



User Manual

 **AntiVir**[®]

Avira Premium Security Suite

www.avira.com

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

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

MD5-Code

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

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

All rights reserved.

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

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

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

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

Expat

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

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

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

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

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

ScewXML

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

c-ares

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Table of Contents

1	Introduction	6
2	Icons and emphases	7
3	Product information	8
3.1	Delivery scope	8
3.2	System requirements	9
3.3	Licensing	10
3.3.1	License manager	11
4	Installation and Deinstallation	12
4.1	Installation	12
4.2	Modification installation	15
4.3	Installation modules	15
4.4	Uninstallation	16
5	Premium Security Suite overview	18
5.1	User interface and operation	18
5.1.1	Control Center	18
5.1.2	Configuration	21
5.1.3	Tray icon	24
5.2	How to...?	25
5.2.1	Activate license	25
5.2.2	Avira Premium Security Suite automatic update	26
5.2.3	Start a manual update	27
5.2.4	On-demand scan: Using a scan profile to scan for viruses and malware	28
5.2.5	On-demand scan: Scan for viruses and malware using Drag&Drop	29
5.2.6	On-demand scan: Scan for viruses and malware via the context menu	30
5.2.7	On-demand scan: Automatically scan for viruses and malware	30
5.2.8	On-demand scan: Targeted scan for active rootkits	31
5.2.9	Reacting to detected viruses and malware	31
5.2.10	Quarantine: Handling quarantined files (*.qua)	33
5.2.11	Quarantine: Restore the files in quarantine	34
5.2.12	Quarantine: move suspicious files to quarantine	35
5.2.13	Scan profile: Amend or delete file type in a scan profile	35
5.2.14	Scan profile: Create desktop shortcut for scan profile	36
5.2.15	Events: Filter events	36
5.2.16	MailGuard: Exclude email addresses from scan	37
5.2.17	MailGuard: Train the anti-spam module	37
5.2.18	Firewall: Select the security level for Firewall	38
5.2.19	Backup: Create backups manually	38
5.2.20	Backup: Create automatic data backups	40
6	Scanner	42
7	Updates	43

8	Backup	44
9	FAQ, Tips	45
9.1	Frequently asked questions (FAQs)	45
9.2	Troubleshooting	48
9.3	Shortcuts	52
9.4	Windows Security Centre	55
10	Viruses and more	58
10.1	Extended threat categories	58
10.2	Viruses and other malware	60
11	Info and Service	63
11.1	Contact address	63
11.2	Technical support	64
11.3	Suspicious file	64
11.4	Report false positive	65
11.5	Your feedback for more security	65
12	Reference: Configuration	66
12.1	Scanner	66
12.1.1	Scan	66
12.1.1.1.	Action for concerning files	69
12.1.1.2.	Further actions.....	71
12.1.1.3.	Archive list.....	72
12.1.1.4.	Exceptions	72
12.1.1.5.	Heuristic	73
12.1.2	Report.....	74
12.2	Guard	75
12.2.1	Scan	75
12.2.1.1.	Action for concerning files	77
12.2.1.2.	Other actions	79
12.2.1.3.	Exceptions	79
12.2.1.4.	Heuristic	81
12.2.2	Report.....	82
12.3	MailGuard	84
12.3.1	Scan	84
12.3.1.1.	Action for concerning files	84
12.3.1.2.	Other actions	86
12.3.1.3.	Heuristic	87
12.3.1.4.	AntiBot	88
12.3.2	General.....	89
12.3.2.1.	Exceptions	89
12.3.2.2.	Cache	91
12.3.2.3.	AntiSpam.....	91
12.3.3	Report.....	92
12.4	Firewall	93

12.4.1	Adapter rules	93
12.4.1.1.	Incoming Rules	97
12.4.1.2.	Outgoing Rules.....	104
12.4.2	Application rules	105
12.4.3	Settings.....	107
12.4.4	Popup settings	107
12.5	WebGuard.....	109
12.5.1	Scan	109
12.5.1.1.	Action for concerning files	109
12.5.1.2.	Locked requests.....	110
12.5.1.3.	Exceptions	112
12.5.1.4.	Heuristic	114
12.5.2	Report.....	115
12.6	Backup.....	116
12.6.1	Settings.....	116
12.6.2	Exceptions	116
12.6.3	Report.....	118
12.7	General.....	119
12.7.1	Email.....	119
12.7.2	Extended threat categories.....	120
12.7.3	Password	120
12.7.4	Security.....	122
12.7.5	Directories.....	123
12.7.6	Update	123
12.7.6.1.	Web server.....	124
12.7.7	Events.....	126
12.7.8	Limit reports	126

1 Introduction

Avira Premium Security Suite from Avira GmbH protects your computer against viruses, malware, adware and spyware, unwanted programs and other dangers. This manual deals with viruses and software in brief.

The manual describes the program installation and operation.



Please go to our website <http://www.avira.com> where you can download the Avira Premium Security Suite manual in PDF form, update Avira Premium Security Suite or renew your license.

You can also find information on our website such as telephone numbers for technical support and information on how to subscribe to our newsletter.

Your Avira GmbH team

2 Icons and emphases

The following icons are used:

Icon	Explanation
✓	Placed before a condition which must be fulfilled prior to implementation.
▶	Placed before an action step that you implement.
→	Placed before an event that follows the previous action.
	Placed before a warning of the danger of critical data loss.
	Placed before a link to particularly important information or a tip which makes Avira Premium Security Suite easier to use.

The following emphases are used:

Emphasis	Explanation
<i>Cursive</i>	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 Avira Premium Security Suite:

- see chapter: Delivery scope
- see chapter: System requirements
- see chapter: Licensing
- see chapter: License manager

Avira Premium Security Suite is a comprehensive and flexible tool you can rely on to protect your computer from viruses, malware, unwanted programs, and other dangers

► Please note the following information:



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.



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 Avira Premium Security Suite is up-to-date with automatic updates. Configure the program accordingly.

3.1 Delivery scope

Avira Premium Security Suite gives you the following functions:

- Control Center for monitoring, administering 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 search 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
- MailGuard (POP3- and SMTP-Scanner) for the permanent checking of emails for viruses and malware. Checking of email attachments is included
- WebGuard for monitoring data and files transferred from the Internet using the HTTP protocol (monitoring of ports 80, 8080, 3128)
- Backup-component for creating backups of your data (mirror backups)
- Integrated quarantine management to isolate and process suspicious files
- Rootkit protection for detecting hidden malware installed in your computer system (rootkits)
(Only for 32-bit systems)
- 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 webserver on the Internet
- User-friendly licensing in License Manager
- Integrated Scheduler to plan one-off or recurring tasks, such as updates or test runs
- Very high rates of virus and malware detection using innovative search technologies (search engines) and heuristic search processes
- Detection of all common archive types, including detection of nested archives and smart extensions
- High-performance multithreading function (simultaneous high-speed scanning of multiple files)
- Firewall to protect your computer against illegal access from the Internet or from a network, and against illegal access from the Internet/network by an unauthorized user.

3.2 System requirements

For Avira Premium Security Suite to work perfectly, the computer system must fulfill the following requirements:

- Computer, Pentium, minimum 133 MHz
- Operating system
- Microsoft Windows Vista (32 or 64 Bit) or
- Microsoft Windows XP Home or Professional, SP2 recommended, or
- Microsoft Windows 2000, SP 4 recommended




Avira Premium Security Suite also supports Microsoft Windows XP x64 Edition and 64 Bit Microsoft Windows Vista.

- At least 192 MB RAM with Windows 2000/XP
- At least 512 MB RAM with Windows Vista
- 40 MB free memory space on the hard disk (more if using the quarantine function)
- 100 MB temporary memory space on the hard disk
- For installation of Avira Premium Security Suite: Administrator rights in Windows NT, 2000 and XP

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 carried out by the operating system after this permission has been obtained.

Avira Premium Security Suite requires administrator rights for some actions in Windows Vista. These actions are identified 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

In order to be able to use Avira Premium Security Suite, you require a license. You thereby accept the license conditions of Avira Premium Security Suite.

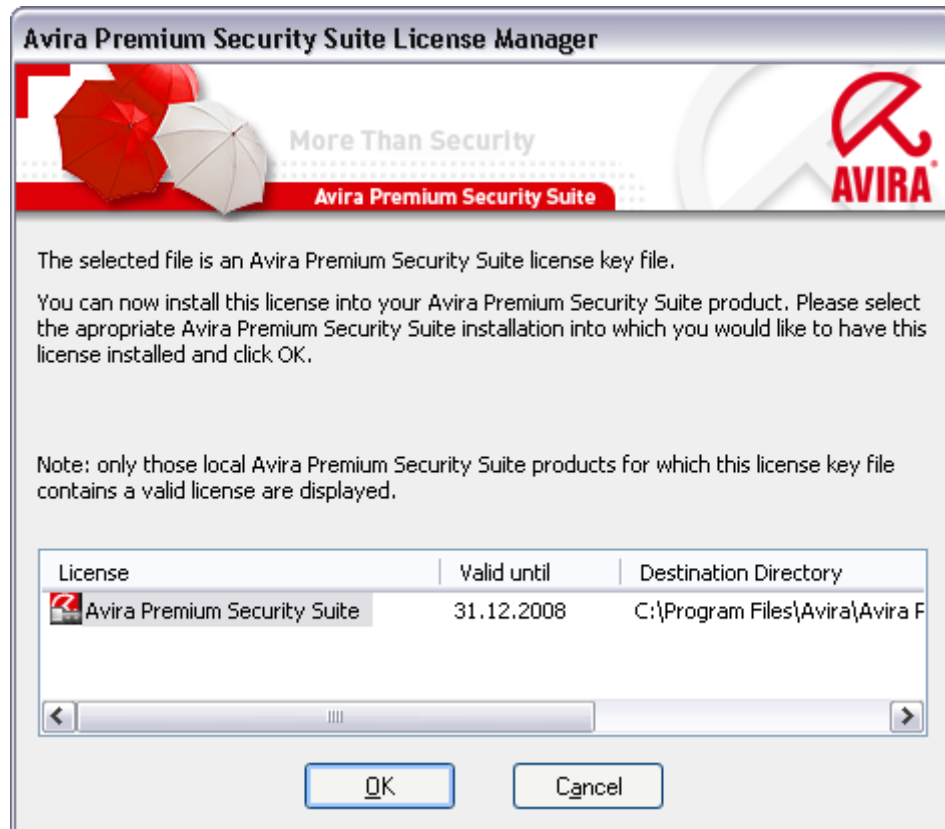
The license is issued via a digital license code in the form of the file hbedv.key. This digital license code is the Control Center of your personal license. It contains exact details of which programs are licensed to you and for what period of time. A digital license code can therefore also contain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

If you purchased Avira Premium Security Suite on the internet, or via a program CD/DVD, the digital license code is sent to you by email. You can load the license key during installation of Premium Security Suite or install it later in License Manager.

3.3.1 License manager

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

Avira Premium Security Suite License Manager



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



The Avira Premium Security Suite License Manager automatically copies the corresponding license in the relevant product folder. If a license already exists, a note appears as to whether the existing license file is to be replaced. The existing file is then renamed hbedv.old.

4 Installation and Deinstallation

This chapter contains information relating to the installation and uninstallation of your Avira Premium Security Suite:

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

4.1 Installation

Before installing Avira Premium Security Suite, check whether your computer fulfils all the minimum system requirements. If so, you can install Avira Premium Security Suite.



From Windows XP, Avira Premium Security Suite generates a restore point of your computer before installation of Avira Premium Security Suite. This enables you to safely remove Avira Premium Security Suite if installation fails. Note that for this the option **Turn off System Restore** under: "Start | Settings | Control Panel | System | Tab System Restore" must not be marked.

If you want to recover your system earlier, you can do so with the function "Start | Programs | Accessories | System Tools | System Restore". The restore point generated by Avira Premium Security Suite is indicated by the entry Premium Security Suite.

Installation types

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

Full

Premium Security Suite is fully installed with all program components. Program files are installed in a predefined default directory in `C:\Program files`.

User-defined

You can choose to install individual program components (see Chapter Installation and uninstallation::Installation modules). A destination 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 and predefine a setting for the Win32 file heuristic.

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.

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.

How to install Premium Security Suite:



The following actions for disabling the Windows Firewall only apply to the Windows XP operating system.

- ▶ Start the installation program by double-clicking on the installation file that you have downloaded from the internet or insert the program CD.
 - ↳ After a security message is displayed confirming the publisher of the software, the installation program dialog box appears.
- ▶ Click **Accept**.
 - ↳ The setup program for Avira Premium Security Suite starts.
- ▶ Click **Continue**.
 - ↳ The dialog box *Welcome...* appears.
- ▶ Click **Next**.
 - ↳ The dialog box *Expanded risk categories* appears containing information on basic and advanced protection.
- ▶ Click **Next**.
 - ↳ The dialog box with the license agreement appears.
- ▶ Confirm that you accept the license agreement and click **Continue**.
 - ↳ The dialog box *Select installation type* appears.
- ▶ Decide whether you want to perform a full or a user-defined installation.
- ▶ Enable the option **Full** or **User-defined** and confirm by clicking **Continue**.

User-defined installation

- ↳ The dialog box *Select destination directory* appears.
- ▶ Confirm the specified destination directory by clicking **Continue**.
 - 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 **Continue**.
 - ↳ If Windows Firewall is installed, a message appears saying it must be disabled to avoid conflicts with Avira Firewall
- ▶ Click **Yes** to confirm.
 - ↳ Windows Firewall is disabled.

- ↳ In the following dialog box you can decide whether to enable the Win32 file heuristic.
- ▶ Click **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**.
- ▶ Skip the following section "Full installation".

Full installation

- ↳ If Windows Firewall is installed, a message appears saying it must be disabled to avoid conflicts with Avira Firewall.
- ▶ Click **Yes** to confirm.
- ↳ Windows Firewall is disabled.

Continue for full and user-defined installation.

- ↳ The dialog box *Install license* appears:
- ▶ Go to the directory in which you have saved the license file, read the message in the dialog box and confirm by clicking **Next**.
- ↳ The license file is copied and the components are installed and started.
- ↳ The setup program asks if *thereadme.txt* file containing up-to-date information on Avira Premium Security Suite should be displayed.
- ▶ Agree where appropriate and click **Finish**.
- ▶ Confirm the information by clicking **OK**.

Next procedure (varies slightly depending on the operating system)):

- ↳ The setup program closes the installation and, where appropriate, creates a desktop shortcut.
- ↳ The file *readme.txt* is displayed where appropriate.
- ↳ You are asked if you want to perform an update.



On the latest version of Avira Premium Security Suite provides reliable protection from the ever-increasing number of viruses and other malware. Perform an update immediately after installation. After this first update, the Windows Security Centre (XP and Vista) announces that Avira Premium Security Suite is ACTIVATED.

- OR -

- ↳ You are asked if you want to restart your computer.
-



In Windows XP, when the Windows Firewall is disabled, a dialog box always appears (for security purposes), indicating that the computer must be restarted..

If you want to perform an update:

- ▶ Click **Yes** to confirm.
- ↳ An update is sought for Avira Premium Security Suite via the existing web server connection.

- ↳ Avira Premium Security Suite then starts an automatic scan of the Windows system directories.



The first scan is particularly important to ensure that your system is free from viruses and malware. Do not cancel the first scan.

If you want to restart the computer:

- ▶ Click **Yes** to confirm.
 - ↳ The computer is restarted.

4.2 Modification installation

You have the option of adding or removing individual program components of the current Avira Premium Security Suite installation (see Chapter Installation and uninstallation::Installation modules)

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

Select Avira Premium Security Suite and click **Change**. In the welcome dialog of Avira Premium Security Suite select the option **Modify**. You will be guided through the installation changes.

4.3 Installation modules

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

- **Premium Security Suite**
This module contains all components required for successful installation of Avira Premium Security Suite.
- **AntiVir Guard**
The AntiVir Guard runs in the background. It monitors and repairs, where necessary, 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), Avira Premium Security Suite automatically scans the file. Renaming a file does not trigger a scan by AntiVir Guard.
- **AntiVir MailGuard**
AntiVir MailGuard is the interface between your computer and the email server from which your email program (mail client) downloads the emails. MailGuard is connected as a so-called proxy between the email program and the email server. All incoming emails are routed through this proxy, scanned for viruses and unwanted programs and forwarded to your email program. Depending on the configuration, the program processes the affected emails automatically or asks the user for a certain action. In addition, the MailGuard can reliably protect you against spam emails.

- **AntiVir WebGuard**

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 checks 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.

- **Avira Firewall**

Avira Firewall controls communication to and from your computer. It permits or denies communications based on security policies.

- **Rootkit Detection**

The Rootkit Detection 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 Avira Premium Security Suite 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.

- **Backup**

The Backup component lets you create mirror backups of your data manually and automatically.

4.4 Uninstallation

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

To uninstall Avira Premium Security Suite (e.g. in Windows XP and Windows Vista):

- ▶ Open the **Control Panel** via the Windows **Start** menu.
- ▶ Double click on **Software** (Windows Vista: **Program files**).
- ▶ Select **Avira Premium Security Suite** and click **Remove**.
 - ↳ You will be asked if you really want to remove the program.
- ▶ Click **Yes** to confirm.
 - ↳ You will be asked if you want to re-enable Windows Firewall (Avira Firewall is disabled).
- ▶ 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.
 - ↳ Avira Premium Security Suite is uninstalled, and all directories, files and registry entries for Avira Premium Security Suite are deleted when your computer is restarted.

5 Premium Security Suite overview

This chapter contains an overview of the functionality and operation of Premium Security Suite.

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

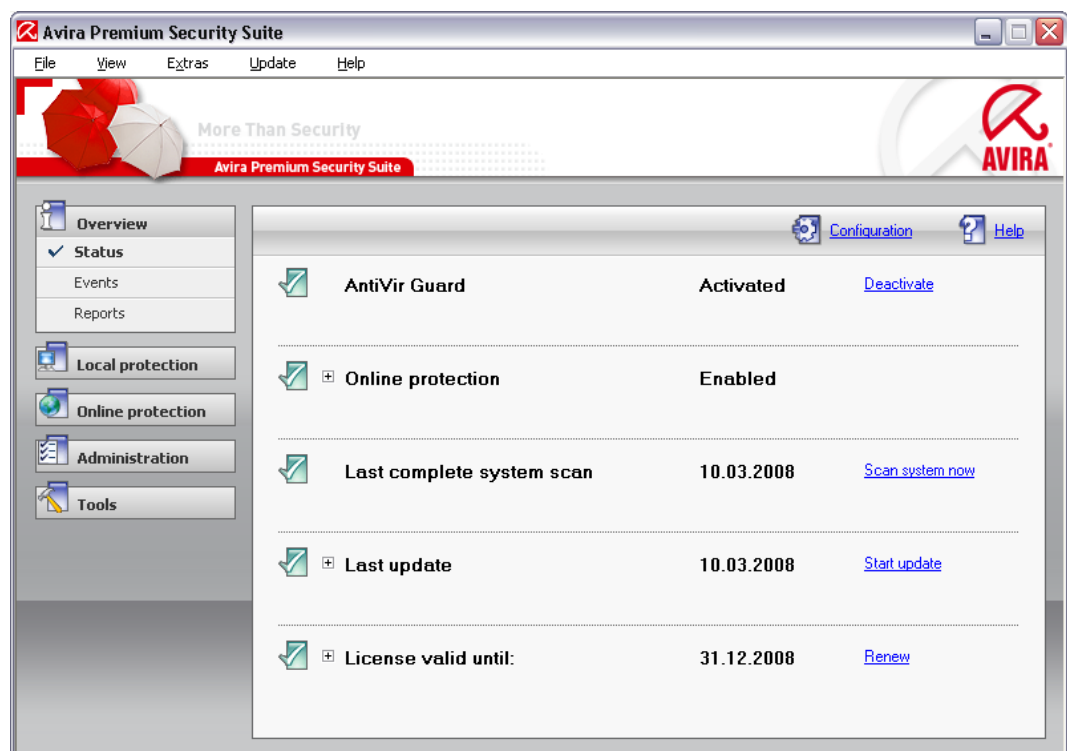
5.1 User interface and operation

Your operate Premium Security Suite via three program interface elements:

- Control Center: Monitoring and control of Premium Security Suite
- Avira Premium Security Suite Configuration: Configuration of Premium Security Suite
- Tray Icon in the system tray of the taskbar: Open 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 Premium Security Suite.



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 Premium Security Suite.

- **Navigation area:** In the navigation area, you can easily swap between the individual sections of Control Center. The individual sections contain information and functions of the program components of Premium Security Suite and are arranged in the navigation bar according to activity. For example: Activity *Overview* - Section **Status**.
- **View:** This window shows the section selected in the navigation area. According to section, in the upper bar of the detail window you will find buttons to execute functions and actions. 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 ending Control Center

To start the Control Center, the following options are available:

- double click the program icon on your desktop
- via the Premium Security Suite program entry in the start menu | program.
- via the Avira Premium Security Suite tray icon.

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

Control Center operation

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 menu *View*.



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 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

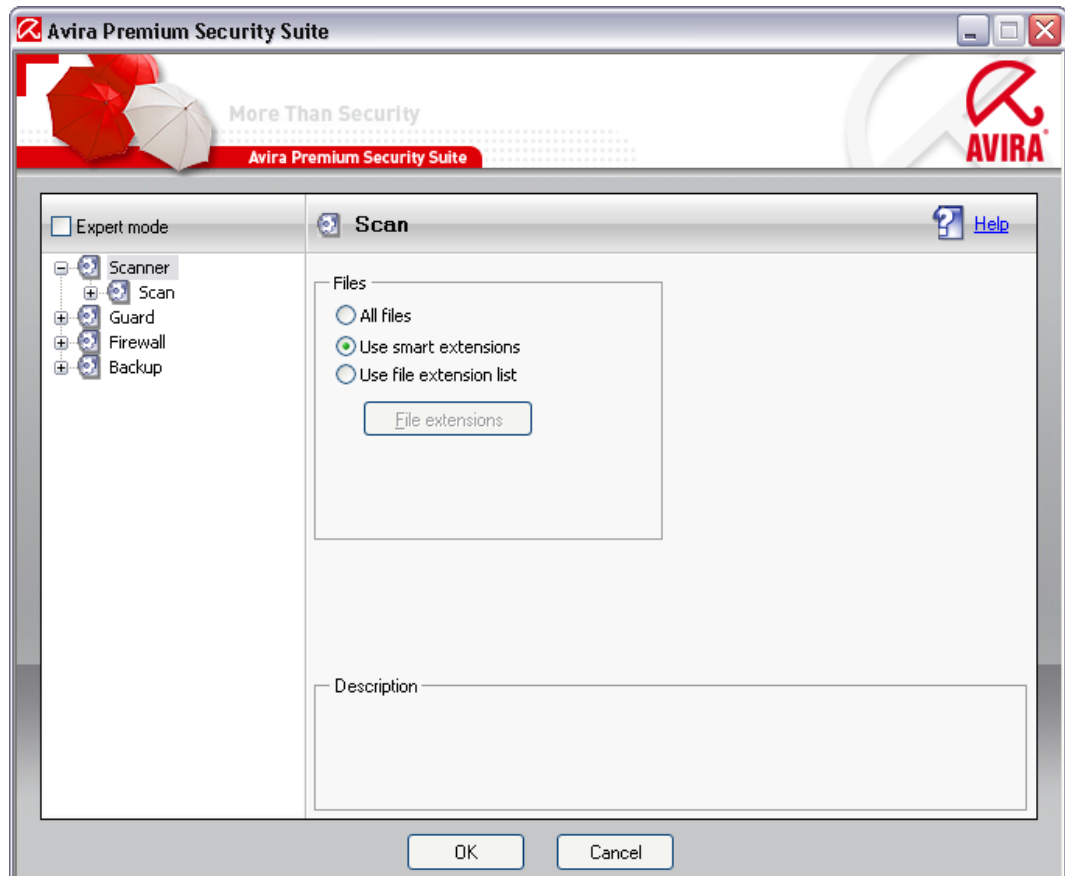
Control Center overview

- **Overview:** In **Overview** you will find all sections with which you can monitor the functioning of Avira Premium Security Suite.
- The **Status** section lets you see at a glance which Avira Premium Security Suite modules are active and provides information on the last update carried out. You can also see whether you own a valid license.
- The Events section enables you to view events generated by certain Avira Premium Security Suite modules.
- The Reports section enables you to view the results of actions executed by Avira Premium Security Suite.

- **Local protection:** In **Local protection** you will find the components for checking the files on your computer system for viruses and malware.
- The Scanner section enables you to easily configure and start an on-demand scan. Predefined profiles enable you to run a scan with preset default options. In the same way it is possible to adapt the scan for viruses and unwanted programs to your personal requirements with the help of manual selection (not saved) or by creating user-defined profiles, .
- The Guard section shows you 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 found 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 MailGuard section shows you the emails scanned by MailGuard, their properties and other statistical data. You can also train the anti-spam filter and exclude email addresses from future scanning for malware or spam. Emails can also be deleted from the MailGuard buffer.
- The WebGuard section shows you information on scanned URLs and detected viruses, as well as other statistical data, which can be reset at any time and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained practically "at the push of a button".
- The Firewall section enables you to configure the basic settings for the Avira Firewall. In addition, the current data transfer rate and all active applications using a network connection are displayed.
- **Administration:** In **Administration** 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 which you would like to place in quarantine. It is also possible to send a selected file to the Avira Malware Research Center by email.
- The Scheduler section enables you to configure scheduled scanning and update jobs as well as backup jobs and to adapt or delete existing jobs.
- **Tools:** In **Tools** you will find other data security tools.
- In the Backup section, you can create backups of your data easily and quickly and initiate backup jobs.

5.1.2 Configuration

In Avira Premium Security Suite Configuration, you can implement settings for Premium Security Suite. After installation, Premium Security Suite is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for Premium Security Suite may mean you need to adapt the protective components of Premium Security Suite.



Avira Premium Security Suite Configuration opens a dialog box: confirm or delete your configuration settings using the OK or Cancel button. You can select individual configuration sections in the left-hand navigation bar.

Accessing Avira Premium Security Suite 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 Avira Premium Security Suite tray icon.
- in the Avira Premium Security Suite Control Center via the menu item Extras | Configuration.
- In the Avira Premium Security Suite Control Center via the button Configuration.



If you are accessing configuration via the **Configuration** button in Control Center, go to the configuration register of the section which is active in Control Center. Expert mode must be activated to select individual configuration registers. In this case, a dialog appears asking you to activate expert mode.

Avira Premium Security Suite Configuration operation

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

- ▶ Click on an entry in the tree structure to display this configuration section in the detail window
- ▶ Click on 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.



All configuration sections are only displayed in expert mode. Activate expert mode to see all configuration sections. Expert mode can be protected by a password which 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.

If you want to finish configuration without confirming your settings:

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

Overview of configuration options

The following configuration options are available:

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

Scan options

Action for concerning files

File scan options

On-demand scan exceptions

On-demand scan heuristics

Report function setting

- **Guard:** On-access scan configuration

Scan options

Action for concerning files

On-access scan exceptions

On-access scan heuristics

Report function setting

- **MailGuard:** Configuration of MailGuard

Scan options

Action on Malware

MailGuard scan heuristics

MailGuard scan exceptions

Configuration of cache, empty cache

Configuration of the anti-spam training database, empty training database

- **WebGuard:** Configuration of WebGuard

Action on detections

Blocked access: unwanted URLs, file types, MIME types

MailGuard scan exceptions

MailGuard heuristics

Report function setting

- **Firewall:** Configuration of Firewall

Adapter rule setting

User-defined application rule settings

Expanded settings: timeout for rules, lock Windows host file, stop Windows Firewall

- **Backup:**

Backup component setting (incremental backup, scan for viruses during backup)

Exceptions: Defining files for saving

Report function setting

- **General:**

Configuration of email using SMTP

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

Password protection for access to Control Center and Avira Premium Security Suite Configuration

Security: Alert for outdated Premium Security Suite, configuration protection, process protection,

Event log configuration



Configuration of report functions

Setting of directories used

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

5.1.3 Tray icon

After installation, you will see the Premium Security Suite tray icon in the system tray of the taskbar:

Icon	Description
	AntiVir Guard is activated and the Firewall is activated
	AntiVir Guard is deactivated or the Firewall is deactivated

The tray icon displays the status of the AntiVir Guard service.

Central functions of Avira Premium Security Suite can be quickly accessed via the context menu of the tray icon. To open the context menu, click on the tray icon with the right-hand mouse button.

Entries in the context menu

- **AntiVir Guard enable:** activates or deactivates the Avira Premium Security Suite Guard.
- **Firewall:**
 - Firewall enable: activates or deactivates the Firewall
 - Block All Traffic: When activated, the firewall blocks all data transfer with the exception of transfers to your own computer system (local host / IP 127.0.0.1).
 - Game Mode enable: activates or deactivates game mode:
When activated, all defined adapter and application rules apply. Applications for which no rule is defined are permitted network access and no pop-up window is opened.
- **Start Avira Premium Security Suite:** opens the Avira Premium Security Suite Control Center.
- **Avira Premium Security Suite configuration:** opens the Avira Premium Security Suite Configuration.
- **Start update:** starts an Update.
- **Help:** opens this online help.
- **Avira on the Internet:** opens the web portal of Premium Security Suite on the Internet. The condition for this is that you have an active connection to the Internet.

5.2 How to...?

5.2.1 Activate license

To activate the Premium Security Suite license:

Activate your license for Avira Premium Security Suite with the license file hbedv.key. You can get a license file from Avira GmbH by email. The license file contains the license for all the products you have ordered.

If you have not yet installed Avira Premium Security Suite:

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

If you have already installed Avira Premium Security Suite:

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

- OR -

- ▶ In the Avira Premium Security Suite Control Center access the menu item Help / License file



Note

In Windows Vista the User Account Control dialog box appears. Log in as administrator if appropriate. Click **Continue**.

- ▶ Highlight the license file and click **Open**.
 - ↳ A message appears.
- ▶ Click **OK** to confirm.
 - ↳ The license is activated.
- ▶ If necessary, restart your system.

5.2.2 Avira Premium Security Suite automatic update



An update job has been pre-installed to update Avira Premium Security Suite every 24 hours if an internet connection is available and additionally when an internet connection is established.

To create a job in AntiVir Scheduler to update Avira Premium Security Suite automatically:

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



- ▶ Click on 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**
 - **Once**
 - **Login**
-



We recommend that you update Avira Premium Security Suite regularly and often, e.g. every 6 hours.

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

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

- **Also start job when internet connection is established**

In addition to the defined frequency, the job is carried out when an internet connection is set up.

In addition to the defined frequency, the job is carried out when an Internet connection is set up.

- **Repeat job if the time has already expired**

Past jobs are carried out that could not be carried out 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 :: Scanner** section with the status activated (check mark).
- ▶ Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:



View properties of a job



Modify job



Delete job

5.2.3 Start a manual update

You have various options for starting an Avira Premium Security Suite update manually: When an update is started manually, the virus definition file and search 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 Avira Premium Security Suite update manually:

- ▶ With the right-hand mouse button, click on the Avira Premium Security Suite tray icon in the taskbar.
 - ↳ A context menu appears.
- ▶ Select **Start update**.
 - ↳ The dialog box *Avira Premium Security Suite Updater* appears.
 - OR -
- ▶ In the Control Center, select the **Overview :: Status** section.
- ▶ In the *Last update* field, click on the link **Start update**.
 - ↳ The Avira Premium Security Suite Updater dialog box appears.
 - OR -
- ▶ In the Control Center, in the **Update** menu, select the menu command *Start update*.
 - ↳ The Avira Premium Security Suite Updater dialog box appears.



We strongly recommend regular automatic updates for Avira Premium Security Suite, e.g. every 6 hours.



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

5.2.4 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.
- Create and apply new scan profile
if you want to create your own scan profile.

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

- In Windows XP and 2000:



This icon starts the scan via a scan profile.

- In Windows Vista:

In Microsoft Windows Vista, the control center at the moment only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the control centre 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:

- ▶ In the Control Center select the **Local protection :: Scanner** section.
 - ↳ Predefined scan profiles appear.
- ▶ Select one of the predefined scan profiles.
-OR-
- ▶ Adapt the scan profile *Manual selection*.
-OR-
- ▶ Create a new scan profile
- ▶ Click on the (Windows XP:  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.

If you want to adapt a scan profile:


- ▶ In the scan profile, expand **Manual Selection** the file tree so that all the drives and directories you want to scan are open.
 - Click on the + symbol: The next directory level is displayed.
 - Click on the - symbol: The next directory level is hidden.


- ▶ Highlight the nodes and directories you want to scan by clicking on the relevant box of the appropriate directory level.

The following options are available, Select directories:

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

If you want to create a new scan profile:

- ▶ Click on the  **Create new profile** icon.
 - ↳ The profile *New profile* appears below the profiles previously created.

- ▶ Where appropriate, rename the scan profile by clicking on the icon .

- ▶ Highlight the nodes and directories to be saved by clicking on the check box of the respective directory level.

The following options are available, Select directories:

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

5.2.5 On-demand scan: Scan for viruses and malware using Drag&Drop

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

- ✓ Open the Control Center of Avira Premium Security Suite.
- ▶ Highlight the file or directory you want to scan.
- ▶ Use the left-hand mouse button to drag the highlighted file or directory into the *Control Center*.
 - ↳ The *Luke Filewalker* window appears and an on-demand scan is started.
 - ↳ When the scan is completed, the results are displayed.


5.2.6 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 or directory 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 the on-demand scan starts.
 - ↳ When the scan is completed, the results are displayed.

5.2.7 On-demand scan: Automatically scan for viruses and malware

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

- ▶ In the Control Center select the **Manager::** section **Scheduler**.
- ▶ Click on 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**
 - **Once**
 - **Login**
- ▶ Where appropriate, specify a date according to the selection.
- ▶ Where appropriate, select the following additional options (availability depends on job type):
 - **Repeat job if the time has already expired**
 - ↳ Past jobs are carried out that could not be carried out 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**.
 - ↳ The job you have just initiated is shown as activated (check mark) on the start page of the *Manager :: Scheduler* section.
- ▶ Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:



View properties of a job



Modify job





Delete job

5.2.8 On-demand scan: Targeted scan for active rootkits

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

To scan for active rootkits systematically:

- ▶ In the Control Center select the **Local protection :: Scanner** section.
 - ↳ Predefined scan profiles appear.
- ▶ Select the predefined scan profile **Scan for rootkits**.
- ▶ Where appropriate, highlight other nodes and directories to be scanned by clicking on the check box of the directory level.
- ▶ Click on the (Windows XP:  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.

5.2.9 Reacting to detected viruses and malware

For the individual protection components of Premium Security Suite, you can define how Premium Security Suite reacts to a detected virus or unwanted program in the configuration under the section *Action for concerning files*.

- **Interactive**

When this option is enabled, 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**

When this option is enabled, if a virus or unwanted program is detected, no dialog box appears and you cannot select an action. The component reacts in accordance with your predefined settings.

If you have selected the option *Interactive* for your protection components, Avira Premium Security Suite gives you the following options for actions to take:



Note

Which options are displayed depends on the operating system and the module, (AntiVir Guard, AntiVir Scanner or AntiVir MailGuard), that makes the detection.

- **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 date or, if necessary, sent to Avira GmbH.

- **Delete**

The file is deleted but can be recovered with the appropriate tools (e.g. *Avira UnErase*). This allows the virus signature to be recovered. This process is significantly quicker than *Overwrite and delete*.

- **Overwrite and delete**

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

- **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.

- **Deny access**

If this option is enabled, the detection is only entered in the report file.

- **Ignore**

Avira Premium Security Suite takes no further action. The infected file remains active on your computer.



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

- **Take no further action**

Access to the file is blocked.

- **Copy file in quarantine before action**

This option can only be selected if one of the options Repair, Delete, Overwrite and delete is selected.

- **Apply selection to all subsequent detections**

The action selected for this detection is applied to the next detection.



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

- ▶ You can also send files reported by the heuristic to us for analysis.

For example, you can upload these files to our website:

<http://www.avira.com/file-upload>

You can identify files reported by the heuristic from the designation *HEUR/* or *HEURISTIC/* that prefixes the file name, e.g.: *HEUR/testdatei.**.

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

- Delete the entire archive
- Rename the archive
- Move archive to Quarantine




Individual infected files cannot be deleted from the archive.

5.2.10 Quarantine: Handling quarantined files (*.qua)

To handle quarantined files:

- ▶ In the Control Center select **Manager :: 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 Avira Premium Security Suite virus definition file 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 are unsure whether the files can be safely deleted:

- ✓ Configured email settings

- ▶ Send the files to Avira GmbH for analysis. To do this, click on 

You can also restore the files in Quarantine:

- see Chapter: Quarantine: Restoring files in quarantine

5.2.11 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 at the moment only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the control centre 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:




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 **Manager :: Quarantine** section.
-




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 on the (Windows 2000/XP:  , Windows Vista ) icon.

This option is not available for emails.




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

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

- ▶ Click **Yes**.

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

To restore a file to a specified directory:

- ▶ Highlight the file and click on 


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

- ▶ Click **Yes**.

- ↳ The Windows default window for selecting the directory appears.
- ▶ Select the directory to restore the file to and confirm.
- ↳ The file is restored to the selected directory.

5.2.12 Quarantine: move suspicious files to quarantine

To move a suspect file to quarantine manually:

- ▶ In the Control Center select **Manager :: 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 AntiVir Scanner:

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

5.2.13 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 and customized scan profiles):

- ✓ In the Control Center go to the section **Local protection :: Scanner**.
- ▶ 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.


5.2.14 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 the Avira Premium Security Suite Control Center.

To create a desktop shortcut to the scan profile:

✓ In the Control Center go to the section **Local protection :: Scanner**.

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

▶ Click on the icon .

↳ The desktop shortcut is created.

5.2.15 Events: Filter events

In Control Center, under **Overview :: Events** events are displayed that have been generated by Premium Security Suite program components. (analogous to the event display of your Windows operating system). The program components are:

- Updater
- Guard
- MailGuard
- Scanner
- Scheduler
- Firewall

The following event types are displayed:

- Information
- Warning
- Error
- Detection

To filter displayed events:

▶ In 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.

5.2.16 MailGuard: Exclude email addresses from scan

To define which email addresses (senders) are excluded from the MailGuard scan (whitelisting):

- ▶ Go to Control Center and select the section **Online protection :: MailGuard**.
 - ↳ The list shows incoming emails.
- ▶ Highlight the email you want to exclude from the MailGuard scan.
- ▶ Click on the appropriate icon to exclude the email from the MailGuard scan:



In future, the selected email address will no longer be scanned for viruses and unwanted programs.



In the future, the selected email address will no longer be scanned for spam.

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



Only exclude email addresses from the MailGuard scan if the senders are completely trustworthy.





You can add other email addresses to the exclusion list or remove email addresses from the exclusion list in the configuration under MailGuard :: General :: Exceptions .

5.2.17 MailGuard: Train the anti-spam module

The anti-spam module contains a training database. Your individual categorization criteria are recorded in this training database. Over time, the internal filter, algorithms and evaluation criteria for spam adapt themselves to your personal criteria.

To categorize emails for the training database:

- ▶ Go to Control Center and select the section **Online protection :: MailGuard**.
 - ↳ The list shows incoming emails.
- ▶ Highlight the email you want to categorize.

- ▶ Click on the appropriate icon to identify the email as either spam  or wanted, i.e. 'good' Email .

- ↳ The email is entered into the training database and applied to the next spam recognition process.



You can delete the training database in the configuration under MailGuard :: General :: AntiSpam.

5.2.18 Firewall: Select the security level for Firewall

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

The following security levels are available:

- **Low**
- Flooding and port scan are detected.
- **Medium**
- Suspicious TCP and UDP packages are discarded.
- Flooding and port scan are prevented.
- **High**
- Computer is invisible on the network.
- Connections from outside are blocked.
- Flooding and port scan are prevented.
- **User**
- User-defined rules: if this security level is selected, the program automatically recognizes that the adapter rules have been modified.



The default security level setting for all predefined Avira Firewall rules is **Medium**.

To define the security level for Firewall:

- ▶ In Control Center, select the section Online **Protection :: Firewall**.
- ▶ Move the slider to the required security level.
 - ↳ The selected security level is applied immediately.

5.2.19 Backup: Create backups manually

The backup tool in Control Center lets you backup your personal data quickly and easily. In Avira Backup you can create so-called mirror backups which let you save and store your most recent data using a minimum of resources. Avira Backup lets you scan your data for viruses and malware during the backup process. Infected files are not saved.



In contrast to version backups, mirror backups do not save individual backup versions. The mirror backup contains the data stock at the time of the last backup. If, however, files from the saved data stock are deleted, no match takes place in the following backup, i.e. the deleted files are still available in the backup.



With the default settings of Avira Backup only modified files are saved, and files are scanned for viruses and malware. You can change these settings in the configuration under Backup::Settings.

To save your data using the backup tool:

- ▶ In the Control Center go to the **Tools:: Backup** section.
 - ↳ Preset backup profiles appear.
- ▶ Select one of the preset backup profiles.


-OR-

- ▶ Adapt the backup profile *Manual selection*.

-OR-

- ▶ Create a new backup profile
- ▶ Enter a save location for the selected profile in the *Destination directory* box.

The save location for the backup can be a directory on your computer, or on a connected network drive, or a removable disk, such as a USB stick or diskette.

- ▶ Click on the icon 
 - ↳ The window *Avira Backup* appears and the backup starts. The status and results of the backup are displayed in the backup window.



If you want to modify a backup profile:

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

The following options are available, Select directories:

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

If you want to create a new backup profile:

- ▶ Click on the icon  **Create new profile.**
 - ↳ The profile *New profile* appears below the profiles previously created.
- ▶ Where appropriate, give the backup profile a name by clicking on the icon .
- ▶ Highlight the nodes and directories to be saved by clicking on the check box of each directory level.


The following options are available, Select directories:

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

5.2.20 Backup: Create automatic data backups

This shows you how to initiate a job to create automatic data backups:

- ▶ In the Control Center go to the **Manager::Scheduler** section.

- ▶ Click on 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 **Backup job**.

- ▶ Click **Next**.

↳ The dialog box *Select profile* appears.

- ▶ Select the profile to be scanned.



Only backup profiles for which a save location has been stipulated are displayed.

- ▶ Click **Next**.

↳ The dialog box *Time of job* appears.

- ▶ Select a time for the scan

- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Once**
- **Login**
- **Plug&Play**

A backup is always created for the Plug&Play event if the removable disk selected as the save location of the backup profile is connected to the computer. The backup event Plug&Play requires a USB stick to be entered as a save location.

- ▶ 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 carried out that could not be carried out 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 backup window
- **Hide:** no backup window

- ▶ Click **Finish**.
 - ↳ The job you have just initiated is shown as activated (check mark) on the start page of the *Manager :: Scheduler* section.
- ▶ Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:



View properties of a job



Modify job



Delete job

6 Scanner

With Avira Premium Security Suite you can carry out manual scans (on-demand scans) for viruses and unwanted programs in several ways.

- **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 Avira Premium Security Suite 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 Avira Premium Security Suite 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.

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 search engine. To carry out updates, the component AntiVir Updater is integrated into Premium Security Suite. AntiVir Updater ensures that Avira Premium Security Suite is always up-to-date and able to deal with the new viruses that appear every day. AntiVir Updater updates the following components:

- Virus definition file:

The virus definition file contains the virus patterns of the harmful programs used by Premium Security Suite to scan for viruses and malware and repair infected objects.

- Search engine:

The search engine contains the methods used by Premium Security Suite 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 search engine are up-to-date and if necessary implements an update. Depending on the settings in the configuration, AntiVir Updater also carries out a product update or informs you of the product updates available. After an update Premium Security Suite does not have to be restarted.



For security reasons, the Avira Premium Security Suite Updater checks whether the Windows host file of your computer was altered to the effect that, for example, the Avira Premium Security Suite update URL was manipulated by malware and diverts the Avira Premium Security Suite Updater to unwanted download sites. If the Windows host file has been manipulated, this is shown in the Avira Premium Security Suite Updater report file.

In the Control Center under Scheduler, you can organize update jobs which are carried out by AntiVir Updater at the intervals stipulated. An update job is created by default after installation of Premium Security Suite. You also have the option to start an update manually:

- in 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 Avira Premium Security Suite Configuration under General:: Update.

8 Backup

There are various options available to you for creating a backup of your data:

Backup via the backup tool

You can use the backup tool to select or create backup profiles and start a backup of a selected profile manually.

Backup via a backup job in Scheduler

Scheduler gives you the option of creating scheduled or event-controlled backup jobs. Scheduler automatically executes the backup jobs. This process is particularly useful if you want to make regular backups of specific data.

9 FAQ, Tips

This chapter provides a collection of frequently asked questions (FAQs) relating to Avira Premium Security Suite, a troubleshooting section and tips and tricks for using Avira Premium Security Suite.

see Chapter: Frequently asked questions (FAQs)

see Chapter: Troubleshooting

see Chapter: Keyboard commands

see Chapter: Windows XP Security Centre

see Chapter: Command line scanner

9.1 Frequently asked questions (FAQs)

Here are the answers to frequently asked questions.

Where can I get Avira Premium Security Suite?

Download the program from the website <http://www.avira.com>.

Will I receive a CD of Avira Premium Security Suite?

The program is only available by download from our website <http://www.avira.com>.

What do I do with the hbedv.key license file?

Licenses available for purchase are activated with the license file hbedv.key. The license file is loaded via the program. See also Control Center :: Help :: Load license file

Should I archive the license file?

After being activated, the file is located in the program directory of Avira Premium Security Suite. This directory is C:\Program Files\Avira Premium Security Suite by default. We recommend saving another copy of the license file somewhere else (e.g. on a floppy disk or in another directory), since the license file is deleted when the program directory of Avira Premium Security Suite is removed.

What should I be aware of with a new installation of Avira Premium Security Suite?

Save the license file (hbedv.key) in another directory or on a floppy disk, for example, since the license file is deleted when Avira Premium Security Suite is removed. The license file is found in the program directory C:\Program Files\Avira Premium Security Suite by default.

When will my license expire?

This information is found in the Control Center

– unter Overview :: Status

- OR -

– in the menu item Help :: About Premium Security Suite... :: License information.

Where can I find detailed version information?

Detailed version information is found in the menu item Help :: About Premium Security Suite... :: Version information of the Control Center.

Which settings should I make for Avira Premium Security Suite?

Avira Premium Security Suite is pre-configured with practical settings after installation. You can adapt these settings, depending on the desired level of security (e.g. heuristic detection or expanding the scan to all file and archive types).

Can I protect settings with a password?

Yes, in the Avira Premium Security Suite Configuration (Expert mode) under General :: Password.

How can I check whether Avira Premium Security Suite is up-to-date?

Avira Premium Security Suite is up-to-date when you have the most current virus definition file. This file is usually updated several times a day.

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

- ▶ Performs an update.

- OR -

- ▶ Visit the website <http://www.avira.com> and read through the following information:

- Current VDF version number
- Date and time of publication of the current VDF

- ▶ In the Control Center, select the section Overview :: Status.
- ▶ Compare this information with the information on the website.

If the information is identical: The Avira Premium Security Suite is up-to-date.

If the information is not identical: The Avira Premium Security Suite is not up-to-date. Carry out an update.

What is an incremental VDF update (IVDF)?

The Avira Premium Security Suite supports the so-called "incremental update" of the virus definition file. Incremental VDF updates (IVDF update) work as follows: daily updates of the VDF file are not downloaded in the form of one large VDF file but as small VDF files (name: antivir3.vdf) that are only a few kilobytes in size and which only contain virus patterns that have been newly added.

This daily VDF file supplements the weekly VDF (Name: antivir2.vdf), the monthly VDF (Name: antivir1.vdf) and the so-called Basic VDF (Name: antivir0.vdf), which are already installed with every Avira Premium Security Suite program package as standard.

If one of the so-called VDF files reaches a determined size its content is transferred to the next higher VDF file, which has to be downloaded additionally.

An advantage of the incremental VDF process is that the download volume is extremely small. This leads to extremely short download times and costs, also if the download is performed via an Internet modem connection.

What is the difference between AntiVir Guard and AntiVir MailGuard?

AntiVir Guard scans every changing file on the computer for viruses and malware.

AntiVir MailGuard scans all incoming emails and their attachments for viruses and malware.

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

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

The on-demand scan is started manually. Specific drives can be systematically scanned for viruses and malware (on-demand scanning).

Is there risk to security if AntiVir MailGuard is not used?

If AntiVir Guard is active, there is no direct security risk. However, AntiVir MailGuard can already remove emails and attachments affected by viruses and malware before they reach the email program.

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

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

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

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

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

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

This is how Avira Premium Security Suite should react to the eicar test virus if a default installation with the preset file types was carried out:

– *eicar.com*

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

– *eicar.com.txt*

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

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

– *eicar_com.zip*

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

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

– *ecarcom2.zip*

Here is the test virus packed in a Zip archive which is itself packed in a Zip archive. These are difficult conditions for a virus scanner. The reactions of AntiVir Guard and the direct scan correspond to those of *ecar_com.zip*.

With the direct scan, the test virus is detected and the message window (see above) appears. AntiVir Guard first reacts with the second, last unpacking, when the *ecar.com* file is present.

Is a manual scan necessary from time to time?

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

Does WebGuard affect how quickly internet sites load?

WebGuard is an HTTP proxy without any cache. For this reason, websites that are called up more than once will not be displayed more quickly. WebGuard only affects the behaviour of the web browser during the loading of a website or while data is being transferred. All data requested and transferred is first fully checked by WebGuard for viruses and unwanted programs before being passed on to the web browser for display. Hence the content of requested websites is not displayed incrementally as is common. Instead the web page is shown in its entirety after a short delay. To prevent delays for streaming audio and video, you can exclude those types of content from the WebGuard scanning. Please be aware of the fact that automatic forwarding can create the impression of a delay. If this makes you click more than once on links which are valid for one instance (click) only, then access will be denied. This is not a function of WebGuard, but is inherent in the server implementation.

9.2 Troubleshooting

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

The error message The license file cannot be opened appears.

Cause: The file is encrypted.

▶ To activate the license, you do not need to open the file, but rather you save it in the program directory of Avira Premium Security Suite. See also Avira Premium Security Suite License Manager.

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

Cause: Your Internet connection is inactive. This is why Avira Premium Security Suite cannot find the web server on the Internet.

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

Cause: The proxy server cannot be reached.

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

Cause: The *update.exe* file is not fully approved by your personal firewall.

▶ Ensure that the *update.exe* file is fully approved by your personal firewall.

Otherwise:

- ▶ Check your settings in the Avira Premium Security Suite Configuration (Expert mode) under General :: Update.

Viruses and malware cannot be moved or deleted.

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

- ▶ Update Avira Premium Security Suite.
- ▶ If you use the operating system Windows XP, deactivate System Restore.
- ▶ Start the computer in Safe Mode.
- ▶ Start Avira Premium Security Suite and the Avira Premium Security Suite 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 Tray Icon shows an inactive state.

Cause: AntiVir Guard is deactivated.

- ▶ In Control Center, click on the section Overview :: Status, find the field AntiVir Guard and click on the **Enable** link.

Cause: AntiVir Guard is being 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. The same applies to AntiVir MailGuard.

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 Premium Security Suite Guard". "Automatic" must be entered as the startup type and "Started" as the service 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.

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

- ▶ Select Guard :: Scan :: Exceptions in the Avira Premium Security Suite Configuration (Expert mode) and enter the process names of the back-up software.

My firewall reports AntiVir Guard and AntiVir MailGuard immediately after activation.

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

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

AntiVir MailGuard does not work

Please check correct functioning of AntiVir MailGuard with the aid of the following checklists if problems occur with AntiVir MailGuard.

Checklist

- ▶ Check whether your mail client communicates with the mail server via IMAP. This protocol is currently not supported.
- ▶ Check whether your mail client logs in on the server via Kerberos, APOP or RPA. These verification methods are currently not supported.
- ▶ Check whether your mail client logs in on the server via SSL (frequently also known as TSL - Transport Layer Security). AntiVir MailGuard supports SSL, but without scanning the encrypted emails for viruses and unwanted programs. The condition for this is that connection is made via port 995 and not via the normal POP3 port 110. This port is also frequently referred to as "Alternate port". Most email servers also support SSL via this port.
- ▶ Is the AntiVir MailGuard service active? If necessary, enable the service: In the taskbar, select "Start | Settings | Control Panel". Start the configuration panel "Services" with a double-click (under Windows 2000 and Windows XP the services applet is located in the sub-directory "Administrative Tools"). Find the entry "Avira Premium Security Suite MailGuard". "Automatic" must be entered as the startup type and "Started" as the status. If necessary, start the service manually by selecting the relevant line and the button "Start". If an error message appears, please check the event display. If this is not successful, you may have to completely deinstall Avira Premium Security Suite via "Start | Settings | Control Panel | Add or Remove Programs", restart the computer and then reinstall Avira Premium Security Suite.

General

- ▶ AntiVir MailGuard does not currently support the so-called IMAP (Internet Message Access Protocol), i.e. if your email program communicates with the email server via this protocol, you are not protected against viruses or unwanted programs.
- ▶ POP3 connections encrypted via SSL (Secure Sockets Layer, also frequently referred to as TLS (Transport Layer Security)) cannot currently be protected and are ignored.
- ▶ Verification to the mail server is currently only supported via "passwords". "Kerberos" and "RPA" are not currently supported.
- ▶ Avira Premium Security Suite does not check outgoing emails for viruses and unwanted programs.



Note

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

There is no network connection available in a virtual machine (e.g. VMWare, Virtual PC, ...) if Avira Firewall is installed on the host machine and the security level of Avira Firewall is set to medium or high level.

If Avira Firewall is installed on a computer on that additionally a virtual machine (for example VMWare, Virtual PC, ...) is running, the firewall will block all network connections for the virtual machine when the security level of the Avira Firewall is set to medium or high. If the security level is set to low, the network connections work as expected.

Cause: The virtual machine emulates through software a network card. This emulation encapsulates the data packages of the guest system in special packages (UDP packages) and routes them via the external gateway back to the host system. Avira Firewall rejects these packages coming from outside starting from security level medium.

To avoid this behavior do the following:

- ▶ In Control Center, select the section **Online protection :: Firewall**.
- ▶ Click the **Configuration** link.
- ▶ The *Avira Premium Security Suite Configuration* dialog box is displayed. You are in the configuration section *Application rules*.
- ▶ Activate the **Expert mode** option.
- ▶ Select the configuration section **Adapter rules**.
- ▶ Click **add rule**.
- ▶ Select **UDP** in the section *Incoming rules*.
- ▶ Type the **name** of the rule in the Section Name of the rule .
- ▶ Click **OK**.
- ▶ Check if the rule is directly above the rule **Deny all IP packets**.



This rule is potentially dangerous because it will allow UDP packets without any filtering! After working with the virtual machine change to your previous security level.

Virtual Private Network (VPN) Connection is blocked, if the security level of Avira Firewall is set to medium or high.

Cause: This problem is caused by the last rule **Deny all IP packets** which discards all packets that do not comply with any of the rules above it. The type of packages dispatched by the VPN software (so called GRE packets) do not fit into the other categories and therefore they are filtered by this rule.

Replace the rule **Deny all IP packets** with two new rules which will deny the TCP and UPD packets. In this way there is the possibility to allow packets of other protocols.

An email sent via a TSL connection has been blocked by MailGuard.

Cause: Transport Layer Security (TLS: encryption protocol for data transfers on the internet) is not supported by MailGuard at this time. The following options are available for sending the email:

- ▶ Use a port other than Port 25 which is used by SMTP. This avoids MailGuard monitoring.
- ▶ Disconnect the encrypted TSL connection and disable TSL support in your email client.
- ▶ Disable (temporarily) monitoring of outgoing emails by MailGuard in the configuration under MailGuard::Scan.

9.3 Shortcuts

Keyboard commands - also called shortcuts - offer a fast possibility to navigate, to retrieve individual modules and to start actions through Avira Premium Security Suite.

Below we provide you with an overview of the available keyboard commands in Avira Premium Security Suite. Please find further indications regarding the functionality in the corresponding chapter of the help.

In dialog boxes

Shortcut	Description
Ctrl + Tab Ctrl + Page down	Go to next section.
Ctrl + Shift + Tab Ctrl + Page up	Go to previous 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.

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.
Shitf + 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.
F6	Shift between the navigation and the subject window.
Page up Page down	Browse through a subject.

In the Control Center**General**

Shortcut	Description
F1	Display help
Alt + F4	Close Control Center
F5	Refresh
F8	Open configuration
F9	Start update

Scanner section

Shortcut	Description
F2	Rename selected profile
F3	Start scan with the selected profile
F4	Create desktop link for the selected profile
Ins	Create new profile
Del	Delete selected profile

Firewall section

Shortcut	Description
Enter	Properties

Quarantine section

Shortcut	Description
F2	Rescan object
F3	Restore object
F4	Send object
F6	Restore object to...
Enter	Properties
Ins	Add file
Del	Delete object

Scheduler section

Shortcut	Description
F2	Edit job
Enter	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)

section

Shortcut	Description
F3	Export event(s)
Return	Display event
Del	Delete event(s)

9.4 Windows Security Centre

- Windows XP Service Pack 2 or higher -

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.

The Windows Security Center and Avira Premium Security Suite

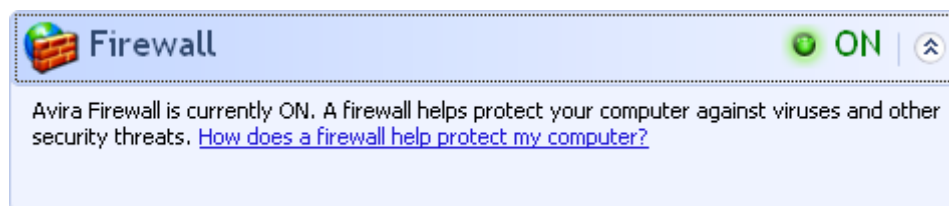
Firewall

You may receive the following information from the Security Center with regard to your firewall:

- Firewall ACTIVE / Firewall on
- Firewall INACTIVE / Firewall off

Firewall ACTIVE / Firewall off

After installation of Avira Premium Security Suite and turned off Windows Firewall, you receive the following message:



Firewall INACTIVE / Firewall off

You receive the following message if you disable the Avira Firewall.



You can enable or disable the Avira Firewall via the index card Status of the Avira Premium Security Suite Control Center.



If you turn the Avira Firewall off, your computer is no longer prevented by unauthorized users from gaining access to it through a network or the Internet.

Virus protection software / Protection against malicious software

You may receive the following information from the Windows Security Center with regard to your virus protection.

Virus protection NOT FOUND

Virus protection OUT OF DATE

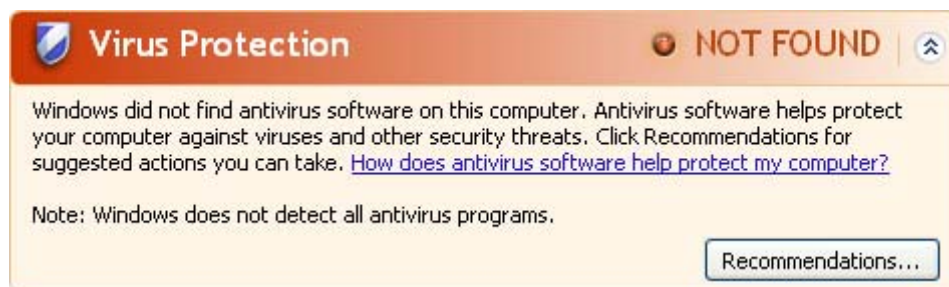
Virus protection ON


Virus protection OFF

Virus protection NOT MONITORED

Virus protection NOT FOUND

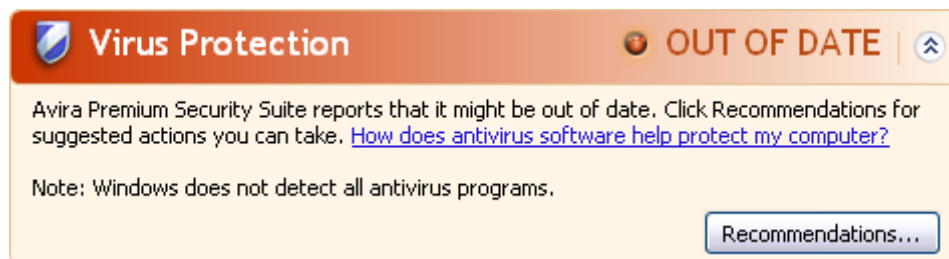
This information of the Windows Security Center appears when the Windows Security Center has not found any anti-virus software on your computer.




 Install Avira Premium Security Suite on your computer to protect it against viruses and other unwanted programs!

Virus protection OUT OF DATE

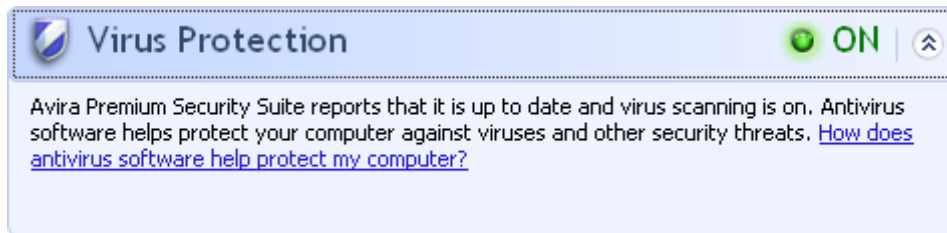
If you have already installed Windows XP Service Pack 2 or Windows Vista and then install Avira Premium Security Suite or you install Windows XP Service Pack 2 or Windows Vista on a system on which Avira Premium Security Suite has already been installed, you receive the following message:



 In order for the Windows Security Center to recognize Avira Premium Security Suite as up to date, an update must be carried out after installation. Update your system by carrying out an Avira Premium Security Suite update.

Virus protection ON

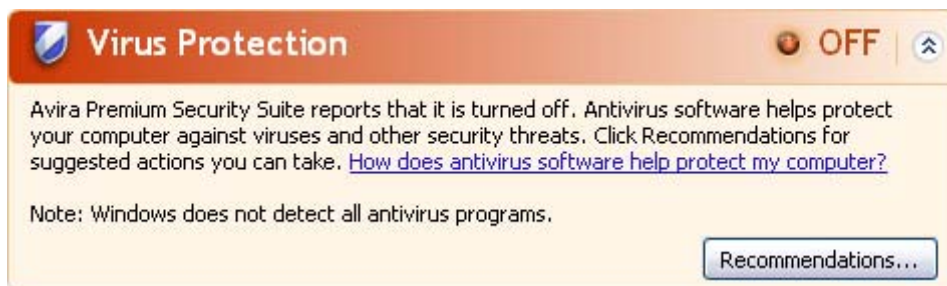
After installation of Avira Premium Security Suite and a subsequent update, you receive the following message:



Avira Premium Security Suite is now up to date and the AntiVir Guard is enabled.

Virus protection OFF

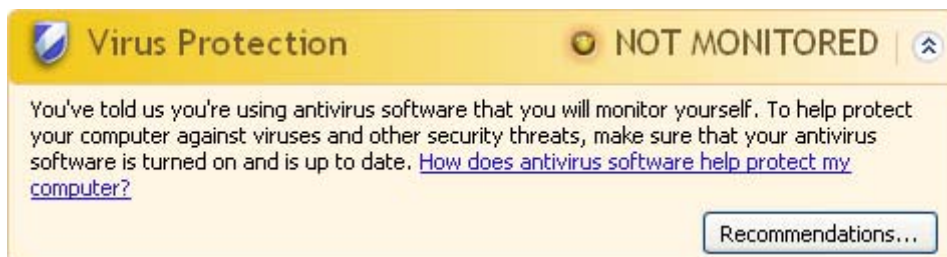
You receive the following message if you disable the AntiVir Guard or stop the Guard service.



You can enable or disable AntiVir Guard in the section Overview :: Status of Avira Premium Security Suite Control Center. You can also see that the AntiVir Guard is enabled if the red umbrella in your taskbar is open.

Virus protection NOT MONITORED

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



The Windows Security Center is supported by Avira Premium Security Suite. You can enable this option at any time via the button "Recommendations..."



Even if you have installed Windows XP Service Pack 2 or Windows Vista, you still require a virus protection solution, e.g. Avira Premium Security Suite. 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!

10 Viruses and more

10.1 Extended threat categories

Dialer (DIALERS)

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 you to directly ask your telephone provider to block this number range to be immediately protected against undesired dialers (0190/0900 dialers).

Avira Premium Security Suite 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.

Avira Premium Security Suite detects computer games. If the **Games** option is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira Premium Security Suite 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 may themselves may cause real damage.

Thanks to the extension of its scanning and identification routines, Avira Premium Security Suite 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 Extended threat categories, a corresponding alert is issued if a joke program is detected.

Security Privacy Risk (SPR)

Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.

Avira Premium Security Suite 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 Avira Premium Security Suite 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.

Avira Premium Security Suite detects "backdoor control software". If the option **Backdoor Clients** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira Premium Security Suite detects such software.

Adware/Spyware (ADSPY)

Software that displays advertising pop-ups or software that very often without the user's consent sends user specific data to third parties and might therefore be unwanted.

Avira Premium Security Suite detects "Adware/Spyware". If the option **Adware/Spyware** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira Premium Security Suite detects such software.

Unusual Runtime Compression Tools (PCK)

Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

Avira Premium Security Suite detects "Unusual runtime Compression Tools". If the option **Unusual runtime Compression Tools** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira Premium Security Suite 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.

Avira Premium Security Suite detects "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 Avira Premium Security Suite 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.

Avira Premium Security Suite detects "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under Extended threat categories, you receive a corresponding alert if Avira Premium Security Suite detects such behavior.

Application (APPL)

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

Avira Premium Security Suite detects "Application (APPL)". If the option **Application (APPL)** is enabled with a check mark in the configuration under Extended threat categories, you receive a relevant alert if Avira Premium Security Suite detects such behavior.

10.2 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 going around 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. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

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), which 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., partly without the affected PC user's knowledge. The main potential of Bot-Nets is that the networks can achieve dimensions on thousands of computers and its bandwidth sum bursts 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. A form of an exploit for example are attacks from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

Hoaxes

The users have obtained virus alerts from the Internet for a few years and alerts against viruses in other networks that are supposed to spread via email. These alerts are spread per 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. It has the function to monitor a network and to protocol attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a Honeypot, it is logged and an alert is triggered.

Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses do consequently 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 to attach 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 his 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 can consequently not 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. We are talking about 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.

11 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

see Chapter: Your feedback for more security

11.1 Contact address

If you have any questions or requests concerning the Avira Premium Security Suite product range, we will be pleased to help you. If you require product information or other information, you can contact the address given below. General information on us and our products can also be obtained from our website <http://www.avira.com>.

Avira GmbH

Lindauer Str. 21

D-88069 Tett nang

Germany

Internet: <http://www.avira.com>

Email: info@avira.com

11.2 Technical support

Avira Premium Security Suite 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/premium-suite-support>.

If you have questions, we recommend that you contact your local dealer first.

Support-Hotline:

Germany: 0900 10 11 900 (1,99 Euro/Min* for calls from the local network)

Austria: 0900 51 03 61 121 (2,16 Euro/Min for calls from the local network)

Switzerland: 0900 51 03 61 (4,23 CHF/Min for calls from the local network)

* Prices are subject to change.

Monday to Friday between 10 a.m. and 7 p.m.

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

- **License information.** These can be found in the Avira Premium Security Suite Control Center under the menu item .
- **Version information.** You can find this in Avira Premium Security Suite Control Center under the menu item Help :: About Premium Security Suite :: 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.

11.3 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.

- In Quarantine manager select the Control Centerfile file and use the context menu or corresponding button to select the item Send file.
- Send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

You can also send us the suspect file via our website.

11.4 Report false positive

If you believe that Avira Premium Security Suite reports something about a file that is most likely "clean", send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus@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).

11.5 Your feedback for more security

The security of our customers plays a central role at Premium Security Suite. Because of this reason, we don't only have an in-house expert team who tests the quality and security of every Premium Security Suite solution before the product is released. We also attach great importance to the indications regarding security relevant gaps which could develop and we treat those frankly.

If you think you have detected a security gap in one of our products, please send us an email to vulnerabilities@avira.com.

12 Reference: Configuration

The configuration reference documents all configuration options available in Avira Premium Security Suite.

12.1 Scanner

The Scanner section of the Avira Premium Security Suite Configuration is responsible for the configuration of the on-demand scan.

12.1.1 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.



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 Avira Premium Security Suite. This means that Avira Premium Security Suite decides respective of their content, whether the files are scanned or not. 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.



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**.



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 window 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.



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 only 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.

Scan memory

If this option is enabled, the Scanner scans the main memory of the workstation with every on-demand scan. This option is enabled as the default setting and is recommended.



Important

This function should always be enabled in order to obtain maximum protection against viruses or unwanted programs. If a virus or unwanted program is active in the memory, all files that are scanned may be infected.

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.

Follow symbolic links

If this option is enabled, Scanner performs a scan that follows all icon shortcuts in the scan profile or selected directory and scans the linked files for viruses and malware. This option is only available for Windows XP and Windows Vista and its default setting is disabled.

Search for Rootkits before scan

If this option is enabled and a scan is started, 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.



Under 64 bit systems the rootkit scan is not yet available!

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 window of the "Luke Filewalker". If you have disabled this setting, the button **Stop** in the window "Luke Filewalker" 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 setting is activated by default and is recommended.

Medium

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

High

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

12.1.1.1. Action for concerning files

Action for concerning files

You can define actions that the Scanner is to carry out when a virus or unwanted program is detected.

Interactive

When this option is enabled, on detection of a virus or unwanted program during an on-demand scan, a dialog window appears in which you can select what is to be done with the affected file. This option is enabled as the default setting.

Further information is available [here](#).

Automatic

If this option is enabled and a virus or unwanted program is detected, no dialogue appears in which an action can be selected. The Scanner reacts according to the settings made by you in this section.

Copy file to quarantine before action

If this option is enabled, the Scanner creates a back-up 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 back-up copy to the Avira Malware Research Center for further investigation.

Primary action

Primary action is the action carried out when the Scanner finds a virus or an unwanted program. If the option **repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.



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.



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, but can be restored if necessary with relevant tools (e.g. Avira UnErase). This means that the virus pattern could be detected again. This process is much faster than "overwrite and delete".

overwrite and delete

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

rename

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

ignore

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



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, but it can be restored if necessary with relevant tools (e.g. Avira UnErase). This means the virus pattern could be detected again. This process is much faster than "overwrite and delete".

overwrite and delete

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

rename

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

ignore

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



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.

12.1.1.2. Further actions

Acoustic alert

Acoustic alert

If this option is enabled, Scanner plays a sequence of notes in the event of a detection. This option is activated by default.

Wave file

In this input box you can enter the name and the associated path of an audio file of your choice. If this box is empty, the default alert sound is played.



The button opens a window in which you can select the required file with the aid of the file explorer.

Test acoustic alert

This button is used to test the selected wave file.

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, for this every file must be opened - which reduces the scanning speed. For 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.



Only those archive types are supported, which are marked in the archive list.

Limit recursion depth

Unpacking and scanning deeply interlaced 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.



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 required recursion depth directly or alter it with the arrow keys to the right of the input box.

Default values

The button restores the pre-defined values for scanning archives.

12.1.1.3. Archive list

In this display area you can set which archives the Scanner should scan. For this, you must select the relevant entries.

12.1.1.4. 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!



The entries on the list must not result more than 6000 characters in total.



These files are not included in a scan!



The files included in this list are entered 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 in the list. This button is not active if no entry is selected.

12.1.1.5. Heuristic

This configuration section contains the settings for the heuristic of the Avira Premium Security Suite search engine.

Avira Premium Security Suite contains very powerful heuristic, which can also detect unknown (new) viruses, worms or Trojans. This is done with a comprehensive analysis and examination of the relevant codes for functions that are typical of viruses, worms or Trojans. If the code examined fulfils these characteristic criteria, it is reported as being suspect. However, this does not necessarily mean that the code is in actual fact a virus, a worm or a Trojan; it may also be a false alert. The user has to decide what to do with the relevant code, for example based on his/her knowledge of whether the source containing the suspect code is reliable.

Macrovirus heuristic

Macrovirus heuristic

Avira Premium Security Suite contains a very powerful macrovirus heuristic. If this option is enabled, all macros 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.

Win32 file heuristic

Avira Premium Security Suite contains a very powerful heuristic for Windows file viruses, worms and Trojans, which can also detect unknown viruses, worms and Trojans. If this option is enabled, here you can set how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira Premium Security Suite detects fewer viruses, worms or Trojans, 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 application of this heuristic.

High detection level

If this option is enabled, Avira Premium Security Suite detects a large number of unknown viruses, worms or Trojans, but you must also expect false positives.

12.1.2 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.



So that you can establish what actions the Scanner has carried out 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.

Extended

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.



If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

12.2 Guard

The Guard section of the Avira Premium Security Suite Configuration is responsible for the configuration of the on-access scan.

12.2.1 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.



To obtain maximum security, you should have enabled this option. However, please note that this may reduce the computer performance, as files may be scanned more than once.

Files

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

All files

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



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 Avira Premium Security Suite. This means that Avira Premium Security Suite 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.



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 pre-defined extension are scanned. All file types that may contain viruses and unwanted programs are pre-defined. The list can be edited manually via the button **File extension**. This option is enabled as the default setting and is recommended.



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 window is opened in which all file extensions are displayed that are scanned in the **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.



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

Archives

The Guard can monitor files that have been compressed with run-time packers.

Unpacking run-time compressed files

If this option is enabled, the files are scanned, decompressed and scanned again. Viruses and unwanted programs hidden in these files can also be found in this way. This option is enabled as the default setting and is recommended.

Scan archive

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. Additional settings are available for restricting the scanning of archives and for setting the recursion depth of the scanning. This is recommended if you activate the archive scan.



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 depth of recursion

When scanning the archives, Guard can use a recursive scan. This unpacks archives that packed inside other archives and checks them for viruses and unwanted programs. You can define the recursion depth. Active this option to do so. Permitted values are 1 to 20. The default value for the recursion depth is 1 and is recommended: all archives that are directly located in the main archive are unpacked and scanned.

Maximum number of files

If this option is enabled, you can restrict the scan to a maximum number of files in the archive. Permissible values are between 1 and 99. The default value of 10 files to be scanned is recommended.

Maximum size (KB)

If this option is enabled you can restrict the scanner to unpacking only archives below a defined maximum size. Permissible values are between 1 and 9999 KB. The standard value of 1000 KB is recommended.

12.2.1.1. Action for concerning files

Action for concerning files

You can define actions that the Guard is to carry out when a virus or unwanted program is detected.

Interactive

If this option is enabled, a dialog window appears during the on-access scan when a virus or unwanted program is detected in which you can choose what is to be done with the file concerned. This option is enabled as the default setting.

Further information is given here.

Automatic

If this option is enabled, then no dialog box for selecting an action appears following the detection of a virus or unwanted program. The Guard reacts according to the settings made by you in this section.

Copy file to quarantine before action

If this option is enabled, the Guard creates a backup copy before carrying out the requested primary or secondary action. The backup copy is saved in quarantine. It can be restored via the Quarantine manager if it is of informative value. You can also send the back-up copy to the Avira Malware Research Center. Depending on the object, there are more selection possibilities in the quarantine manager.

Primary action

Primary action is the action carried out when the Guard finds a virus or an unwanted program. If the option **Repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.



The option Secondary action can only be selected if the option Repair was selected under Primary action.

repair

If this option is enabled, the Guard repairs affected files automatically. If the Guard cannot repair an affected file, it carries out the action selected under Secondary action.



An automatic repair is recommended, but means that the Guard modifies files on the workstation.

delete

If this option is enabled, the file is deleted, but can be restored if necessary with relevant tools (e.g. Avira UnErase). This means that the virus patterns could be detected again. This process is much faster than "overwrite and delete".

overwrite and delete

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

rename

If this option is enabled, the Guard 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.



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

deny access

If this option is enabled, the Guard only enters the detection in the report file if the report function is enabled. In addition, the Guard writes an entry in the event log, if this option is enabled.

quarantine

If this option is enabled, the Guard moves the file to the quarantine. The files in this directory 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 option **Repair** was selected under **Primary action**. With this option it is possible to decide what should be done with the affected file if it cannot be repaired.

delete

If this option is enabled, the file is deleted, but can be restored if necessary with relevant tools (e.g. Avira UnErase). This means that the virus patterns could be detected again. This process is much faster than "overwrite and delete".

overwrite and delete

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

rename

If this option is enabled, the Guard 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.



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

deny access

If this option is enabled, the Guard only enters the detection in the report file if the report function is enabled. In addition, the Guard writes an entry in the event log, if this option is enabled.

quarantine

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

12.2.1.2. Other actions

Notifications**Use event log**

When this option is enabled, an entry is added to the event log for every detection. The administrator can identify detections and react accordingly. This option is enabled by default.

Acoustic alert

When this option is enabled, Guard plays a sequence of notes when a detection is made. This setting is enabled by default.

12.2.1.3. 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 back-up solutions.

Processes to be omitted for the Guard

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

Input box

In this box you can enter the name of the process that is not included in the on-access scan. No process is entered as the default setting. The names of the individual process can most easily be obtained via the task manager. You can find the names of all currently active processes under the index card "Processes" of the task manager. Select "your" process and enter its name (found under "Image Name").



You can enter up to 20 processes.



Only the first 15 characters of the process name (including the file extension) are considered. If there are 2 processes with the same name, Guard excludes both processes from the monitoring.



Please note that all file accesses by processes recorded in the list are excluded from the scan for viruses and unwanted programs! The Windows Explorer and the operating system itself cannot be excluded. A corresponding entry in the list is ignored.

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 for the Guard

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



The entries on the list must not contain more than 6000 characters in total.

Input box

In this box you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.



The 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 observe the following points:

- The file name can only contain the wildcards * (any number of characters) and ? (a single character).
- Directory names must end with a backslash \, otherwise a file name is assumed.
- The list is processed from top to bottom.
- Individual file extensions can also be excluded (inclusive wildcards).
- If a directory is excluded, all its sub-directories are automatically also excluded.
- 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.
- In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.



A file name that contains wildcards may not be terminated with a backslash.

For example:

```
C:\Program Files\Application\applic*.exe\
```

This entry is not valid and not treated as an exception!

Examples:

C:

C:\

C:*.*

C:*

*.exe

*.xl?

.

C:\Program Files\Application\application.exe

C:\Program Files\Application\applic*.exe

C:\Program Files\Application\applic*

C:\Program Files\Application\applic?????.e*

C:\Program Files\

C:\Program Files

C:\Program Files\Application*.mdb

12.2.1.4. Heuristic

This configuration section contains the settings for the heuristic of the Avira Premium Security Suite search engine.

Avira Premium Security Suite contains very powerful heuristic, which can also detect unknown (new) viruses, worms or Trojans. This is done with a comprehensive analysis and examination of the relevant codes for functions that are typical of viruses, worms or Trojans. If the code examined fulfils these characteristic criteria, it is reported as being suspect. However, this does not necessarily mean that the code is in actual fact a virus, a worm or a Trojan; it may also be a false positive. The user has to decide what to do with the relevant code, for example based on his/her knowledge of whether the source containing the suspect code is reliable.

Macrovirus heuristic

Macrovirus heuristic

Avira Premium Security Suite contains a very powerful macrovirus heuristic. If this option is enabled, all macros 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.

Win32 file heuristic

Avira Premium Security Suite contains a very powerful heuristic for Windows file viruses, worms and Trojans, which can also detect unknown viruses, worms and Trojans. If this option is enabled, here you can set how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira Premium Security Suite detects fewer viruses, worms or Trojans, 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 application of this heuristic.

High detection level

If this option is enabled, Avira Premium Security Suite detects a large number of unknown viruses, worms or Trojans, but you must also expect false positives.

12.2.2 Report

The Guard has a comprehensive reporting function that can provide the user or the administrator with precise information on the type of malware detected.

Reporting

The scope of content of the report file is defined in this group.

Off

If this option is enabled, the Guard does not create a report. Only refrain from enabling reporting in exceptional cases, for example if you carry out test runs with many viruses or unwanted programs.

Default

If this option is enabled, the Guard adds important information (on the found, alerts and errors) to the report file, less important information is ignored in order to provide a clear overview. This option is enabled as the default setting.

Extended

If this option is enabled, the Guard also includes less important information in the report file.

Complete

If this option is enabled, the Guard includes all information - also that on file size, file type, date etc. - in the report file.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: 1 to 100 MB. This option is enabled as the default setting, with a value of 1 MB. A tolerance of approximately 50 kilobytes is included in order to minimize load of the computer. If the size of the report file exceeds the pre-defined size by 50 kilobytes, old entries are automatically deleted until the pre-defined size -50 kilobytes has been reached.

Backup report file before shortening

If this option is enabled, the report file is backed up before being shortened in the report directory.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan used is written in the report file.

Display user who accesses the file

You can select whether the name of the user who accesses the infected file is to be written into the report file. This logging function can be disabled, enabled or used with restrictions with the option 'Only for altered files'.



This option is only available with minifilter. After reinstallation of Premium Security Suite, an IFS filter is installed by default. For further information, please contact technical support (see ch.: Technical Support).

12.3 MailGuard

The MailGuard section of the Avira Premium Security Suite Configuration is responsible for the configuration of the MailGuard.

12.3.1 Scan

Use MailGuard to scan incoming emails for viruses and malware and for spam. Outgoing emails can be scanned for viruses and malware by MailGuard. Outgoing emails which are spam sent from an unknown bot on your computer can be blocked by MailGuard.

Scan

Scan incoming emails (POP3)

If this option is enabled, incoming emails are scanned for viruses, malware and spam.

Scan outgoing emails (SMTP)

If this option is enabled, outgoing emails are scanned for viruses and malware. Emails which are spam sent by unknown bots are blocked.

12.3.1.1. Action for concerning files

This configuration section contains settings for actions performed when MailGuard finds a virus or unwanted program in an email or in an attachment.



These actions are performed both when a virus is detected in incoming emails and when a virus is detected in outgoing emails.

Action for concerning files

Interactive

If this option is enabled, a dialog window appears when a virus or unwanted program is detected in an email or attachment in which you can choose what is to be done with the email or attachment concerned. This option is enabled as the default setting.

Further information is given here.

Show progress bar

If this option is enabled, the MailGuard shows a progress bar during downloading of emails. This option can only be enabled if the option **Interactive** has been selected.

Automatic

If this option is enabled, you are no longer notified when a virus or unwanted program is found. The MailGuard reacts according to the settings made by you in this section.

Primary action

Primary action is the action carried out when the MailGuard finds a virus or an unwanted program in an email. If the option **Ignore email** is selected, it is also possible to select under **Affected attachments** what is to be done if a virus or unwanted program is detected in an attachment.

Delete email

If this option is enabled, the email concerned is automatically deleted if a virus or unwanted program is found. The body of the email is replaced by the default text given below. The same applies to all attachments included; these are also replaced by a default text.

Isolate email

If this option is enabled, the complete email including all attachments is placed in Quarantine if a virus or unwanted program is found. If required, it can later be restored. The affected email itself is deleted. The body of the email is replaced by the default text given below. The same applies to all attachments included; these are also replaced by a default text.

Ignore email

If this option is enabled, the email concerned is ignored despite detection of a virus or unwanted program. However, you can decide what is to be done with the affected attachment:

Affected attachments

The option **Affected attachments** can only be selected if the setting **Ignore email** has been selected under **Primary action**. With this option it is now possible to decide what is to be done if a virus or unwanted program is found in an attachment.

delete

If this option is enabled, the affected attachment is deleted if a virus or unwanted program is found and replaced by a default text.

isolate

If this option is enabled, the affected attachment is placed in quarantine and then deleted (replaced by a default text). If required, it can later be restored.

ignore

If this option is enabled, the attachment is ignored despite detection of a virus or unwanted program and delivered.



If you select this option, you have no protection against viruses and unwanted programs by the MailGuard. Only select this point if you know exactly what you are doing. Disable the preview in your email program, never open attachments by double-clicking!

12.3.1.2. Other actions

This configuration section contains other settings for actions performed when MailGuard finds a virus or unwanted program in an email or in an attachment.



These actions are performed exclusively when a virus is detected in incoming emails.

Default text for deleted and moved emails

The text in this box is inserted in the email as a message instead of the affected email. Please note that you can also format the text in this edit box. You can enter a maximum of 500 characters.

You can use the following key combination for formatting:

Ctrl + **Enter** inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

Default text for deleted and moved attachments

The text in this box is inserted in the email as a message instead of the affected attachment. Please note that you can also format the text in this edit box. You can enter a maximum of 500 characters.

You can use the following key combination for formatting:

Ctrl + **Enter** inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

12.3.1.3. Heuristic

This configuration section contains the settings for the heuristic of the Avira Premium Security Suite search engine.

Avira Premium Security Suite contains very powerful heuristic, which can also detect unknown (new) viruses, worms or Trojans. This is done with a comprehensive analysis and examination of the relevant codes for functions that are typical of viruses, worms or Trojans. If the code examined fulfils these characteristic criteria, it is reported as being suspect. However, this does not necessarily mean that the code is in actual fact a virus, a worm or a Trojan; it may also be a false alert. The user has to decide what to do with the relevant code, for example based on his/her knowledge of whether the source containing the suspect code is reliable.

Macrovirus heuristic

Macrovirus heuristic

Avira Premium Security Suite contains a very powerful macrovirus heuristic. If this option is enabled, all macros 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.

Win32 file heuristic

Avira Premium Security Suite contains a very powerful heuristic for Windows file viruses, worms and Trojans, which can also detect unknown viruses, worms and Trojans. If this option is enabled, here you can set how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, Avira Premium Security Suite detects fewer viruses, worms or Trojans, 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 application of this heuristic. This option is enabled as the default setting and is recommended.

High detection level

If this option is enabled, Avira Premium Security Suite detects a large number of unknown viruses, worms or Trojans, but you must also expect false positives.

12.3.1.4. AntiBot

The AntiBot function of MailGuard prevents your computer from becoming part of a so-called bot-net and being used to send out spam emails: to send spam via a bot-net an attacker usually infects a number of computers with a bot, which then connects to an IRC server, opens a particular channel and waits for the command to send the spam emails. To distinguish spam emails from an unknown bot from genuine emails, MailGuard checks if the SMTP server and email sender for an outgoing email are included in the lists of permitted servers and senders. If this is not the case, the outgoing emails are blocked, i.e. the email is not sent. A dialog box appears in which you can choose what to do with the email.



The AntiBot function can only be used, if the MailGuard scan of outgoing emails is enabled (see the option **Scan outgoing emails** under MailGuard :: Scan).

Permitted servers

All servers in this list are authorized to send emails: emails sent to these servers are **not** blocked by MailGuard. If no servers are included in the list, the SMTP server used to send outgoing emails is not scanned. If the list is populated, MailGuard blocks emails sent to any SMTP server not included in the list.

Input box

Enter the host name or IP address of the SMTP server you use to send your emails in this box.



Note

You can find details of the SMTP server used by your email program to send emails in your email program under the date the user account was created.

Add

You can use this button to include servers specified in the input box in the list of permitted servers.

Delete

This button deletes a highlighted entry from the list of permitted servers. This button is inactive if no entry is selected.

Delete all

This button deletes all entries from the list of permitted servers.

Permitted senders

All senders in this list are authorized by MailGuard to send emails: emails sent from this email address are **not** blocked by MailGuard. If no senders are included in the list, the email address used to send outgoing emails is not scanned. If the list is populated, MailGuard blocks emails from senders not included in the list.

Input box

Enter your email sender address(es) in this box.

Add

You can use this button to include senders specified in the input box in the list of permitted senders.

Delete

This button deletes a highlighted entry from the list of permitted senders. This button is inactive if no entry is selected.

Delete all

This button deletes all entries from the list of permitted senders.

12.3.2 General

12.3.2.1. Exceptions

Email addresses not scanned

This table shows you the list of email addresses excluded from scanning by AntiVir MailGuard (white list).



The list of exceptions is used exclusively by MailGuard with regard to incoming emails.

Status

Icon	Description
	This email address will no longer be scanned for spam.
	This email address will no longer be scanned for malware.
	This email address will not be scanned for malware or spam.

Email address

Email that is no longer to be scanned.

Malware

When this option is enabled, the email address is no longer scanned for malware.

Spam

When this option is enabled, the email address is no longer scanned for spam.

Up

You can use this button to move a highlighted email address to a higher position. If no entry is highlighted or the highlighted address is at the first position in the list, this button is not enabled.

Down

You can use this button to move a highlighted email address to a lower position. If no entry is highlighted or the highlighted address is at the last position in the list, this button is not enabled.

Input box

In this box you enter the email address that you want to add to the list of email addresses not to be scanned. Depending on your settings, the email address will no longer be scanned in future by the MailGuard.



You can use wildcards when entering email addresses: ***** for any number of characters and **?** for a single character. Wildcards can however be used exclusively for email addresses that are not scanned for spam. You will receive an error message if you attempt to exclude an address containing wildcards from the malware scan by checking the **Malware** exclusion list box. Please note that when entering addresses with wildcards, the specified character sequence must be consistent with the structure of an email address (***@*.***).



Please note the examples given for the use of wildcards. Only use wildcards selectively and be careful which email addresses containing wildcards you include in the spam whitelist.

Examples: Use of wildcards in email addresses (spam whitelist)

- `virus@avira.*` / = all emails with this address and any top level domain: `virus@avira.de`, `virus@avira.com`, `virus@avira.net`,...
- `*@avira.com` = all emails sent from the domain **avira.com**: `info@avira.com`, `virus@avira.com`, `kontakt@avira.com`, `employee@avira.com`
- `info@*.com` = all email addresses with the top level domain **com** and the address **info**: the second level domain can be anything: `info@name1.com`, `info@name2.com`,...

Add

With this button you can add the email address entered in the input box to the list of email addresses not to be scanned.

Delete

This button deletes a highlighted email address from the list.

Import Outlook address book

You can use this button to import email addresses from the address book of the MS Outlook email program into the list of exceptions. Imported email addresses are not scanned for spam.

Import Outlook Express address book

You can use this button to import email addresses from the address book of the MS Outlook Express email program into the list of exceptions. Imported email addresses are not scanned for spam.

12.3.2.2. Cache

Cache

The MailGuard cache contains data regarding the scanned emails that is displayed as statistical data in Control Center under MailGuard. Copies of incoming emails are also deposited in the cache. The emails can also be used for the anti-spam module's training functions (Good email - use for training, Spam - use for training).



The anti-spam module must be activated for incoming emails to be backed up in the cache.

Maximum number of emails to be stored in the cache

This field is used to set the maximum number of emails that are stored by MailGuard in the cache. Emails are deleted oldest first.

Maximum storage period of an email in days

The maximum storage period of an email in days is entered in this box. After this time, the email is removed from the cache.

Empty cache

Click on this button to delete the emails stored in the cache.

12.3.2.3. AntiSpam

AntiSpam

The AntiVir MailGuard scans emails for viruses and unwanted programs. It can also reliably protect you against spam emails.

AntiSpam

Activate AntiSpam module

Enabling this option activates the anti-spam function of MailGuard.

Mark email subject

When this option is enabled, a note is added to the original subject line when a spam email is detected.

Simple

If a spam or phishing email is received, an addendum [SPAM] or [Phishing] is added. This option is enabled as the default setting.

Detailed

The subject line of a spam or phishing email is prefixed by an addendum drawing attention to the likelihood that the respective message is spam.

Report

If this option is enabled, MailGuard creates a special anti-spam report file.

Use real-time black lists

When this option is enabled, a so-called "black list" is queried in real time, which provides additional information to classify emails of dubious origin as spam.

Timeout: n second(s)

If the information of a black list is not available after n seconds, the attempt to query the black list is aborted.

Delete training database

Click on the button to delete the training database.

Recipients of outgoing emails are automatically added to the whitelist

If this option is enabled, the receiver addresses of outgoing emails are automatically added to the spam whitelist (list of emails not scanned for spam, defined in **MailGuard :: General :: Exceptions**). Incoming emails sent from addresses on the spam whitelist are not scanned for spam. They are however scanned for viruses and malware. This option is disabled as the default setting.



This option can only be enabled if the MailGuard scan of outgoing emails is enabled (see the option **Scan outgoing emails** under MailGuard :: Scan).

12.3.3 Report

MailGuard includes an extensive logging function to provide the user or administrator with exact information on the type of detection.

Logging

This group allows for the content of the report file to be determined.

Off

If this option is enabled, MailGuard does not create a log.

Only turn off the logging function in exceptional cases, such as if you are executing test runs with multiple viruses or unwanted programs.

Default

If this option is enabled, MailGuard records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, MailGuard also logs less important information in the report file.

Complete

If this option is enabled, MailGuard 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 is restricted to a specific size. Permitted values are between 1 and 100 MB. This option is activated by default with a value of 1 MB. Up to 50 kilobytes of extra space are allowed 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 then deleted until the indicated size minus 50 kilobytes is attained.

Backup report file before shortening

If this option is enabled, the abbreviated report file is saved.

Write configuration in report file

If this option is enabled, the MailGuard configuration is recorded in the report file.

12.4 Firewall

The Firewall section of the Avira Premium Security Suite Configuration is responsible for the configuration of the Avira Firewall.

12.4.1 Adapter rules

An adapter represents for the Avira Firewall a software simulated hardware device (e.g. miniport, bridge connection, etc.) or a real hardware device (e.g. network card).

Avira Firewall displays the adapter rules of all existing adapters on your computer for which a driver was installed.

A predefined adapter rule depends on the security level. You can change the security level in the Online protection :: Firewall section of Avira Premium Security Suite Control Center or you can define your own adapter rules. If you have defined your own adapter rules, in the Firewall section of the Avira Premium Security Suite Control Center, the security level is set to custom.



The default setting of the Security Level for all predefined adapter rules of the Avira Firewall is **Medium**.

ICMP protocol

The Internet Control Message Protocol (ICMP) is used to exchange error and information messages on networks. The protocol is also used for status messages with ping or tracert.

With this rule you can define the incoming and outgoing blocked message types, the behavior in case of flooding and the reaction of fragmented ICMP packets. This rule serves for preventing so called ICMP flood attacks, which results in increase of the CPU load of the attacked machine as it responds to every packet.

Predefined rules for the ICMP protocol

Low level	Medium level	High level
Incoming blocked typed: no type . Outgoing blocked types: no type . Assume flooding if delay between packets is less than 50 ms. Reject fragmented ICMP packets.	Same rule as for the low level.	Incoming blocked typed: several types Outgoing blocked types: several types Assume flooding if delay between packets is less than 50 ms. Reject fragmented ICMP packets.

Incoming blocked type: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can specify the desired incoming ICMP message types you want to block.

Outgoing blocked type: no types/several types

With a mouse click on the link a list of ICMP packet types is displayed. From this list you can select the desired outgoing ICMP message types you want to block.

Flooding

With a mouse click on the link a dialog box is displayed where you can enter the maximum allowed ICMPPA delay.

Fragmented ICMP packets

With a mouse click on the link you have the choice to reject or don't reject fragmented ICMP packets.

TCP port scan

With this rule you can define in what case a TCP port scan is assumed by the Firewall and what should be done furthermore. This rule serves for preventing so called TCP port scan attack, which results in a detection of open TCP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the TCP port scan

Low level	Medium level	High level
Assume a port scan if 20 or more ports were scanned in 5000 milliseconds. When detected, log attacker's IP and don't add rule to block the attack.	Assume a port scan if 7 or more ports were scanned in 5000 milliseconds. When detected, log attacker's IP and add rule to block the attack.	Same rule as for the medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a TCP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of TCP port scans.

Report file

With a mouse click on the link you have the choice to log or don't log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or don't add the rule to block the TCP port scan attack.

UDP port scan

With this rule you can define in what case a UDP port scan is assumed and what should be done furthermore. This rule serves for preventing so called UDP port scan attack, which results in a detection of open UDP ports on your computer. This kind of attack is used to search a computer for weak spots and is often followed by more dangerous attack types.

Predefined rules for the UDP port scan

Low level	Medium level	High level
Assume a port scan if 20 or more ports were scanned in 5000 milliseconds. When detected, log attacker's IP and don't add rule to block the attack.	Assume a port scan if 7 or more ports were scanned in 5000 milliseconds. When detected, log attacker's IP and add rule to block the attack.	Same rule as for the medium level.

Ports

With a mouse click on the link a dialog box appears in which you can enter the number of ports that must have been scanned so that a UDP port scan is assumed.

Port scan time window

With a mouse click on this link a dialog box appears in which you can enter the time span for a certain number of UDP port scans.

Report file

With a mouse click on the link you have the choice to log or don't log the attacker's IP address.

Rule

With a mouse click on the link you have the choice to add or don't add the rule to block the UDP port scan attack.

12.4.1.1. Incoming Rules

Incoming rules are defined to control incoming traffic by Avira Firewall.



When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only, if you are completely aware of what you are doing.

Predefined rules for the TCP traffic monitor

Low level	Medium level	High level
No incoming traffic is blocked by Avira Firewall.	<ul style="list-style-type: none"> – Allow established TCP connections on 135 <p>Allow TCP packets from address 0.0.0.0 with mask 0.0.0.0 if local ports in {135} and remote ports in {0-65535}. Apply for packets of existing connections. Don't log when packet matches rule. Advanced: Discard packets that have following bytes <empty> with mask <empty> at offset 0.</p>	<ul style="list-style-type: none"> – Monitor established TCP traffic <p>Allow TCP packets from address 0.0.0.0 with mask 0.0.0.0 if local ports in {0-65535} and remote ports in {0-65535}. Apply for packets of existing connections. Don't log when packet matches rule. Advanced: Discard packets that have following bytes <empty> with mask <empty> at offset 0.</p>

Low level	Medium level	High level
	<ul style="list-style-type: none"> <li data-bbox="756 389 1021 1097"> – Deny TCP packets on 135 Deny TCP packets from address 0.0.0.0 with mask 0.0.0.0 if local ports in {135} and remote ports in {0-65535}. Apply for all packets. Don't log when packet matches rule. Advanced: Discard packets that have following bytes <empty> with mask <empty> at offset 0. <li data-bbox="756 1151 1021 2072"> – Monitor TCP healthy traffic Allow TCP packets from address 0.0.0.0 with mask 0.0.0.0 if local ports in {0-65535} and remote ports in {0-65535}. Apply for connection initiation and existing connection packets. Don't log when packet matches rule. Advanced: Discard packets that have following bytes <empty> with mask <empty> at offset 0. 	

Accept / deny TCP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming TCP packets.

IP address

With a mouse click on the link a dialog box appears in which you can define the desired IP address.

IP mask

With a mouse click on the link a dialog box appears in which you can define the desired IP mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply the rule for connection initiation and existing connection packets or only for packets of existing connections or for all packets.

Report file

With a mouse click on the link you have the choice to log or don't log when packet rule matches.

The **advanced feature** enables content filtering. For example packets can be rejected if they contains some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where TCP header ends.

Predefined rules for the UDP traffic monitor

Low level	Medium level	High level
-	<ul style="list-style-type: none"> – Monitor UDP accepted traffic <p>Allow UDP packets from address 0.0.0.0 with mask 0.0.0.0 if local port is in {0- 66535} and remote port is in {0-66535}. Apply rule to open ports. Don't log when packet matches rule. Advanced: Discard packets that have following bytes <empty> with mask <empty> at offset 0.</p>	Same rule as for the medium level.

Accepting of UDP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming UDP packets.

IP address

With a mouse click on the link a dialog box appears in which you can define the desired IP address.

IP mask

With a mouse click on the link a dialog box appears in which you can define the desired IP mask.

Local ports

With a mouse click on this link a dialog box appears in which you can define the local port number(s) or complete port ranges.

Remote ports

With a mouse click on this link a dialog box appears in which you can define the remote port number(s) or complete port ranges.

Application method

With a mouse click on this link you have the choice to apply this rule to all ports or only to all opened ports.

Report file

With a mouse click on the link you have the choice to log or don't log when packet rule matches.

The **advanced feature** enables content filtering. For example packets can be rejected if they contains some specific data at a certain offset. If you do not want to use this option do not select a file or choose an empty file.

Filtered content data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where UDP header ends.

Predefined rules for the ICMP traffic monitor

Low level	Medium level	High level
-	<ul style="list-style-type: none"> – Do not discard ICMP based on IP address. <p>Allow ICMP packets from address 0.0.0.0 with mask 0.0.0.0.</p> <p>Don't log when packet matches rule.</p> <p>Advanced: Discard packets that have following bytes <empty> with mask <empty> at offset 0.</p>	Same rule as for the medium level.

Accepting of ICMP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming ICMP packets.

IP address

With a mouse click on the link a dialog box appears in which you can define the desired IP address.

IP mask

With a mouse click on the link a dialog box appears in which you can define the desired IP mask.

Report file

With a mouse click on the link you have the choice to log or don't log when packet rule matches.

The **advanced feature** enables content filtering. For example packets can be rejected if they contains some specific data at a certain offset. If you do not want to use this option do not select an file or choose an empty file.

Filtered content data

With a mouse click on the link a dialog box appears in which you can select a file that contains the specific buffer.

Filtered content mask

With a mouse click on the link a dialog box appears in which you can select the specific mask.

Filtered content offset

With a mouse click on the link a dialog box appears in which you can define the filtered content offset. The offset is computed from where ICMP header ends.

Predefined rules for IP packets

Low level	Medium level	High level
-	<ul style="list-style-type: none">Deny all IP packets <p>Deny IP packets from address 0.0.0.0 with mask 0.0.0.0. Don't log when packet matches rule.</p>	Same rule as for medium level.

Accepting of TCP packets

With a mouse click on the link you have the choice to allow or deny special defined incoming IP packets.

IP address

With a mouse click on the link a dialog box appears in which you can define the desired IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Report file

With a mouse click on the link you have the choice to log or don't log when packet rule matches.

Possible rules for monitoring IP packages based on IP protocols

IP packages

By clicking on the link with the mouse, you can decide whether you want to accept or reject specially defined IP packages.

IP address

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP address.

IP mask

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP mask.

Protocol

By clicking on this link with the mouse, a dialog window opens in which you can enter the required IP protocol.

Report file

By clicking on the link with the mouse you can decide whether to write to a report file or not if the package complies with the rule.

12.4.1.2. Outgoing Rules

Outgoing rules are defined to control outgoing traffic by Avira Firewall. You can define a outgoing rule for one of the following protocols: IP, ICMP, UDP and TCP. You can define a outgoing rule for one of the following protocols: IP, ICMP, UDP and TCP.



When a packet is filtered the corresponding rules are applied successively, therefore the rule order is very important. Change the rule order only, if you are completely aware of what you are doing.

Buttons

Button	Description
Add rule	Allows you to create a new rule. If you press this button, the "Add new rule" dialog box is opened. In this dialog box, you can create new incoming or outgoing rules or select a predefined rule.
Remove rule	Removes the selected rule.
Rule down	Moves the selected rule down one line, i.e. reduces the rule priority.
Rule up	Moves the selected rule up one line, i.e. increases the rule priority.
Rename rule	Allows you to give the selected rule another name.



You can add new rules for individual adapters or for all adapters present on the computer. To add an adapter rule for all adapters, select **Computer** from the adapter hierarchy that is displayed and click on the **Add** button.

12.4.2 Application rules

Application rules for user

This list contains all users in the system. If you are logged in as an administrator, you can select the user you want to apply the rules for. If you are not a privileged user, you can see only the current user logged on.

Application list

This table shows the list of applications for which rules are defined. The application list contains the settings of each application that was executed and had a rule saved since the Avira Firewall was installed.

Normal view

	Description
Application	Name of the application.
Action	Shows the action that the Avira Firewall will automatically take when the application is using the network, whatever the network usage type is. With a mouse click on the link you can switch to another action type. The values are Ask , Allow or Deny . Ask is the default action.

Expert view

If you want to choose the action for every type of network access individually, you have to select the **Expert Mode** in the configuration. Please set the option in the **Advanced options** area of the Firewall :: Settings section to Network events: define one action for each. Directly after changing the option, the table with the list of applications is displayed as follows.

	Description
Application	Name of the application.
Connect	With a mouse click on the link you can allow or deny access or have the Avira Firewall ask you when the application can connect to the Internet or network.
Listen	With a mouse click on the link you can allow or deny or have the Avira Firewall ask you when the application passively listens for contact from the Internet or network.
UDP Send	With a mouse click on the link you can allow, deny or have the Avira Firewall ask you when the application sends data to the Internet or network via UDP protocol.
UDP Receive	With a mouse click on the link you can allow, deny or have the Avira Firewall ask you when the application receives data from the Internet or network via UDP protocol.
Code injection	A mouse click on the link lets you to accept or refuse a code injection by the application, or enable the Firewall to monitor each execution attempt. Code injection is a technique for introducing code into the address space of another process to execute actions, forcing this process to load a dynamic link library (DLL). Code injection is used by malware, amongst other things, to execute code under cover of another program. In this way, access to the internet in front of the Firewall can be hidden. In default mode, code injection is enabled for all signed applications.

Application details

In this box you can see details of the application selected in the application list box.

	Description
Name	Name of the application.
Path	Full path to the executable file.

Buttons	
Button	Description
Add rule	Allows you to create a new application rule. If you press this button, a dialog window is opened. Here you can select the required application for creating a new rule.
Remove rule	Removes the selected application rule.
Reload	Reloads the list of applications and simultaneously discards the changes just made to the application rules just made.
Apply	Changed settings are accepted and immediately applied by the Avira Firewall.

12.4.3 Settings

Timeout of the rule

Always block

If this option is enabled, a rule that was automatically created, for example, during a port scan is retained.

Remove rule after n seconds

If this option is enabled, a rule that was automatically created for example during a port scan, is removed again after the time you have defined. This option is enabled as the default setting.

Advanced options

Windows Host file is not locked/locked.

If this option is set to LOCKED, the windows host file is write protected. Manipulation is no longer possible. For example, malware is not able to redirect you to undesired websites. The state of this option is NOT LOCKED as the default setting.

Deactivate Windows Firewall on reboot

If this option is enabled, the Windows Firewall is deactivated when the computer is rebooted. This option is enabled as the default setting.

12.4.4 Popup settings

Popup settings

Inspect process launch stack

If this option is enabled, the process stack inspection allows a more accurate control. The Firewall will assume that any of the untrustworthy processes in the stack may actually be the one accessing the network through its child process. Therefore a different popup window will be opened for each untrustworthy process in the process stack. This option is disabled as the default setting.

Allow multiple popups per process

If this option is enabled, every time an application is making a network connection, a popup is triggered. Alternatively you will be informed only on the first connection attempt. This option is disabled as the default setting.

Network events: define one action for all/one action for each

If this option is set to ONE ACTION FOR EACH, the application list of the section **Online protection :: Firewall :: Application rules** allows individual definition of actions for the different types of network access. Alternatively, only one action is possible for all types of network access. The state of this option is ONE ACTION FOR ALL as the default setting.

Remember action for this application

Always enabled

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is activated as the default setting. This option is enabled as the default setting.

Always disabled

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is disabled as the default setting.

Allow signed application

When this option is enabled, the option "Save action for this application" of the dialog box "Network event" is automatically enabled during network access by signed applications. The manufacturers are: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlett Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Remember last used state

When this option is enabled, the option "Save action for this application" in the dialog box "Network event" is enabled in the same way as for the last network event. If the option "Save action for this application" of the dialog box "Network event" was enabled, this option is enabled for the following network event. If the option "Save action for this application" was disabled for the last network event, this option is also disabled for the following network event.

Show details

In this group of configuration options, you can setup the display of detailed information in the **Network event** window.

Show details on demand

If this option is enabled, the detailed information is only displayed in the *Network event* window on request, i.e. the detailed information is displayed by clicking on the **Show details** button in the *Network event* window.

Always show details

If this option is enabled, detailed information is always displayed in the *Network event* window.

Remember last used state

If this option is enabled, the display of detailed information is administered in the same way as for the previous network event. If detailed information was displayed or accessed during the last network event, detailed information is displayed for the following network event. If detailed information was hidden and not displayed during the last network event, detailed information is not displayed for the following network event.

12.5 WebGuard

The WebGuard section of Avira Premium Security Suite Configuration is used to configure WebGuard.

12.5.1 Scan

12.5.1.1. Action for concerning files

Action for concerning files

You can define the actions to be carried out by WebGuard when a virus or unwanted program is detected.

Interactive

If this option is enabled, a dialog window 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.](#)

Display 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, then no dialog box for selecting an action appears following the detection of a virus or unwanted program. WebGuard reacts according to the settings you define in this section.

Primary action

The primary action is the action carried out when WebGuard finds a virus or an unwanted program.

Deny access

The website requested by the web server and/or the transferred data and files are not sent to your web browser. An error message about the denial of access is displayed in the web browser. WebGuard logs the detection to the report file if the report function is activated. WebGuard also appends an entry to the event log if this option is enabled.

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 infected file can be restored via the Quarantine Manager if it is of informative value or - if necessary - sent to the Avira Malware Research Center.

ignore

The website requested by the web server and/or the transferred data and files are forwarded on by WebGuard to your web browser. Access to the file is permitted and the file is ignored.



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

12.5.1.2. Locked requests

In **Locked requests** you can specify the file types and MIME types (content types for the transferred data) to be blocked by WebGuard. The Web filter lets you block known phishing and malware-URLs. WebGuard prevents the transfer of data from the internet to your computer system.

File types / MIME types to be blocked by WebGuard (user-defined)

All file types and MIME types (content types for the transferred data) in the list are blocked by WebGuard.

Input box

In this box, enter the names of the MIME types and file types you want WebGuard to block. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, sub-type. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.



Files which are already stored on your computer system as temporary internet files and blocked by WebGuard can however be downloaded locally from the internet by your computer's internet browser. Temporary internet files are files saved on your computer by the internet browser so that websites can be accessed more quickly



The list of blocked file and MIME types is ignored if they are entered in the list of excluded file and MIME types under WebGuard::Scan::Exceptions.



No wildcards (* for any number of characters or ? nbsp for a single character) can be used when entering file types and MIME types.

MIME types: Examples for media types:

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

Examples: Excluded file and MIME types

- `application/octet-stream` = `application/octet-stream` MIME type files (executable files `*.bin`, `*.exe`, `*.com`, `*.dll`, `*.class`) are blocked by WebGuard.
- `application/olescript` = `application/olescript` MIME type files (ActiveX script-files `*.axs`) are blocked by WebGuard.
- `.exe` = All files with the extension `.exe` (executable files) are blocked by WebGuard.
- `.msi` = All files with the extension `.msi` (Windows Installer files) are blocked by WebGuard.

Add

With this button, you can add the MIME OR file type entered in the input box to the display window.

Delete

This button deletes an entry highlighted in the list. This button is inactive if no entry is selected.

Web filter

The Web filter is based on an internal database, updated daily, that classifies URLs according to content.

Block phishing and malware URLs

If this option is enabled, known phishing and malware URLs are blocked by WebGuard.



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

12.5.1.3. 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.

Input box

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. z.B. **.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, z.B. **video/mpeg** or **audio/x-wav**.



No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.



All file types and content types on the exclusion list are downloaded into the internet browser without further scanning of the blocked access (List of file and MIME types to be blocked in WebGuard::Scan::Blocked access) or by WebGuard: For all entries on the exclusion list, the entries on the list of file and MIME types to be blocked are ignored. No scan for viruses and malware is carried out.

MIME types: Examples for media types:

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

Examples: Excluded file and MIME types

- 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 rule

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/**. Indicate websites with any top-level domain (.com or .net) with a concluding 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).



No wildcards (* for any number of characters or ? for a single character) can be used when entering URLs.



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 carried out. Only trusted URLs should therefore be excluded from WebGuard scans. Make sure not strings are entered with a concluding dot, as all URLs with a corresponding top-level domain are excluded from WebGuard scans.

Add rule

The button allows you to copy URLs (internet addresses) 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.

Examples: Excluded URLs

- `www.domainname.com` = All pages from the URL, such as `www.domain.com/page/` are excluded from WebGuard scans.
- `domainname.com` = All pages of the URL and all subdomains of the URL are excluded from WebGuard scans; `www.domain.com/page/`, `www.subdomain.domain.com/`
- `avira.` = All websites with the second-level domain `avira` are excluded from WebGuard scans: `www.avira.de`, `www.avira.com`
- `net` = All websites with the `.net` top-level domain are excluded from WebGuard scans: `www.name1.net`, `www.name2.net`

12.5.1.4. Heuristic

This configuration section contains the settings for the heuristic of the Avira Premium Security Suite search engine.

Avira Premium Security Suite contains very powerful heuristics that can uncover even unknown (new) viruses, worms and Trojans. This occurs through an extensive analysis and investigation of the affected codes for functions typical of viruses, worms or Trojan horses. 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 a virus, worm or Trojan horse. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristic

Macrovirus heuristic

Avira Premium Security Suite contains a highly powerful macro virus heuristic. If this option is enabled, all macros are deleted if repair is possible. Alternatively, suspect documents may simply be reported, i.e. you will receive an alert. This option is enabled as the default setting and is recommended.

Win32 file heuristic

Avira Premium Security Suite contains a very powerful heuristic for detecting viruses, worms and Trojan horses in Windows. It is also able to detect unknown viruses, worms and Trojans. If this option is activated, you can define how "aggressive" this heuristic should be. This option is activated by default.

Low detection level

If this option is enabled, Avira Premium Security Suite identifies fewer viruses, worms and Trojan horses, but there is less risk of potential false positives.

Medium detection level

This setting is activated by default if you have selected the use of this heuristic.

High detection level

If this option is enabled, Avira Premium Security Suite identifies a large number of unknown viruses, worms and Trojan horses, but you must also accept that there are likely to be false positives.

12.5.2 Report

WebGuard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Logging

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 activated by default.

Extended

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

Limit size to n MB

If this option is enabled, the report file is restricted to a specific size. Permitted values are between 1 and 100 MB. This option is activated by default with a value of 1 MB. Up to 50 kilobytes of extra space are allowed to minimise 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 then deleted until the indicated size minus 50 kilobytes is attained.

Write configuration in report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

12.6 Backup

The Backup section of Avira Premium Security Suite Configuration is responsible for configuration of the Avira Backup component.

12.6.1 Settings

In **Settings** you can configure the behavior of the Backup component.

Settings

Backup modified files only

If this option is enabled, an incremental backup is created: Only files which have been modified since the last backup are saved in the backup profile. If this option is disabled, a full backup is created for each saved backup profile: All files are saved in the backup profile. This option is enabled as the default setting and is recommended as incremental backups can be created more quickly and are less resource-heavy than full backup.

Scan for viruses and unwanted programs before backup

If this option is enabled, the files being saved are scanned for viruses and malware during the backup. Infected files are not saved. This option is enabled as the default setting and is recommended.

12.6.2 Exceptions

Under exceptions, you can specify which file objects and file types are saved, and which are not saved in the backup.

Skipped files from the backup

The list in this window contains the files and paths which are not saved in the backup.



The entries on the list must not contain more than 6000 characters in total.



The files included in this list are recorded in the Report file.

Input box

Enter the names of the file objects that are not to be saved in this box. The path for the temporary directory for the local settings of the logged-in user is entered as default.



The button opens a window in which you can select the file or path you want. You can isolate a particular file from the backup if you have the full name and path of the file. If you have entered a file name or path, every file with this name (irrespective of the path or drive) is not saved.

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.

Reset list

This button restores preset default values.

Please note the following points:

- The file name can only contain the wildcards * (any number of characters) and ? (a single character).
- The list is processed from top to bottom.
- If a directory is excluded, all its sub-directories are automatically also excluded.
- Individual file extensions can also be excluded (inclusive wildcards).
- In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.



A file name that contains wildcards may not be terminated with a backslash.

For example:

`C:\Program Files\Application\applic*.exe\`

This entry is not valid and not treated as an exception!

Examples:

`application.exe`

`\Program files\`

`C:*.*`

`C:*`

`*.exe`

`*.xl?`

`*.*`

`C:\Program Files\Application\application.exe`

`C:\Program Files\Application\applic*.exe`

`C:\Program Files\Application\applic*`

`C:\Program Files\Application\applic?????.e*`

`C:\Program Files\`

`C:\Program Files`

`C:\Program Files\Application*.mdb`

File extension lists

Allow all file extensions

If this option is enabled, all files in the backup profile are saved.

Enable file extensions excluded by the backup

If this option is enabled, all files in the backup profile are saved, except files whose extensions are entered in the list of excluded file extensions.

File extensions

This button opens a dialog box displaying all file extensions not saved during a backup when the option "Excluded file extensions" is enabled. Default entries are set for the extensions, but entries can be added or deleted.

Enable file extension lists consulted by the backup

If this option is enabled, only files whose file extensions have been entered in the list of file extensions to be consulted are saved.

File extensions

This button opens a dialog box displaying all file extensions saved during a backup when the option "File extensions included" is enabled. Default entries are set for the extensions, but entries can be added or deleted.

12.6.3 Report

The Backup component includes a comprehensive log function.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, Backup component does not create a log. Only turn off the logging function in exceptional cases.

Default

If this option is enabled, Backup component records important information (on saving, virus detections, alerts and errors) in the report file, and less important information is ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, Backup component includes less important information in the report file.

Full

If this option is enabled, Backup component includes all information on the backup process and virus scan in the report file.

12.7 General

12.7.1 Email

Avira Premium Security Suite can send messages via email. This is done with the Simple Message Transfer Protocol (SMTP).

The messages can be triggered by various events. Transmission of emails is supported by the following modules:

- Examination enquiries of suspicious files to the Avira Malware Research Center



Please note that ESMTP is not supported. In addition, an encrypted transfer via TLS (Transport Layer Security) or SSL (Secure Sockets Layer) is currently not possible.

Email messages

SMTP server

Enter the name of the host to be used here - either its IP address or the direct host name. The maximum possible length of the host name is 127 characters.

For example:

192.168.1.100 or mail.musterfirma.de.

Sender address

In this input box, enter the email address of the sender. The maximum length of the sender's address is 127 characters.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an email is sent. Avira Premium Security Suite can transmit alerts with authentication to the SMTP server via email.

Use authentication

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

- **User name:** Enter your user name here.
- **Password:** Enter the relevant password here. The password is saved in encrypted form. For security, the actual characters you type in this space are replaced by asterisks (*).

Send test email

When you click on the button, Avira Premium Security Suite attempts to send a test email to the sender address to check the data entered.

12.7.2 Extended threat categories

Selection of extended threat categories

Avira Premium Security Suite protects you against computer viruses.

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

- Backdoor control software (BDC)
- Dialer
- Games (GAMES)
- Joke programs (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Unusual runtime packers (PCK)
- Files with hidden file endings (HEUR-DBLEXT)
- Phishing
- Application (APPL)

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

Enable all

If this option is enabled, all types are enabled.

Default values

This button restores the predefined default values.



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.

12.7.3 Password

You can protect Avira Premium Security Suite in different areas with a password. If a password has been issued, you will be asked for this password every time you want to open the protected area.

Password

Enter password

Enter your required password here. For security, the actual characters you type in this space are replaced by asterisks (*). The password can only have a maximum of 19 chars. Once the password has been issued, the program refuses access if an incorrect password is entered. An empty box means "No password".

Confirm password

Confirm the password entered above by entering again here. For security, the actual characters you type in this space are replaced by asterisks (*).



The password is case-sensitive!

Areas protected by password

Avira Premium Security Suite can protect individual errors with a password. By clicking on the relevant box, the password request can be disabled or reactivated for individual areas as required.

Password-protected area	Function
Control Center	If this option is enabled, a password is required to start the Control Center.
Enable / disable Guard	If this option is enabled, the pre-defined password is required to enable or disable the AntiVir Guard.
Enable / disable MailGuard	If this option is enabled, the pre-defined password is required to enable/disable the MailGuard.
Firewall enable / disable	If this option is enabled, the pre-defined password is required to enable/disable the Firewall.
Enable/disable WebGuard	If this option is enabled, the pre-defined password is required to enable/disable the WebGuard.
Adding and changing jobs	If this option is enabled, a password is required when adding and changing jobs in Scheduler.
Start product updates	If this option is enabled, a password is required to start the product update in the update menu.
Quarantine	If this option is enabled, all possible areas of the quarantine manager protected by a password are enabled. By clicking on the relevant box, the password enquiry can be disabled or enabled again on request for individual areas.
Restore affected objects	If this option is enabled, a password is required to recover an object.
Repairing affected objects	If this option is enabled, a password is required to repair an object.
Properties of affected objects	If this option is enabled, a password is required to display the properties of an object.
Deleting affected objects	If this option is enabled, a password is required to delete an object.
Send email to AntiVir	If this option is enabled, a password is required to send an object to the Avira Malware Research Center for examination.

Configuration	If this option is enabled, configuration of Avira Premium Security Suite is only possible after entering the pre-defined password.
Enable expert mode	If this option is enabled, a password is required to enable expert mode.
Installation / Uninstallation	If this option is enabled, a password is required for installation or uninstallation of Avira Premium Security Suite.

12.7.4 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 of Avira Premium Security Suite. If this number is exceeded, a warning is displayed in the Scheduler.

Show notice if the signature database with detection patterns is out of date

If this option is enabled, you will obtain an alert message 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 message if the last update is older than n day(s).

Protect configuration file against unwanted modifications

Protect configuration

If this option is enabled, the Avira Premium Security Suite Configuration can only be saved with administrator rights.



This option is only effective if Avira Premium Security Suite is installed on an NTFS partition.

Protect job files

When this option is enabled, only a user with administrator rights can change existing scanning and update jobs and protect jobs he has created.

Protect processes

Prevent AntiVir processes from being terminated

If this option is enabled, the AntiVir processes 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 by default.



Protection is not yet available for 64-bit systems!

Protect Firewall process against termination

If this option is enabled, the Firewall are protected against unwanted termination by viruses and malware or against 'uncontrolled' termination by a user via Task-Manager. This option is enabled by default.

12.7.5 Directories

Temporary path

In this input box you enter the temporary path with which Avira Premium Security Suite works.

Use default system settings

If this option is enabled, the settings of the system are used for handling temporary files.



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.

12.7.6 Update

The section **Update** of the Avira Premium Security Suite Configuration is responsible for the configuration of the Updater .

Product updates**Download and automatically install product updates**

If this option is enabled, product updates are downloaded and automatically installed by AntiVir Updater as soon as updates become available.. Updates to the virus definition file and search engine always function 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 search engine always function 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 a warning message from AntiVir Updater in the Control Center under Manager ::Scheduler.

Do not download product updates

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

12.7.6.1. Web server

Web server

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 Avira Premium Security Suite Updater automatically detects which connection options are available. Connection options which are not available are grayed out and cannot be activated. A dial-up connection can be established manually via a phone book entry in Windows, for example.

- **User**
- **Password:** Enter the password for this account. For security, the actual characters you type in this space are replaced by asterisks (*).



If you have forgotten an existing Internet account name or password, contact your Internet Service Provider.



The automatic dial-up of the updater through so called dial-up tools (e.g. SmartSurfer, Oleco, ...) is currently not available in Avira AntiVir Professional.

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 carried out.

Download

Here you enter the address (URL) of the web server from which the updates are to be downloaded. The web server can be a server on the Internet or intranet.

Standard

The button resets the default address.

Proxy

Proxy server

Do not use a proxy server

If this option is enabled, your connection to the web server is not carried out 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.

Use the following proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

Address

Please enter the URL or the IP address of the proxy server you should use to connect to the web server.

Port

Please enter the port number of the proxy server you should use to connect to the web server.

Login name

Enter your login name on the proxy server here.

Login password

Enter the relevant password for logging in on the proxy server here. For security, the actual characters you type in this space are replaced by asterisks (*).

Examples:

Address:	proyx.domain.com	Port:	8080
Address:	192.168.1.100	Port:	3128

12.7.7 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 10 000 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)

If this option is enabled, the size of the event database is not limited.

12.7.8 Limit reports

Limit number of reports

Limit the number to n units

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

Delete all reports more than n day(s) old

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are between 1 and 90 days. This option is enabled by default with a value of 30 days.

Do not limit number of reports (manually delete reports)

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



Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: <http://www.avira.com>

© Avira GmbH. All rights reserved.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q1/2008

AntiVir® is a registered trademark of the Avira GmbH. 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. However, this does not mean that they may be used freely.