Avira AntiVir Personal – Free Antivirus
User Manual

AVIRA

Trademarks and Copyright

Trademarks
AntiVir is a registered trademark of 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
Code provided by third party providers was used for Avira AntiVir Personal – Free Antivirus. 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 AntiVir Personal – Free Antivirus.

Table of Contents

1 Introduction

Your AntiVir program 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/free-av

The Avira website lets you......

- – access information on other AntiVir desktop programs
- – download the latest AntiVir 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

2 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.
→	Placed before an event that follows the previous action.
Warning	Placed before a warning of the danger of critical data loss.
Note	Placed before a link to particularly important information or a tip which makes your AntiVir program easier to use.

The following emphases are used:

Emphasis	Explanation
Cursive	File name or path data.
	Displayed software interface elements (e.g. window heading, window field or options box).
Bold	Clicked software interface elements (e.g. menu item, section or button).

3 Product information

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

- – see Chapter: Delivery scope
- – see Chapter: System requirements
- – see Chapter: Licensing

AntiVir programs 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:

Note
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 AntiVir program is up-to-date with automatic updates. Configure the program accordingly.

3.1 Delivery scope

Your AntiVir program 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
- – Scanner (on-demand scan) with profile-controlled and configurable scan for all known types of virus and malware
- – Integration into the Windows Vista User Account Control allows you to carry out tasks requiring administrator rights.
- – Guard (on-access scan) for continuous monitoring of all file access attempts
- – Avira SearchFree Toolbar (powered by Ask.com), a search toolbar integrated in the web browser providing quick and convenient search options.
- – For Avira AntiVir Personal Edition users, only in combination with the Avira SearchFree Toolbar: WebGuard 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
- – Rootkit 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
- 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)

3.2 System requirements

The system requirements are as follows:

- Computer Pentium or later, at least 266 MHz
- Operating system
- Windows XP, SP2 (32 or 64 bit) or
- Windows Vista (32 or 64 bit, SP 1)
- Windows 7 (32 or 64 bit)
- At least 150 MB of free hard disk memory space (more if using quarantine for temporary storage)
- At least 256 MB RAM under Windows XP
- At least 1024 MB RAM under Windows Vista, Windows 7
- For the program installation: Administrator rights
- For all installations: Windows Internet Explorer 6.0 or higher
- Internet connection where appropriate (see Installation)

Avira SearchFree Toolbar
- Operating system
- Windows XP, SP2 (32 or 64 bit) or
- Windows Vista (32 or 64 bit, SP 1 recommended)
- Windows 7 (32 or 64 bit)
- Web browser
- Windows Internet Explorer 6.0 or higher, or
- Mozilla Firefox 3.0 or higher

Note
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.

Information for Windows Vista users

On Windows 2000 and 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 is introducing the "User Account Control" with Windows Vista. This offers more protection for users who are logged in as administrators: thus in Windows Vista, one administrator only has the privileges of a normal user at first. Actions for which administrator rights are required are clearly marked in Windows Vista with an information icon. In addition, the user must explicitly confirm the required action. Privileges are only increased and the administrative task performed by the operating system after this permission has been obtained.

The AntiVir program requires administrator rights for some actions in Windows Vista. 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 Vista 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.

3.3 Licensing and Upgrade

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

The license is provided in the form of an activation key. The activation key is a code comprising letters and numbers that you will receive after purchasing the AntiVir product. The activation key contains the exact data of your license, i.e. which programs have been licensed for which period of time.

The activation key will be sent to you by email, if you have purchased your AntiVir program on the Internet or it is rendered on the product packaging.

In order to license your program, please enter your activation key to activate the program. The product activation may be performed during installation. However, you can also activate your AntiVir program after the installation in License Manager, under Help::License management .

A valid activation key is already contained in Avira AntiVir Personal. For this reason, product activation is not required.

In License Manager, you have the option of launching an upgrade for a product from the AntiVir desktop product family. Manual uninstallation of the old product and manual installation of the new product is not required. When upgrading from License Manager, you enter the activation code for the product you want to upgrade in the License Manager input box. The new product is automatically installed.

The following product upgrades can be executed automatically via License Manager:

– Upgrade of Avira AntiVir Personal to Avira AntiVir Premium

– Upgrade of Avira AntiVir Personal to Avira Premium Security Suite

– Upgrade of Avira AntiVir Premium to Avira Premium Security Suite

4 Installation and uninstallation

This chapter contains information relating to the installation and uninstallation of your AntiVir program.

- – see Chapter Installation: Conditions, Installation types, Install
- – see Chapter Installation modules
- – see Chapter Modification installation
- – see Chapter Uninstallation: Uninstall

4.1 Installation

Before installation, check whether your computer fulfils all the minimum system requirements. If your computer satisfies all requirements, you can install the AntiVir program.

Note
During the installation process you have the option of creating a restore point. A purpose of a restore point is to reset the operating system to its pre-installation status. If you want to use this option, ensure that the operating system permits the creation of a restore point:
Windows XP: System properties -> System restore: Disable the option **Disable system restore**.
Windows Vista/Windows 7: System properties -> Computer protection: In the **Protection settings** area, highlight the drive on which the system is installed and click the **Configure** button. In the **System protection** window, enable the option **System settings and restore previous file versions**.

Installation types

During installation you can select a setup type in the installation wizard:

Express

- – Your AntiVir program is completely installed with all program components.
- – The program files are installed into a specified default folder under
  `C:\Program Files`.
- – Your AntiVir program is installed with default settings. You have the option of defining custom settings using the configuration wizard.

User-defined

- – You can choose to install individual program components (see Chapter Installation and uninstallation::Installation modules).
- – 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 AntiVir
   program and initiate a short system scan that is performed automatically after
   installation.

Before starting installation

▶ Close your email program. It is also recommended to end 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.

▶ Establish an Internet connection: The Internet 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)

▶ Registering as a user

▶ Where appropriate, carrying out a update after completed installation

▶ Keep the license key for your AntiVir program handy when you want to activate the
   program.

Note
Internet-based installation:
For the Internet-based installation of the program, an installation program is provided
that loads the current program file prior to installation by the Avira GmbH web servers.
 This process ensures that your AntiVir program is installed with the latest virus
definition file.
Installation with an installation package:
The installation package contains both the installation program and all necessary
program files. No language selection for your AntiVir program is available for
installation with an installation package. We recommend that you carry out an update of
the virus definition file after installation.

Note
For registration, your AntiVir program uses the HTTP protocol and Port 80 (web
communication), as well as encryption protocol SSL and port 443, to communicate with
the Avira GmbH 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.

Install

The installation program runs in self-explanatory dialog mode. Every window contains a
certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions:

– **OK:** Confirm action.

– **Abort:** Abort action.

– **Next:** Go to next step.

– **Back:** Go to previous step.

Installing your AntiVir program:

▶ Start the installation program by double-clicking the installation file you have
   downloaded from the Internet or insert the program CD.

Internet-based installation

The dialog box *Welcome...* appears.

▶ Click **Next** to continue with the installation.

The dialog box *Language selection* appears.

▶ Select the language you want to use to install your AntiVir program and confirm your language selection by clicking **Next**.

The dialog box *Download* appears. All files necessary for installation are downloaded from the Avira GmbH web servers. The *Download* window closes after conclusion of the download.

Installation with an installation package

The installation wizard opens with the dialog box *Avira AntiVir Personal*.

▶ Click *Accept* to begin the installation.

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

The dialog box *Welcome...* appears.

▶ Click **Next**.

Continuing Internet-based installation and installation with an installation package

The dialog box with the license agreement appears.

▶ Confirm that you accept the license agreement and click **Next**.

The dialog box *Private use* appears.

▶ Confirm that your AntiVir program will be used exclusively for private purposes and not for commercial purposes and click **Next**.

The dialog box *Generate serial number* appears.

▶ Where appropriate, confirm that a random serial number has been generated and transmitted during update, and click **Next**.

The dialog box *Select installation type* appears.

▶ Enable the option **Express** or **User-defined**. If you want to create a restore point, enable the **Creating system restore point** option. Click **Next** to confirm your settings.

The dialog box *WebGuard with Avira SearchFree Toolbar (powered by Ask.com)* appears.

▶ If you want to install the Avira SearchFree Toolbar, confirm that you accept the terms of the Ask.com End User License Agreement and want to install the WebGuard with the Avira SearchFree Toolbar.

Note
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.

▶ If necessary, enable the **Make Ask.com my browser default search provider** option and click **Next:**.

User-defined installation

The dialog box *Select destination directory* appears.

▶ Confirm the specified destination directory by clicking **Next**.

- OR -

Use the **Browse** button to select a different destination directory and confirm by clicking **Next**.

The dialog box *Install components* appears:

▶ Enable or disable the required components and confirm by clicking **Next**.

In the following dialog box you can decide whether to create a desktop shortcut and/or a program group in the Start menu.

▶ Click **Next**.

Resume: Express installation und user-defined installation

The license wizard is opened.

In the license wizard you have the possibility of registering as a customer and subscribing to the Avira Newsletter. Your personal data are required for this purpose.

▶ If necessary, enter your data and confirm by clicking **Next**.

In case of a registration, the following dialog box will display the result of the activation.

Click **Next**.

The program features will be installed. Installation progress is displayed in the dialog box.

In the following dialog box you can choose whether to open the Readme file after installation is completed and whether to restart your computer.

▶ Agree where appropriate and complete the installation by clicking *Finish*.

The installation wizard is closed.

Resume: User-defined installation
Configuration wizard

If you choose user-defined installation, the configuration wizard is opened in the following step. The configuration wizard enables you to define custom settings for your AntiVir program.

▶ Click **Next** in the welcome window of the configuration wizard to begin configuration of the program.

The *Configure AHeAD* dialog box enables you to select a detection level for the AHeAD technology. The detection level selected is used for the Scanner (On-demand scan) and Guard (On-access scan) AHeAD technology settings.

▶ Select a detection level and continue the installation by clicking **Next**.

In the following dialog box *Select extended threat categories*, you can adapt the protective functions of your AntiVir program to the threat categories specified.

▶ Where appropriate, activate further threat categories and continue the installation by clicking *Next*.

If you have selected the AntiVir Guard installation module, the *Guard start mode* dialog box appears. You can stipulate the Guard start time. At each computer reboot, the Guard will be started in the start mode specified.

Note
The specified Guard start mode is saved in the registry and cannot be changed via the Configuration.

▶ Enable the required option and continue the configuration by clicking *Next*.

In the following *System scan* dialog box, a short system scan can be enabled or disabled. The short system scan is performed after the configuration has been completed and before the computer is rebooted, and scans running programs and the most

important system files for viruses and malware.

▶ Enable or disable the *Short system scan* option and continue the configuration by clicking *Next*.

In the following dialog box, you can complete the configuration by clicking *Finish*

▶ Click *Finish* to complete the configuration.

The specified and selected settings are accepted.

If you have enabled the *Short system scan* option, the Luke Filewalker window opens. The Scanner performs a short system scan.

Resume: Express installation und user-defined installation

If you selected the **Restart computer** option in the final installation wizard, the computer reboots.

After the computer restart the Readme file is displayed if you selected the **Show Readme.txt** option in the installation wizard.

After a successful installation, we recommend that you check the program is up-to-date in the Control Center under *Overview::Status*.

▶ Where appropriate, perform an update to ensure the virus definition file is up-to-date.

▶ Then perform a complete system scan.

4.2 Change installation

You have the option of adding or removing individual program components of the current AntiVir program installation (see Chapter Installation and uninstallation::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.

Select your AntiVir program and click **Change**. In the welcome dialog of the program, select the option **Modify**. You will be guided through the installation changes.

Note
If you uninstall the Avira SearchFree Toolbar, WebGuard is also uninstalled.

4.3 Installation modules

In a user-defined installation or a change installation, the following installation modules can be selected, added or removed.

– **AntiVir Personal**
This module contains all components required for successful installation of your AntiVir program.

– **AntiVir Guard**
The AntiVir Guard runs in the background. It monitors and repairs, if possible, files during operations such as open, write and copy in on-access mode. Whenever a user carries out a file operation (e.g. load document, execute, copy), the AntiVir program automatically scans the file. Renaming a file does not trigger a scan by AntiVir Guard.

– **AntiVir WebGuard** (for Avira AntiVir Personal Edition users, only in combination with the Avira SearchFree Toolbar)
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 AntiVir Guard is not possible. This could allow viruses and unwanted programs to access your computer system. WebGuard 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.

– *AntiVir Rootkit Protection*
AntiVir Rootkit 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.

– **Shell Extension**
The Shell Extension generates an entry 'Scan selected files with AntiVir' in the context menu of the Windows Explorer (right-hand mouse button). With this entry you can directly scan files or directories.

4.4 Uninstallation

If you wish to remove the AntiVir program from your computer, you can use the option **Add or Remove Programs** to **Change/Remove** programs in the Windows Control Panel.

To uninstall your AntiVir program (e.g. in Windows XP and Windows Vista):

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

▶ Double click on **Programs** (Windows XP: **Software**).

▶ Select your AntiVir program in the list and click **Remove**.

You will be asked if you really want to remove the program.

▶ Click **Yes** to confirm.

All components of the program are removed.

▶ Click on **Finish** to complete uninstallation.

Where appropriate, a dialog box appears recommending that your computer be restarted.

▶ Click **Yes** to confirm.

The AntiVir program is uninstalled and all directories, files and registry entries for the program are deleted when your computer is restarted.

11

Note
The Avira SearchFree Toolbar is not included in the uninstallation program and must be uninstalled separately by following the steps detailed above. To do this in Firefox the Avira SearchFree Toolbar must be enabled via the Add-On Manager (does not apply to Internet Explorer). After uninstallation the search toolbar is no longer integrated in your web browser .

Note
If you uninstall the Avira SearchFree Toolbar, WebGuard is also uninstalled.

5   Overview of AntiVir Personal

This chapter contains an overview of the functionality and operation of your AntiVir program.

- – see Chapter Interface and operation
- – see Chapter How to...?

5.1 User interface and operation

You operate your AntiVir program via three program interface elements:

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

5.1.1   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 AntiVir program.
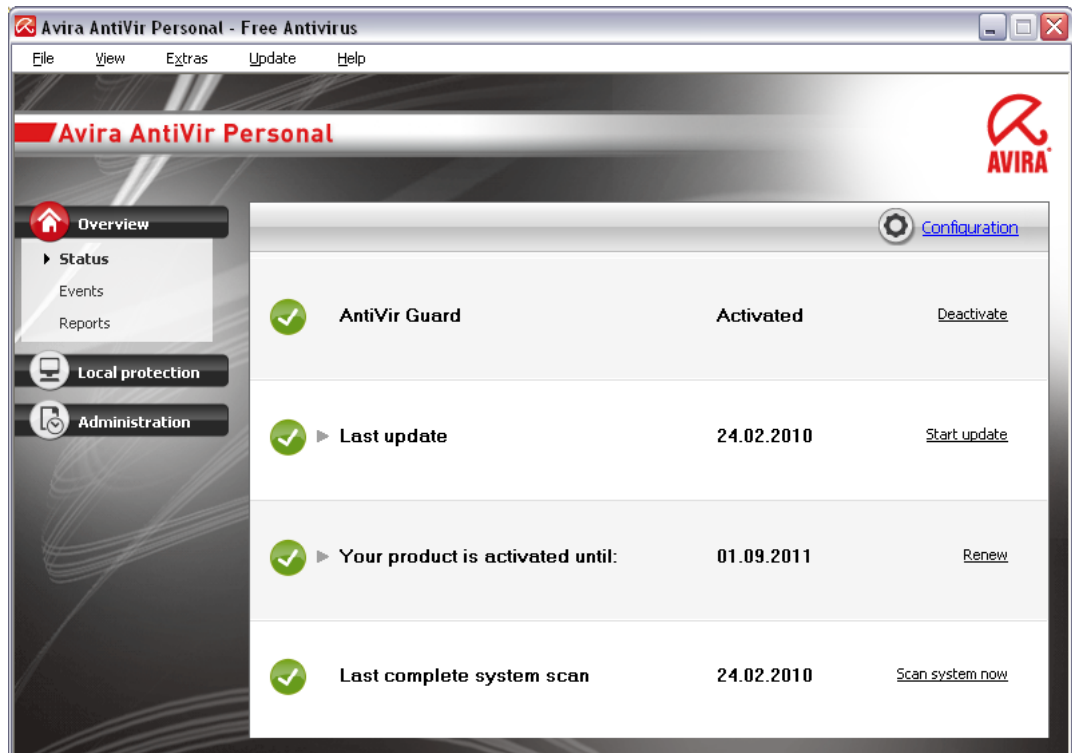
The Control Center window is divided into three areas: The **Menu bar**, the **Navigation bar** and the detail window **View**:

- – **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 *Overview* - Section **Status**.

– **View:** This window shows the section selected in the navigation area. Depending on the section, you will find buttons to execute functions and actions in the upper bar of the detail window. Data or data objects are displayed in lists in the individual sections. You can sort the lists by clicking in the box defining how you wish to sort the list.

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 AntiVir program.

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.

- OR -

▶ Select a section via the *View* menu.

> **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

– **Overview**: In **Overview** you will find all sections with which you can monitor the functioning of your AntiVir program.

- The **Status** section lets you see at a glance which program modules are active and provides information on the last update performed. You can also see whether you own a valid license.

- The Events section enables you to view events generated by certain program modules.

- Die Reports section enables you to view the results of actions performed.

  – **Local protection**: In**Local protection** you will find the components for checking the files on your computer system for viruses and malware.

- The Scan section enables you to easily configure and start an on-demand scan. Predefined profiles enable you to run a scan with already adapted standard 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 (not saved) .

- The Guard 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".

  – **Online protection**: In **Online protection** you will find the components to protect your computer system against viruses and malware from the Internet, and against unauthorized network access.

- The WebGuard 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".

  – **Management**: In **Management** 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 and to adapt or delete existing jobs.

5.1.2 Configuration

You can define settings for your AntiVir program   in the Configuration. After installation, your AntiVir program is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for your AntiVir program may mean you need to adapt the protective components of the program.
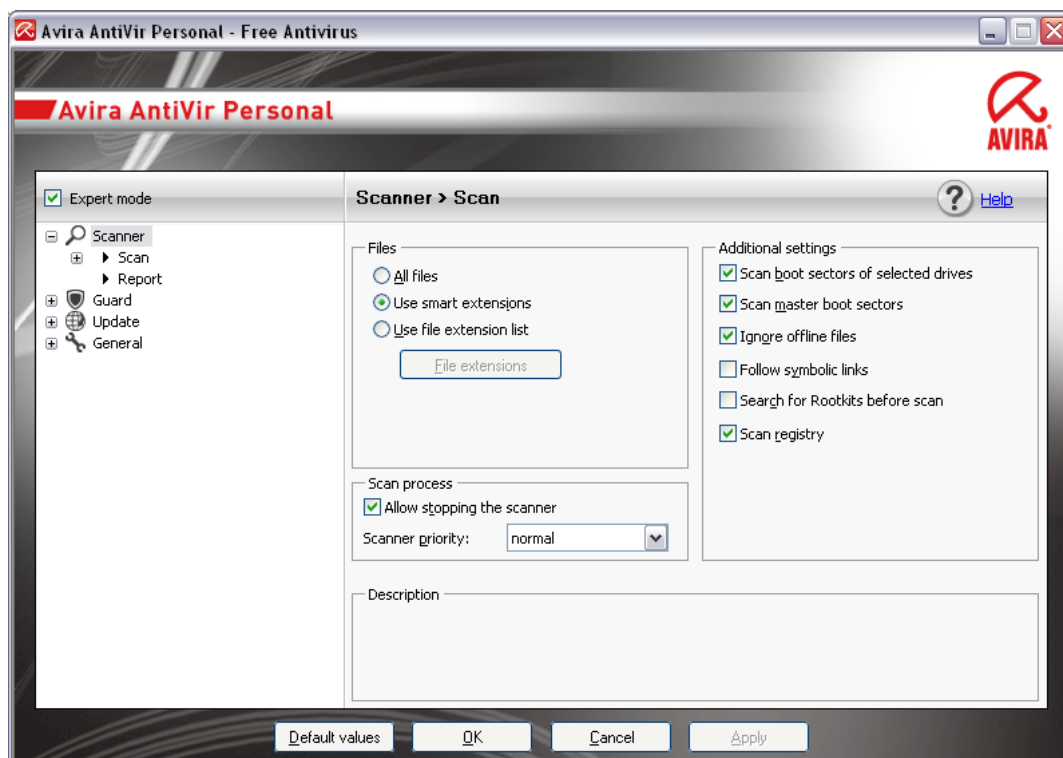
The Configuration opens a dialog box: You can save your configuration settings via the OK or Apply buttons, delete your settings by clicking the Cancel button or restore your default configuration settings using the Default values button. You can select individual configuration sections in the left-hand 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 AntiVir program.

– 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. Expert mode must be activated to select individual configuration registers. In this case, a dialog appears asking you to activate expert mode.

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.

Note

All configuration sections are only displayed in expert mode. Activate expert mode to view all configuration sections. Expert mode can be protected by a password that must be defined during activation.

If you want to confirm your Configuration settings:

▶ Click **OK**.

> The configuration window is closed and the settings are accepted.

> - OR -

▶ Click **Accept**.

> 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 **Restore defaults**.

> All settings of the configuration are restored to default values. All amendments and custom entries are lost when default settings are restored.

Overview of configuration options

The following configuration options are available:

– **Scanner**: Configuration of on-demand scan

Scan options

Action on detection

File scan options

On-demand scan exceptions

On-demand scan heuristics

Report function setting

– **Guard**: Configuration of on-access scan

Scan options

Action on detection

On-access scan exceptions

On-access scan heuristics

Report function setting

– **WebGuard**: Configuration of WebGuard

Scan options, enabling and disabling the WebGuard

Action on detection

Blocked access: Web filter for known unwanted URLS (malware, phishing, etc.)

WebGuard scan exceptions: URLs, file types, MIME types

WebGuard heuristics

Report function setting

– **General**:

Extended risk categories for on-demand and on-access scan

Security: Update status display, complete system scan status display, product protection

WMI: Enable WMI support

Event log configuration

Configuration of report functions

Setting of directories used

Update: Configuration of connection to download server, set-up of product updates

Configuration of acoustic alerts when malware is detected

5.1.3   Tray icon

After installation, you will see the tray icon of your AntiVir program in the system tray of the taskbar:

Icon	Description
	AntiVir Guard is enabled
	AntiVir Guard is disabled

The tray icon displays the status of the Guard service.

Central functions of your AntiVir program 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

– **Activate AntiVir Guard**: Enables or disables the AntiVir Guard.

– **Enable AntiVir WebGuard**: Enables or disables the AntiVir WebGuard.

– **Start AntiVir**: Opens the Control Center.

– **Configure AntiVir**: Opens the Configuration

– **Start update** Starts an update.

– Help: opens the Online Help.

– **About AntiVir Personal:** Opens a dialog box with information on your AntiVir program: 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.

5.2 Toolbar

5.2.1 Overview

After successful installation, the Avira SearchFree Toolbar is integrated in your web browser. When the browser is first accessed a status window opens containing important information on toolbar functions.

The toolbar consists of a search box, an Avira logo linked to the Avira website, two status displays and the **Options** menu.

– **Search toolbar**
Use the search toolbar for free to quickly search the Internet using the Ask.com search engine.

– **Status display**
The status displays provide information on the status of the WebGuard and the current update status of Avira AntiVir and helps you identify which actions you need to take to protect your PC.

– **Options**
You can use the options menu to access the toolbar options, clear the history, find toolbar help and information and also uninstall the Avira SearchFree Toolbar directly via the web browser (Firefox only).

5.2.2 Uninstallation

To uninstall your Avira SearchFree Toolbar (e.g. in Windows XP and Windows Vista):

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

▶ Double click on **Programs** (Windows XP: **Software**).

▶ Select the **Avira SearchFree Toolbar plus WebGuard** in the list and click **Remove**.

You will be asked if you really want to uninstall this product.

▶ Click **Yes** to confirm.

Avira SearchFree Toolbar plus WebGuard is uninstalled and all directories, files and registry entries for the Avira SearchFree Toolbar plus WebGuard are deleted when your computer is restarted.

Installation via the web browser

You also have the option of uninstalling the Avira SearchFree Toolbar directly in the browser:

▶ In the search toolbar open the **Options** menu.

▶ Click **Uninstall**.

If you have opened your web browser, you will now be asked to close it.

▶ Close the web browser and click **OK**.

Avira SearchFree Toolbar plus WebGuard is uninstalled and all directories, files and registry entries for the Avira SearchFree Toolbar plus WebGuard are deleted when your computer is restarted.

Note

If you uninstall the Avira SearchFree Toolbar, WebGuard is also uninstalled.

Note

Note that to uninstall the Avira SearchFree Toolbar from Firefox, the toolbar must be enabled in the Add-On Manager.

5.2.3 Use

Search toolbar

You can use the search toolbar to define any number of terms to browse the Internet.

Enter the term in the search box and press the Enter key or click on **Search**. The Ask.com search engine then searches the Internet for you and displays all hits in the browser window.

To find out how to custom configure the Avira SearchFree Toolbar in Internet Explorer and Firefox, go to **Options.**

Status display

WebGuard

WebGuard is enabled.

Avira WebGuard is turned on and your PC is protected.

WebGuard is disabled.

Avira WebGuard is turned off. Check your application and turn on WebGuard to be protected.

Update status

The status message with information on the update status of Avira appears on the right-hand side. You can use the icons and messages to identify which actions you need to take to protect your PC.

Daily update complete

If you move the cursor over the icon, the following message appears: **Avira is up-to-date, your PC is protected.**

▶ No further action is necessary.

Update Avira

If you move the cursor over the icon, the following message appears: **Avira is not up to date. Click here to download the latest update to keep your PC protected.**

▶ Click the yellow icon or text to update Avira AntiVir. This is done in accordance with the custom settings you defined in Avira AntiVir.

During the update, you will receive the message **Updating…**

After a successful update, the green icon is once again displayed with the message **Daily update complete**.

Avira is unavailable.

If you move the cursor over the icon, the following message appears: **Avira is unavailable. To ensure your protection, check to make sure that your application is still installed and running.**

▶ Click the gray icon or text to go to the Avira Help page. There you will find
instructions on what to do next.

5.2.4 Options

The Avira SerachFree Toolbar is compatible with Internet Explorer and Firefox and can
be configured in both web browsers:

Internet Explorer configuration options
Firefox configuration options

Internet Explorer

In Internet Explorer, the following configuration options for the Avira SearchFree
Toolbar are available in the **Options** menu:

<u>Toolbar options</u>

Scan

– **Ask search engine**
In the **Ask search engine** menu, you can select which search engine to use for
the search. Search engines are available for the USA, Brazil, Germany, Spain,
Europe, France, Italy, the Netherlands, Russia and the United Kingdom.

– **Open searches in**
In the **Open searches in** option menu, you can select where the search result
should be displayed; in the **Current window**, in a **New window** or on a **New
tab**.

– **Display recent searches**
If the **Display recent searches** option is enabled, you can display previous
search terms under the text entry box of the search toolbar.

– **Auto clear recent search history when I close the browser**
Enable the option **Auto clear recent search history when I close the
browser** if you do not want to save previous searches and want to clear the
history when you close the web browser.

More options

– **Select toolbar language**
Under **Select toolbar language** you can select the language in which the Avira
SearchFree Toolbar is displayed. The toolbar is available in English, German,
Spanish, French, Italian and Portuguese.

N**ote**
Where possible, the default Avira SearchFree Toolbar language corresponds to that of
your program. If the Toolbar is not available in your language, the default language is
English.

– **Show button text labels**
Disable the **Show button text labels** option if you want to hide the text next to
the Avira SearchFree Toolbar icons.

<u>Clear history</u>

Enable the **Clear history** option if you do not want to save previous searches and want
to clear the history immediately.

<u>Help</u>

Click on **Help** to access the website containing frequently asked questions (FAQs) relating to the Toolbar.

<u>Uninstall</u>

You can also uninstall the Avira SearchFree Toolbar directly in Internet Explorer: Uninstallation in the web browser

<u>Info</u>

Click on **Info** to display which version of the Toolbar is installed.

Firefox

In the Firefox web browser, the following configuration options for the Avira SearchFree Toolbar are available in the **Options** menu:

<u>Toolbar options</u>

Scan

  – **Select Ask search engine**
  In the **Ask search engine** menu, you can select which search engine to use for the search. Search engines are available for the USA, Brazil, Germany, Spain, Europe, France, Italy, the Netherlands, Russia and the United Kingdom.

  – **Display recent searches**
  If the **Display recent searches** option is enabled, you can display previous search terms by clicking on the arrow in the search toolbar. Select a term if you want to display the search result again.

  – **Auto clear recent search history when I close the browser**
  Enable the option **Auto clear recent search history when I close the browser** if you do not want to save previous searches and want to clear the history when you close the web browser.

  – **Display Ask search results when I type keywords or invalid URLs into the browser address bar**
  If this option is enabled, a search is initiated and the search result displayed every time you enter keywords or an invalid URL into the web browser's address bar.

More options

  – **Select toolbar language**
  Under **Select toolbar language** you can select the language in which the Avira SearchFree Toolbar is displayed. The toolbar is available in English, German, Spanish, French, Italian and Portuguese.

Note
Where possible, the default Avira SearchFree Toolbar language corresponds to that of your program. If the Toolbar is not available in your language, the default language is English.

  – **Show button text labels**
  Disable the **Show button text labels** option if you want to hide the text next to the Avira SearchFree Toolbar icons.

<u>Clear history</u>

One click on **Clear history** deletes all previous Avira SearchFree Toolbar search terms.

Help

Click on **Help** to access the website containing frequently asked questions (FAQs) relating to the Toolbar.

Uninstall

You can also uninstall the Avira SearchFree Toolbar directly in Firefox: Uninstallation in the web browser

Info

Click on **Info** to display which version of the Toolbar is installed.

5.3 How to...?

5.3.1 Perform automatic updates

To create a job with the AntiVir Scheduler to update your AntiVir program automatically:

▶ In the Control Center, select the section **Management :: Scheduler**.

▶ Click the ⏱ *Create new job with the wizard* 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* 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**

Note
We recommend regular and frequent updates. The recommended update interval is: 24 hours.

▶ Where appropriate, specify a date according to the selection.

▶ Where appropriate, select additional options (availability depends on type of job):

- **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 *Select display mode* appears.

▶ Select the display mode of the job window:

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

▶ Click **Finish**.

Your newly created job appears on the start page of the **Manager :: Scan** section with the status activated (check mark).

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

Use the following icons to further define your jobs:

 View properties of a job

 Modify job

 Delete job

 Start job

 Stop job

5.3.2 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. A product update can only take place if you have activated the option **Download and automatically install product updates** in the configuration under General :: Update

To start an update of your AntiVir program manually:

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

A context menu appears.

▶ Select **Start update**.

The *Updater* dialog box appears.

- OR -

▶ In the Control Center, select the section **Overview :: 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: 24 hours.

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

5.3.3   On-demand scan: 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.

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

– In Windows XP and 2000:

This icon starts the scan via a scan profile.

– In Windows Vista:

In 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 Windows Vista 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 **Local protection::Scan**.

Predefined scan profiles appear.

▶ Select one of the predefined scan profiles.

-OR-

▶ Adapt the scan profile *Manual selection*.

▶ Click the icon (Windows XP: or Windows Vista:).

▶ The *Luke Filewalker* window appears and an on-demand scan is started.

When the scan is completed, the results are displayed.

If you want to adapt a scan profile:

▶ In the scan profile, expand **Manual Selection** the file tree so that all the drives you want to scan are open:

▶ Highlight the nodes you want to scan by clicking on the box:

5.3.4 On-demand scan: Scan for viruses and malware using Dragamp;Drop

To scan for viruses and malware systematically using Drag&Drop:

The Control Center of your AntiVir program has been opened.

▶ Highlight the file you want to scan.

▶ Use the left-hand mouse button to drag the highlighted file into the *Control Center*.

The *Luke Filewalker* window appears and an on-demand scan is started.

When the scan is completed, the results are displayed.

5.3.5 On-demand scan: 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 you want to scan.

The Windows Explorer context menu appears.

▶ Select **Scan selected files with AntiVir** in the context menu.

The *Luke Filewalker* window appears and an on-demand scan is started.

When the scan is completed, the results are displayed.

5.3.6 On-demand scan: 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 **Management:: 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 *Select profile* appears.

▶ Select the profile to be scanned.

▶ Click **Next**.

The dialog box *Time of job* appears.

▶ Select a time for the scan:

- **Immediately**

- **Daily**

- **Weekly**
- **Interval**
- **Single**

▶ 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 *Select display mode* appears.

▶ Select the display mode of the job window:

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

▶ Select the *Shut down computer* 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 *Manager :: Scheduler* section with the status activated (check mark).

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

Use the following icons to further define your jobs:

View properties of a job

Modify job

Delete job

Start job

Stop job

5.3.7   On-demand scan: 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 **Local protection:: 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: [icon] or Windows Vista: [icon]).

The *Luke Filewalker* window appears and an on-demand scan is started.

When the scan is completed, the results are displayed.

5.3.8 React to detected viruses and malware

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

There are no configurable action options with the Guard component. When a virus or unwanted program is detected, you will receive a desktop notification. In the desktop notification you can remove the detected malware or forward the malware using the Details button to the Scanner component for further virus management. The 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::Scanner):

Action options for the Scanner:

– **Interactive**

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

– **Automatic**

In automatic action mode, when a virus or unwanted program is detected the action you selected in this area is executed automatically.

Action options for , WebGuard:

– **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.

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 (AntiVir Guard, AntiVir Scanner, AntiVir WebGuard) reporting the detection, and the type of malware detected.

Actions of the Scanner and the Guard:

  – **Repair**

The file is repaired.

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

  – **Move to 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 GmbH.

  – **Delete**

The file will be deleted. If a boot sector virus is detected, this can be deleted by deleting the boot sector. A new boot sector is written.

  – **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.

  – **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.

  – **Always ignore**

Action option for Guard detections: No further action is taken by Guard. 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.

  – **Copy to quarantine**

Action option for a rootkit 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 AntiVir program 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.

WebGuard 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 WebGuard 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.

5.3.9   Quarantine: Handling quarantined files (*.qua)

To handle quarantined files:

▶ In the Control Center, select the section **Management :: 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 .

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 AntiVir program 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 on-demand scan settings.

After the scan, the dialog *Scan 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 .

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 **False positive**.

▶ 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 AntiVir program 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.
>
> **Note**
> The size of the files you upload is limited to 20 MB uncompressed or 8 MB compressed.
>
> **Note**
> You can only upload one file at a time.

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

▶ Highlight the quarantined object and click on ⟳ .

   A text file opens containing the data from the selected quarantined object.

▶ Save the text file.

You can also restore the files in quarantine:

   – see Chapter: Quarantine: Restoring files in quarantine

5.3.10 Quarantine: Restore the files in quarantine

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

   – In Windows XP and 2000:

This icon restores the files to their original directory.

This icon restores the files to a directory of your choice.

   – In Windows Vista:

In 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 **Management :: 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 2000/XP: , Windows Vista).

This option is not available for emails.

Note

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 for selecting the directory appears.

▶ Select the directory to restore the file to and confirm.

The file is restored to the selected directory.

5.3.11 Quarantine: Move suspicious files to quarantine

To move a suspect file to quarantine manually:

▶ In the Control Center, select the section **Management :: Quarantine** section.

▶ Click on .

The Windows default window for selecting a file appears.

▶ Select the file and confirm.

The file is moved to quarantine.

You can scan files in quarantine with the AntiVir Scanner:

• see Chapter: Quarantine: Handling quarantined files (*.qua)

5.3.12 Scan profile: 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):

In the Control Center, go to the **Local protection::** *Scan* 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 the file type.

▶ Click **Add** 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 as replacements.

5.3.13 Scan profile: Create desktop shortcut for scan profile

You can start an on-demand scan directly from your desktop via a desktop shortcut to a scan profile without accessing your AntiVir program's Control Center.

To create a desktop shortcut to the scan profile:

In the Control Center, go to the **Local protection::** *Scan* section.

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

▶ Click the icon .

The desktop shortcut is created.

5.3.14 Events: Filter events

Events that have been generated by program components of your AntiVir program are displayed in the Control Center under **Overview::Events** (analogous to the event display of your Windows operating system). The program components are:

– Updater
– Scheduler
– Guard
– Scanner
– WebGuard
– Helper Service

The following event types are displayed:

– Information
– Warning
– Error
– Detection

To filter displayed events:

▶ In the Control Center, select the section **Overview :: 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.

6 Scanner

With the 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:

- **On-demand scan via context menu**
  The on-demand-scan via the context menu (right-hand mouse button - entry **Scan selected files with AntiVir**) 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 an on-demand scan via the context menu.
- **On-demand scan via drag & drop**
  When a file or directory is dragged into the program window of the Control Center, the 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.
- On-demand 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.
- **On-demand 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 **Scan for boot sector viruses** in the **Extras** menu

7 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 AntiVir. The Updater ensures that your AntiVir program 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 AntiVir program to scan for viruses and malware and repair infected objects.

– Scan engine:

The scan engine contains the methods used by your AntiVir program 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 and scan engine are up-to-date and if necessary implements an update. Depending on the settings in the configuration, the Updater also carries out a product update or informs you of the product updates available. 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.

> **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: 24 hours. 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 a Web server of the manufacturer. The existing network connection is the default connection to the download servers of Avira GmbH. You can change this default setting in the Configuration under General :: Update.

8 FAQ, Tips

This chapter contains important information on troubleshooting and further tips on using your AntiVir program.

see Chapter Troubleshooting

see Chapter Keyboard commands

see Chapter Windows Security Center

8.1 Help in case of a problem

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

– Webchat is not operational: Chat messages will not be displayed

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 (expert mode) under General::UpdateYour settings.

Viruses and malware cannot be moved or deleted.

Reason: The file was loaded by windows and is active.

▶ Update your AntiVir product.

▶ If you use the Windows XP operating system, deactivate System Restore.

▶ Start the computer in Safe Mode.

▶ Start the AntiVir program and the 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 it is available and to be used.

The status of the tray icon is disabled.

Reason: AntiVir Guard is disabled.

▶ In the Control Center in the section Overview::Status in the AntiVir Guard area, click on the **Enable** link.

Reason: AntiVir Guard is blocked by a firewall.

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

Otherwise:

▶ Check the startup type of the AntiVir Guard 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 2000 and Windows XP the services applet is located in the sub-directory "Administrative Tools"). Find the entry *Avira AntiVir Guard*. "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, AntiVir Guard scans all files being used by the backup procedure.

▶ Select Guard::Scan::Exceptions in the Configuration (expert mode) and enter the process names of the back-up software.

My firewall reports AntiVir Guard

Reason: Communication with AntiVir Guardoccurs 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.

Note
We recommend regularly installing Microsoft updates to close any gaps in security.

Webchat is not operational: Chat messages are not 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: WebGuard checks the data sent completely for viruses and undesired programs first of all, before the data are loaded into the web browser. During a data transfer with 'transfer-encoding= chunked', WebGuard cannot determine the message length or the data volume.

▶ Enter the configuration of the URL of the web chats as an exception (see Configuration: WebGuard::Exceptions).

8.2 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.

8.2.1 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.
Tab	Change to the next option or options group.
Shift + Tab	Change to the previous option or options group.
← ↑ → ↓	Change between the options in a marked drop-down list or between several options in a group of options.
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.

8.2.2 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.

8.2.3   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
F3	Start scan with the selected profile
F4	Create desktop link for the selected profile

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)

8.3 Windows Security Center

- Windows XP Service Pack 2 or higher -

8.3.1   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.

8.3.2   The Windows Security Center and your AntiVir program

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.
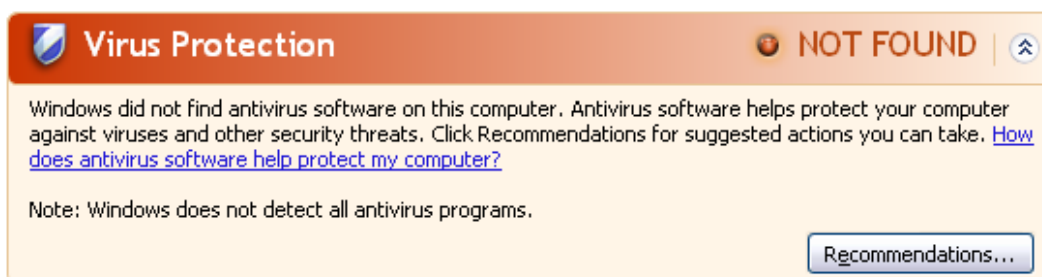
Note
Install your AntiVir program on your computer to protect it against viruses and other unwanted programs!

Virus protection OUT OF DATE

If you have already installed Windows XP Service Pack 2 or Windows Vista and then install your AntiVir program or you install Windows XP Service Pack 2 or Windows Vista on a system on which your AntiVir program has already been installed, you will receive the following message:
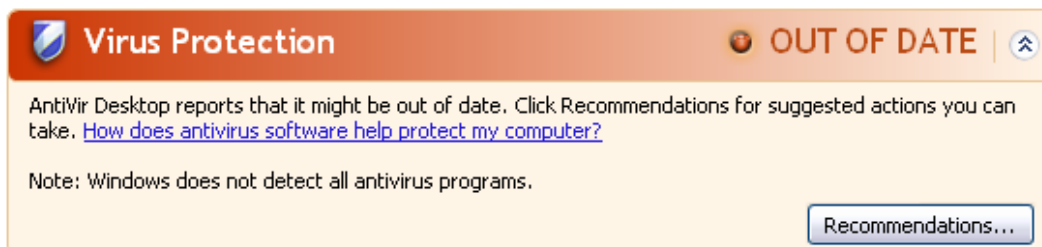
Note
In order for the Windows Security Center to recognize your AntiVir program as up-to-date, an update must be performed after installation. Update your system by carrying out an update.

Virus protection ON

After installation of your AntiVir program and a subsequent update, you will receive the following message:
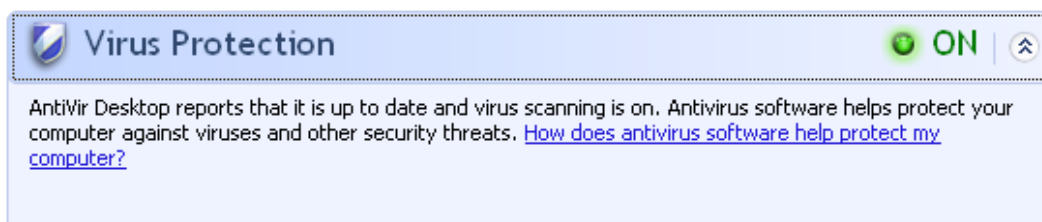
Your AntiVir program is now up-to-date and the AntiVir Guard is enabled.

<u>Virus</u> <u>protection</u> <u>OFF</u>

You receive the following message if you disable the AntiVir Guard or stop the Guard service.
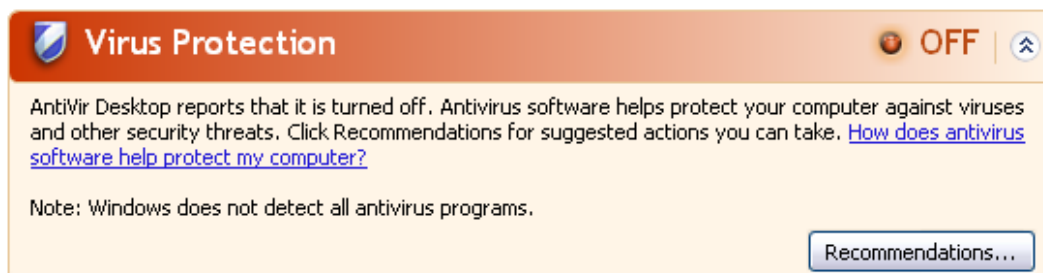
Note
You can enable or disabled AntiVir Guard in the Overview::Status section of the Control Center. You can also see that the AntiVir Guard is enabled if the red umbrella in your taskbar is open.

<u>Virus</u> <u>protection</u> <u>NOT</u> <u>MONITORED</u>

If you receive the following message from the Windows Security Center, you have decided that you want to monitor your anti-virus software yourself.

Note
This function is not supported by Windows Vista.
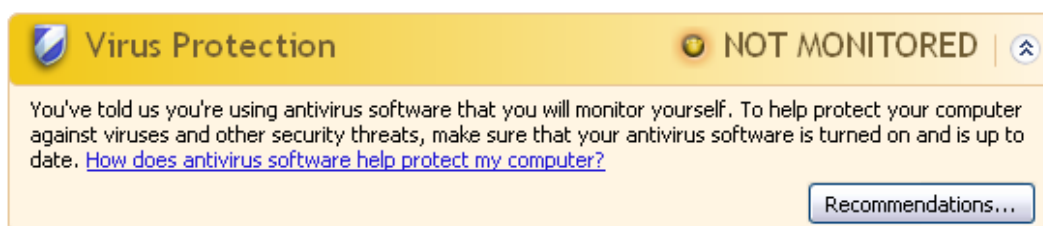
Note
The Windows Security Center is supported by your AntiVir program. You can enable this option at any time via the "Recommendations...." button.

Note
Even if you have installed Windows XP Service Pack 2 or Windows Vista, you still require a virus protection solution. Although Windows XP Service Pack 2 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!

9 Viruses and more

9.1 Extended threat categories

Dialer (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 AntiVir program can detect the familiar dialers by default.

If the option **Dialers** is enabled with a check mark in the configuration under Extended 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.

Games (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 AntiVir program 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 AntiVir program detects a game. The game is now over in the truest sense of the word, because you can simply delete it.

Jokes (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 AntiVir program 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.

Security Privacy Risk (SPR)

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 AntiVir program detects "Security Privacy Risk" software. If the option **Security Privacy Risk** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects such software.

Backdoor Clients (BDC)

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 AntiVir program recognizes "Backdoor control software". If the **Backdoor control software (BDC)** option is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects such software.

Adware/Spyware (ADSPY)

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 AntiVir program recognizes "Adware/Spyware". If the option **Adware/Spyware (ADSPY)** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects adware or spyware.

Unusual Runtime Packers (PCK)

Files that have been compressed with an unusual runtime packer and that can therefore be classified as potentially suspicious.

Your AntiVir program recognizes "Unusual runtime packers". If the option **Unusual runtime packers** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects such packers.

Double Extension Files (HEUR-DBLEXT)

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Your AntiVir program recognizes "Double Extension Files". If the option **Double Extension files** (HEUR-DBLEXT) is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects such files.

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 AntiVir program recognizes "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects such behavior.

Application (APPL)

The term APPL refers to an application which may involve a risk when used or is of dubious origin.

Your AntiVir program recognizes "Application (APPL)". If the option **Application (APPL)** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if your AntiVir program detects such behavior.

9.2 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.

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

Macroviruses 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.

Rootkit

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.

10 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 Report false positives

10.1   Contact address

If you have any questions or requests concerning the AntiVir product range, we will be pleased to help you. For our contact addresses, please refer to the Control Center under Help :: About Avira AntiVir Personal.

10.2   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/personal-support

So that we can provide you with fast, reliable help, you should have the following information ready:

– **Version information**. You can find the program interface under the menu item Help :: About Avira AntiVir Personal:: 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.

10.3   Suspicious file

Viruses that may not yet be detected or removed by our products or suspect files 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-personal@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).

10.4   Reporting false positives

If you believe that your AntiVir program 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-personal@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).

11 Reference: Configuration options

The configuration reference documents all available configuration options.

11.1   Scanner

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

11.1.1 Scan

Here you define the basic behavior of the scan routine for an on-demand scan. If you select certain directories to be scanned with an on-demand scan, depending on the configuration the Scanner scans:

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

Files

The 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.

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 AntiVir 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 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 Scanner scans the boot sectors of the drives selected for the on-demand scan. This option is enabled as the default setting.

Scan master boot sectors

If this option is enabled, the 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.

> **Important**
> This option is only available with Windows Vista and higher.

> **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 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

Follow symbolic links

If this option is enabled, 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. This option is not supported by Windows 2000 and has been deactivated.

> **Important**
> 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 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.

> **Important**
> The rootkit scan is not available for Windows XP 64 bit !

Scan Registry

If this option is enabled, the Registry is scanned for references to malware.

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 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 Scanner is only allocated processor time by the operating system if no other process requires computation time, i.e. as long as only the 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 Scanner continues running in the background. This option is enabled as the default setting and is recommended.

Medium

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

11.1.1.1. Action on detection

Action on detection

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

Interactive

If this option is enabled, the results of the Scanner scan are displayed in a dialog box. When carrying out a scan with the 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 Scanner.

> **Note**
> The action Move to quarantine is preselected by default in the Scanner notification. Further actions can be selected via a context menu.

Click here for more information.

Automatic

If this option is enabled, no dialog box in case of a virus detection appears. The Scanner reacts according to the settings you predefine in this section as primary and secondary action.

Backup to quarantine

If this option is enabled, the 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.

Primary action

Primary action is the action performed when the 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 Scanner repairs affected files automatically. If the 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 Scanner modifies files on the workstation.

delete

If this option is enabled, the file is deleted.

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.

> **Warning**
> The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

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.

delete

If this option is enabled, the file is deleted.

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.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to Quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Note
If you have selected **Delete** or 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.

When scanning archives, the 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 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 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.

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 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 Scanner should scan. For this, you must select the relevant entries.

11.1.1.2. Exceptions

File objects to be omitted for the Scanner

The list in this window contains files and paths that should not be included by the 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 add a complete partition to the list of the file objects, only those files that are saved directly under the partition will be excluded from the scan, which does not apply to files in sub-directories on the corresponding partition:
> Example: File object to be skipped: `D:\` = `D:\file.txt` will be excluded from the scan of the Scanner, `D:\folder\file.txt` will not be excluded from the scan.

11.1.1.3. Heuristics

This configuration section contains the settings for the heuristic of the scan engine.

AntiVir 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 AntiVir 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 AntiVir program contains a very powerful heuristic in the form of AntiVir 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 is enabled as 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.

11.1.2 Report

The 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 enable you to establish what actions the Scanner has performed when viruses or unwanted programs have been detected, a report file should always be created.

Reporting

Off

If this option is enabled, the Scanner does not report the actions and results of the on-demand scan.

Default

When this option is activated, the Scanner logs the names of the files concerned with their path. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

Advanced

When this option is activated, the Scanner logs alerts and tips in addition to the default information.

Complete

When this option is activated, the 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.

11.2   Guard

The Guard section of the configuration is responsible for the configuration of the on-access scan.

11.2.1 Scan

You will normally want to monitor your system constantly. To this end, use the Guard (= on-access Scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

Scan mode

Here the time for scanning of a file is defined.

Scan when reading

If this option is enabled, the Guard scans the files before they are read or executed by the application or the operating system.

Scan when writing

If this option is enabled, the Guard scans a file when writing. You can only access the file again after this process has been completed.

Scan when reading and writing

If this option is enabled, the Guard scans files before opening, reading and executing and after writing. This option is enabled as the default setting and is recommended.

Files

The Guard 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.

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 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.

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.

Maximum recursion depth

When scanning archives, the Guard 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 archives that are directly located in the main archive are scanned.

Maximum 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.

Maximum 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.

11.2.1.1. Action on detection

Notifications

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.

Autostart

Block autostart function

When this option is enabled, the execution of the Windows Autostart function is blocked on all connected drives, including USB sticks, CD and DVD drives and network drives. With the Windows Autostart 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 Autostart 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 Autostart function is permitted on CD and DVD drives.

> **Warning**
> Only disable the Autostart function for CD and DVD drives if you are sure you are only using trusted data media.

11.2.1.2. Exceptions

With these options you can configure exception objects for the Guard (on-access scan). The relevant objects are then not included in the on-access scan. The Guard 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 Guard

All file accesses of processes in this list are excluded from monitoring by Guard.

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.

Note
You can enter up to 128 processes.

Note
When entering the process, Unicode symbols are accepted. You can therefore enter process or directory names containing special symbols.

Note
You have the option of excluding processes from monitoring by the Guard without full path details.
application.exe
This however only applies to processes where the executable files are located on hard disk 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.

Note
Drive information must be entered as follows: [Drive letter]:\
The colon symbol (:) is only used to specify drives.

Note
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 Guard, specifications exclusively comprising the following characters are invalid: * (asterisk), ? (question mark), / (forward slash), \ (backslash), . (dot), : (colon).

Note
The specified path and file name of the process should contain a maximum of 255 characters. The entries in the list must not result in more than 6000 characters in total.

[...]

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 Guard

All file accesses to objects in this list are excluded from monitoring by the Guard.

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.

Note
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

Note
Directory names must end with a backslash \, otherwise a file name is assumed.

Note
The entries in the list must have no more than 6000 characters in total.

Note
If a directory is excluded, all its sub-directories are automatically also excluded.

Note
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

Note
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 Guard 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:

Note
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.

Note
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!

Note
You can locate the path Guard uses to scan for infected files in the Guard report file. Indicate exactly the same path in the list of exceptions. Proceed as follows: Set the protocol function of the Guard to **Complete** in the configuration under Guard::Report. Now access the files, folders, mounted drives with the activated Guard. You can now read the path to be used from the Guard report file. The report file can be accessed in the Control Center under Local protection::Guard.

Examples for processes to be excluded:

 – application.exe

The application.exe process is excluded from the Guard 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 Guard scan.

 – C:\Program Files1*.exe

All processes for executable files located under the path C:\Program Files1 are excluded from the Guard scan.

Examples for files to be excluded:

– *.mdb

All files with the extension 'mdb' are excluded from the Guard scan

– *.xls*

All files with a file extension beginning 'xls' are excluded from the Guard 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 Guard scan.

11.2.1.3. Heuristics

This configuration section contains the settings for the heuristic of the scan engine.

AntiVir 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 AntiVir 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 AntiVir program contains a very powerful heuristic in the form of AntiVir 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 is enabled as 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.

11.2.2 Report

Guard 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 Guard 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, Guard 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.

Advanced

If this option is enabled, Guard logs less important information to the report file as well.

Complete

If this option is enabled, Guard 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, 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.

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 100MB. 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.

11.3   WebGuard

The WebGuard section of the Configuration is responsible for the configuration of the WebGuard.

11.3.1 Scan

WebGuard protects you against viruses or malware that reaches your computer from web pages that you load on your web browser from the Internet. The *Scan* heading can be used to set the behavior of the WebGuard component.

Scan

Enable WebGuard

If this option is enabled, the web pages you request using an Internet browser are scanned for viruses and malware. WebGuard monitors the data transferred from the Internet using the HTTP protocol at ports 80, 8080, 3128. If any affected web pages are detected, the loading of the web pages is blocked. If this option is disabled, the WebGuard service is still started, but the scan for viruses and malware is disabled.

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 Suspect 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.

Default

If this option is enabled, I-Frames with suspect content is blocked.

Advanced

If this option is enabled, I-Frames with suspect content and I-Frames used in a suspicious way are blocked. The use of I-Frames is considered suspect if the I-Frame is very small and is therefore invisible or almost invisible in the browser of if the I-Frame is placed in an unusual position on the web page.

11.3.1.1. Action on detection

Action on detection

You can define the actions to be performed by WebGuard 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.

Click here for more information.

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 WebGuard, 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.

Automatic

If this option is enabled, no dialog box in case of a virus detection appears. WebGuard reacts according to the settings you predefine in this section as primary and secondary action.

Primary action

The primary action is the action performed when WebGuard 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. WebGuard logs the detection to the report file if the report function is activated.

Isolate

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 WebGuard 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!

11.3.1.2. Locked requests

The Web filter lets you block known phishing and malware URLs. WebGuard prevents the transfer of data from the Internet to your computer system.

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 WebGuard.

Note
The Web filter is ignored for entries in the list of excluded URLs under WebGuard::Scan::Exceptions.

Note
Spam URLs are URLs sent with spam emails. The Fraud and Deception category covers web pages with "Subscription Expires" and other offers of services whose costs are hidden by the provider.

11.3.1.3. 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 WebGuard. The MIME types and URLs specified are ignored by WebGuard, i.e. that data is not scanned for viruses and malware when it is transferred to your computer system.

MIME types skipped by WebGuard

In this field you can select the MIME types (content types for the transferred data) to be ignored by WebGuard during scanning.

File types/MIME types skipped by WebGuard (user-defined)

All MIME types (content types for the transferred data) in the list are ignored by WebGuard during scanning.

<u>Input box</u>

In this box you can input the name of the MIME types and file types to be ignored by WebGuard 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 by WebGuard: No scan for viruses and malware is performed.

<u>MIME types: Examples for media types:</u>

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

<u>Examples: Excluded file and MIME types</u>

- `audio/` = All audio media type files are excluded from WebGuard scans

- `video/quicktime` = All Quicktime sub-type video files (*.qt, *.mov) are excluded from WebGuard scans
- `.pdf` = All Adobe PDF files are excluded from WebGuard 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 WebGuard

All URLs in this list are excluded from WebGuard scans.

Input box

In this box you can input URLs (Internet addresses) to be excluded from WebGuard 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 WebGuard: For all entries in the list of excluded URLs, the entries in the web filter (see WebGuard::Scan::Blocked access) are ignored. No scan for viruses and malware is performed. Only trusted URLs should therefore be excluded from WebGuard 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 WebGuard 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 WebGuard scans.

- `avira.com -OR- *.avira.com`

= All URLs with the second and top-level domain 'avira.com' are excluded from WebGuard 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 WebGuard 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 WebGuard 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 WebGuard scans: www.name1.net, www.name2.net, etc.

> **Warning**
> Enter the URLs you want to exclude from the WebGuard 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 WebGuard 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

11.3.1.4. Heuristics

This configuration section contains the settings for the heuristic of the scan engine.

AntiVir 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 AntiVir 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 AntiVir program contains a very powerful heuristic in the form of AntiVir 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 is enabled as 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.

11.3.2 Report

The WebGuard 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 WebGuard 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, WebGuard 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.

Advanced

If this option is enabled, WebGuard logs less important information to the report file as well.

Complete

If this option is enabled, WebGuard logs all available information in the report file, including file size, file type, date, etc.

Limit report file

<u>Limit</u> <u>size</u> <u>to</u> <u>n</u> <u>MB</u>

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% .

<u>Backup</u> <u>report</u> <u>file</u> <u>before</u> <u>shortening</u>

If this option is enabled, the report file is backed up before shortening.

<u>Write</u> <u>configuration</u> <u>in</u> <u>report</u> <u>file</u>

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 100MB. Entries are deleted until the size of the report file reaches 80 MB.

11.4 Update

In the *Update* section you can configure the automatic receiving of updates. You can specify various update intervals and activate or deactivate automatic updating.

Automatic update

<u>Activate</u>

If this option is enabled, automatic updates are performed for the enabled events at the specified interval.

<u>Automatic</u> <u>update</u> <u>every</u> <u>n</u> <u>days</u> <u>/</u> <u>hours</u> <u>/</u> <u>minutes</u>

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 key to the right of the input box.

<u>Repeat</u> <u>job</u> <u>if</u> <u>the</u> <u>time</u> <u>has</u> <u>already</u> <u>expired</u>

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.

11.4.1 Start product update

Under **Product update**, configure how product updates or the notification of available product updates are handled.

Product updates

<u>Download</u> <u>and</u> <u>automatically</u> <u>install</u> <u>product</u> <u>updates</u>

If this option is enabled, product updates are downloaded and automatically installed by the Update component as soon as they become available. Updates to the virus definition file and scan engine are performed independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Download product updates. If a restart is necessary, install the update after the system restart, otherwise install it immediately.

If this option is enabled, product updates will be downloaded as soon as they become available. If no restart is necessary, the update is installed automatically after the update file is downloaded. If a product update requires you to restart your computer, it will be executed at the next user-controlled system reboot and not immediately after the download of the update file. This has the advantage that the restart is not performed while users are working at their computers. Updates to the virus definition file and scan engine are performed independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Notification when new product updates are available

If this option is enabled, you will be notified by email when new product updates become available. Updates to the virus definition file and scan engine are performed independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server. You will receive notifications via a desktop popup window and via an alert from the Updater in the Control Centre under Overview::Events.

Notify again after n day(s)

If the product update was not installed after the initial notification, enter in this box the number of days that are to elapse before you are again notified that product updates are available.

Do not download product updates

If this option is enabled, no automatic product updates or notifications of available product updates by the Updater are performed. Updates to the virus definition file and search engine are performed independently of this setting.

Important
An update of the virus definition file and of the search engine is performed during every update process independent of the settings for the product update (see Chapter Updates).

Note
If you have enabled an option for an automatic product update, you can configure further restart notification and cancellation options under Restart settings.

11.4.2 Restart settings

When a product update for your AntiVir program is performed, you may have to restart your computer system. If you have selected automatic product updates under General::Update::Product update , you can choose between the different restart notification and restart cancellation options under **Restart settings**.

Note
Note that your restart settings allow you to choose between two options for executing a product update requiring a computer restart in the configuration under General::Update::Product update.

Automatic execution of the product update with the required computer restart when update is available: The update and the restart are performed while users are working on their computers. If you have enabled this option, it may be useful to select restart routines with a cancel option or reminder function.

Execution of the product update where a computer restart is required after the next system reboot: the update and the restart are performed after users have started up their computers and logged in. Automatic restart routines are recommended for this option.

Restart settings

Restart the computer after n seconds

If this option is enabled, the restart which is necessary after a product update has been executed is performed **automatically** at the specified interval. A countdown message appears with no option for canceling the computer restart..

Reminder message for restart every n seconds

If this option is enabled, the restart which is necessary after a product update has been executed is **not** performed automatically. At the specified interval, you will receive restart notifications without cancel options. These notifications let you confirm the computer restart or select the "**Remind me again"** option.

Query whether computer should be restarted

If this option is enabled, the restart which is necessary after a product update has been executed is **not** performed automatically. You will receive only one message, which offers the option to perform a restart directly or cancel the restart routine.

Restart computer without query

If this option is enabled, the restart which is necessary after a product update has been executed is performed **automatically**. You will not receive any notification.

The update can be performed directly via a web server on the Internet.

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 RDT connection made for the update is automatically interrupted again as soon as the download has been successfully performed.

Note
This option is not available under Vista. Under Vista the dial-up connection opened for the update is always terminated as soon as the download has been performed.

11.5   General

11.5.1 Threat categories

Selection of threat categories

Your AntiVir product protects you against computer viruses.

In addition, you can scan according to the following extended threat categories.

– Backdoor Clients (BDC)
– Dialer (DIALER)
– Games (GAMES)
– Jokes (JOKES)
– Security Privacy Risk (SPR)
– Adware/Spyware (ADSPY)
– Unusual runtime packers (PCK)
– Double Extension Files (HEUR-DBLEXT)
– Phishing
– Application (APPL)

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.

11.5.2 Security

Update

Alert if last update 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).

Product protection

> **Note**
> The product protection options are not available if the Guard 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 protection. The option is enabled as the default setting. To disable this option, you have to restart your computer.

> **Important**
> Password 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.

11.5.3 WMI

Support for Windows Management Instrumentation

Windows Management Instrumentation is a basic Windows management technique that uses script and programming languages to allow read and write access, both local and remote, to settings on Windows systems. Your AntiVir program supports WMI and provides data (status information, statistical data, reports, planned requests, etc.) as well as events via an interface. WMI gives you the option of downloading operating data from the program

Enable WMI support

When this option is enabled, you can download operating data from the program via WMI.

11.5.4 Proxy

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 Windows 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.

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

11.5.5 Directories

Temporary path

In this input box, enter the path where the program will store its temporary files.

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.

[...]

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.

11.5.6 Events

Limit size of event database

Limit maximum number of events to 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 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.

Do not limit size of event database (delete events manually)

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.

11.5.7 Limit reports

Limit number of reports

<u>Limit the number to n units</u>

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.

<u>Delete all reports more than n day(s) old</u>

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.

<u>Do not limit number of reports (manually delete reports)</u>

If this option is enabled, the number of reports is not restricted.

11.5.8 Acoustic alerts

Acoustic alert

When a virus or malware is detected by the Scanner or Guard, an acoustic alert is sounded 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 Scanner is set in the configuration under Scanner::Scan::Action on detection.

<u>No warning</u>

When this option is enabled, there is no acoustic alert when a virus is detected by the Scanner or Guard.

<u>Use PC speakers (only in interactive mode)</u>

If this option is enabled, there is an acoustic alert with the default signal when a virus is detected by the Scanner or Guard. The acoustic alert is sounded on the PC's internal speaker.

<u>Use the following Wave file (interactive mode only)</u>

If this option is enabled, there is an acoustic alert with the selected Wave file when a virus is detected by the Scanner or Guard. The selected Wave file is played over a connected external speaker.

<u>Wave file</u>

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.

11.5.9 Warnings

Your AntiVir program generates so-called slide-ups, desktop notifications for specific events, which give information on successful or failed program sequences such as updates. In *Warnings* 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 reverse the disabling of the notification in *Warnings*.

Warnings

on dial-up connections 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).

on successfully updated files

If this option is enabled, you will receive a desktop notification whenever an update has been successfully performed and files updated.

on failed update

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.

that no update is 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.

AVIRA

live *free.*™