatically by AntiVir Guard. The files on the computer which are currently being accessed are scanned for viruses and malware (on-access scan).

The direct scan is carried out manually. Specific drives and directories can be scanned for viruses and malware in a targeted way (on-demand scanning).

Are there any problems when using several virus protection programs at the same time?

When using different virus protection programs with the reasoning *the more the better*, the following rules must be followed:

- ▶ Use only one on-access scanner (also called Guard).
- ▶ Before installing a second software package, decide which on-access scanner you want to trust. If you decide on a new on-access scanner, deinstall the on-access scanner currently in use. Otherwise, serious errors can occur.

The parallel installation of scanners with which scans are started manually is usually possible. Under certain circumstances, error messages can arise if an anti-virus program uses unencrypted search strings for detection or has repaired a file only partially.

I want to test my virus protection program to see if it really works. Are there test viruses which will not harm my computer?

The European Institute for Computer Anti-Virus Research (EICAR) provides files with test viruses on their website http://www.eicar.org/anti_virus_test_file.htm. These are not real viruses, rather so-called signatures. These files cannot cause damage to your computer.

This is how the Avira AntiVir PersonalEdition Classic should react to the EICAR test virus if a default installation with the preset file types was carried out:

- *ecar.com*

The bare test virus is detected immediately by AntiVir Guard (if activated). Of course, it is also detected via a direct scan (Right-click the test virus. A pop-up menu opens. Select **Scan selected files with AntiVir**). Depending on the settings in the options, a warning message enquiring about how to proceed further is displayed.
- *ecar.com.txt*

Beforehand: To see doubled file extensions, you must activate this option in Windows Explorer. This version is not rejected by AntiVir Guard at first, since *.txt files do not contain executable program code and are therefore safe. If the file is renamed *ecar.com*, AntiVir Guard will react to the file as described above.

The test virus is detected by the direct scan. Processing (see above) is offered.
- *ecar_com.zip*

Here, the test virus is packed in a Zip archive. Since a Zip archive is not dangerous in itself, AntiVir Guard does not react. It first takes action once the archive is unpacked.

The test virus is found in the archive by the direct scan. A message window is displayed and informs you that a virus or malware has been found, but cannot be processed in the Zip archive because otherwise the integrity of the archive would be endangered.

- *eicarcom2.zip*

Here, the test virus is packed in a Zip archive which is packed in a Zip archive itself. These are difficult conditions for a virus scanner. The reactions of AntiVir Guard and the direct scan correspond to those to *eicar_com.zip*. With the direct scan, the test virus is detected and the message window (see above) is displayed. AntiVir Guard first reacts during the second, i.e., last unpacking, once the *eicar.com* file is present.

Is a manual scan necessary from time to time?

AntiVir Guard monitors your system constantly (on-access scan). To ensure that you are always protected, check whether AntiVir Guard is active. In addition, we recommend performing a manual scan (direct scan) regularly for better security.

8.2 Help in case of a problem

Here you will find information on causes of and solutions to possible problems.

The error message *Connection failed while downloading the file ... is displayed when attempting to start an update.*

Cause: Your Internet connection is inactive. This is why Avira AntiVir PersonalEdition Classic cannot find the web server on the Internet.

- ▶ Test whether other Internet services such as WWW or email work. If not, re-establish the Internet connection.

Cause: The proxy server cannot be reached.

- ▶ Check whether the login for the proxy server has changed and adapt it to your configuration, if necessary.

Cause: 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 Avira AntiVir PersonalEdition Classic Configuration (Expert mode) under **General / Update**.

Viruses and malware cannot be moved or deleted.

Cause: The file was loaded by Windows and is active.

- ▶ Update Avira AntiVir PersonalEdition Classic.
- ▶ When using the operating system Windows XP, deactivate System Restore.
- ▶ Start the computer in Safe Mode.
- ▶ Start the Avira AntiVir PersonalEdition Classic Configuration (Expert mode).
- ▶ Select **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 available, and to be used.

The Tray Icon shows an inactive state.

Cause: AntiVir Guard is deactivated.

- ▶ Click the **Activate** link in the AntiVir Guard section of the **Status** tab in the Control Center.

Cause: Communication between the AntiVir Guard and the graphic user interface is being blocked via a firewall.

- ▶ Define a general approval for AntiVir Guard in the configuration of your firewall. AntiVir Guard exclusively works with the address 127.0.0.1 (localhost). An Internet connection is not established.

The computer is extremely slow when I perform a data backup.

Cause: During the back-up procedure, AntiVir Guard scans all files being used by the back-up procedure.

- ▶ Select **Guard / Scan / Exceptions** in the Avira AntiVir PersonalEdition Classic Configuration (Expert mode) and enter the process names of the back-up software.

My firewall reports AntiVir Guard

Cause: Communication with AntiVir Guard occurs via the TCP/IP Internet protocol. A firewall monitors all connections via this protocol.

- ▶ Define a general approval for AntiVir Guard. AntiVir Guard only works with the address 127.0.0.1 (localhost). An Internet connection is not established.

During installation, the computer can crash during the memory test if there is an error in the installed graphic driver.

During installation, the computer can crash during the memory test if there is an error in the installed graphic driver.

- ▶ Restart the computer.



We recommend regular installation of Microsoft updates to close any gaps in security.

8.3 Forum

Before you contact the Hotline, we recommend you visit our user forum at <http://forum.antivir-pe.de>. Your questions may already have been posed and answered by other users here. You can also ask questions there.

8.4 Service hotline

All relevant information concerning our comprehensive support service can be found on our website <http://www.free-av.com>. The experts answer your questions and help you with difficult technical problems.

8.4.1 Preparing your request

Our support staff will ask you some questions to localize the problem. These questions are listed in the following. Prepare yourself for these questions in advance - this can minimize call times and, therefore, costs.

- Have you already contacted us regarding this problem?
 - If yes, what is your call number (support case number)?
 - If no, what is your serial number? This number is found in the **Help** menu of the Control Center.
- Limit the reason for your call using the following three criteria:
 - Problems regarding installation/configuration
 - Problems regarding general use of the program
 - Problems caused by viruses or malware
- Describe the reason for your support case in two to three sentences.
 - Which operating system do you use (Windows 2000, Windows XP, Windows Vista etc.)?
 - What sort of basic changes did you make to your operating system before the error occurred? This could include installation or deinstallation of software, operating system updates and hardware components, for example.
 - Which version of the virus definition file are you using? You can find this information in the Control Center in the menu item **Help / About AntiVir PersonalEdition Classic... / Version information**.

8.5 Online shop

You want to purchase a full version conveniently with the click of a button?

In the online shop of Avira GmbH, you can purchase, extend and enhance licenses quickly and securely under <https://shop.antivir-pe.de/en/>. The online shop guides you through the ordering menu step-by-step. Our multilingual Customer Care Center provides information on ordering process, payment and delivery. Resellers can order on account.

www.avira.com



Avira GmbH

Lindauer Str. 21
D-88069 Tettngang
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Email: info@avira.com
Internet: <http://www.avira.com>

All rights reserved. Subject to change.
© Avira GmbH

MORE THAN SECURITY

