

AVG 8.5 Internet Security

User Manual

Document revision 85.6 (24.7.2009)

Copyright AVG Technologies CZ, s.r.o. All rights reserved. All other trademarks are the property of their respective owners.

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

This product uses compression library zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler.



Contents

1. Introduction ·······	5
2. AVG Installation Requirements	•
2.1 Operation Systems Supported)
2.2 Minimum Hardware Requirements ······)
3. AVG Installation Options 10)
4. AVG Download Manager 12	L
4.1 Language Selection	L
4.2 Connectivity Check	Ĺ
4.3 Proxy Settings	3
4.4 Select License Type ······ 14	1
4.5 Download Files to Install	כ
5. AVG Installation Process	5
5.1 Installation Launch ······ 16	5
5.2 License Agreement ······ 17	7
5.3 Checking System Status ······ 18	3
5.4 Select Installation Type)
5.5 Activate your AVG License)
5.6 Custom Installation - Destination Folder	L 2
5.7 Custom Installation - Component Selection	÷ ₹
5.8 AVG Security Toolbal	, 1
5.10 Setup Summary	5
5.11 Application Termination	5
5.12 Installing AVG ······ 26	5
5.13 Installation Complete ······ 27	7
6. AVG First Run Wizard 28	3
6.1 Introducing the AVG First Run Wizard ······ 28	3
6.2 Schedule regular scans and updates 29)
6.3 Help us to identify new online threats 29)
6.4 Configure the AVG Security Toolbar)
6.5 Update AVG protection ······ 31	L



A 💒 A
Tough on thread
6.6 AVG Configuration finished ······ 31
7. Firewall Configuration Wizard 33
7.1 Network Connection Options
7.2 Scan for Internet Applications
7.3 Select Profile to Activate
7.4 Configuration Review ······· 36
8 After Installation 37
o. Alter Installation
8.1 Product Registration
8.2 Access to User Interface
8.3 Scanning of the whole computer
8.4 Elcar Test
8.5 AVG Default Configuration
9. AVG User Interface
9.1 System Menu 40
9.1.1 File
9.1.2 Components ······ 40
9.1.3 History
9.1.4 Tools
9.1.5 Help
9.2 Security Status Info 43
9.3 Quick Links ····································
9.4 Components Overview
9.5 Statistics
9.6 System Tray Icon
10. AVG Components
10.1 Anti-Virus
10.1.1 Anti-Virus Principles ······ 48
10.1.2 Anti-Virus Interface ······ 48
10.2 Anti-Spyware ····· 50
10.2.1 Anti-Spyware Principles 50
10.2.2 Anti-Spyware Interface 50
10.3 Anti-Spam
<i>10.3.1 Anti-Spam Principles</i>
10.3.2 Anti-Spam Interface
10.4 Anti-Rootkit ······ 53



	Tough on three
10.4.1 Anti Rootkit Principles	51
10.4.1 Anti-Rootkit Principles	53
10.5 System Tools	54
10.5 1 Processes	
10.5.1 Processes	
10.5.2 Network Connections	
10.5.4 Browcar Extensions	
10.5.4 Diowser Extensions	
10.6 Eirowall	60
10.6 1 Firewall Principles	
10.6.2 Firewall Profiles	
10.0.5 Thewall Interface	
10.7 L Final Scanner Principles	
10.7.2 E-mail Scanner Interface	
10.7.3 E-mail Scanner Detection	
10.8 License	
10.9 Link Scanner	
10.9.1 Link Scanner Principles	
10.9.2 Link Scanner Interface	
10.9.3 AVG Search-Shield	
10 9 4 AVG Active Surf-Shield	
10 10 Web Shield	
10 10 1 Web Shield Principles	
10.10.2 Web Shield Interface	
10.10.3 Web Shield Detection	
10.11 Resident Shield	
10.11.1 Resident Shield Principles	
10.11.2 Resident Shield Interface	
10.11.3 Resident Shield Detection	
10.12 Update Manager ·····	
10.12.1 Update Manager Principles	
10.12.2 Undate Manager Interface	
10.13 AVG Security Toolbar	
11. AVG Advanced Settings	
11 1 Appearance	



	A 🛃
	Tough on threats.
11.3 Virus Vault ·····	
11.4 PUP Exceptions	
11.5 Anti-Spam ·····	
11.5.1 Settings	
11.5.2 Performance	
11.5.3 RBL ·····	
11.5.4 Whitelist ·····	
11.5.5 Blacklist	
11.5.6 Advanced Settings	
11.6 Web Shield	
11.6.1 Web Protection ·····	
11.6.2 Instant Messaging ·····	
11.7 Link Scanner ·····	
11.8 Scans ·····	
11.8.1 Scan Whole Computer	
11.8.2 Shell Extension Scan	
11.8.3 Scan Specific Files or Folders	
11.8.4 Removable Device Scan ·····	
11.9 Schedules ······	
11.9.1 Scheduled Scan ·····	
11.9.2 Virus Database Update Schedule ·····	
11.9.3 Program Update Schedule ·····	
11.9.4 Anti-Spam Update Schedule ·····	
11.10 E-mail Scanner ·····	
11.10.1 Certification ·····	
11.10.2 Mail Filtering ·····	
11.10.3 Logs and Results ·····	
11.10.4 Servers ·····	
11.11 Resident Shield ······	
11.11.1 Advanced Settings	
11.11.2 Exceptions ·····	
11.12 Anti-Rootkit	
11.13 Update ······	135
11.13.1 Proxy	
11.13.2 Dial-up	
11.13.3 URL	
11.13.4 Manage	
11 14 Remote Administration	



	A 📷
	Tough on threats
12. Firewall Settings	
12.1 General ······	
12.2 Security	
12.3 Areas and Adapters Profiles	
12.4 Logs	
12.5 Profiles	
12.5.1 Profile Information	
12.5.2 Defined Adapters	
12.5.3 Defined Networks	
12.5.4 Defined Services	
12.5.5 Applications	
12.5.6 System Services	
13. AVG Scanning	
	163
13.2.1 Scan Whole Computer	
13.2.2 Scan Specific Files or Folders	170
13.3 Scanning in Windows Explorer	
13.4 Command Line Scanning	
13.4.1 CMD Scan Parameters	
13.5.1 Schedule Settings	
13.5.2 How to Scan	
13.5.3 What to Scan	1.01
13.6 Scan Results Overview	101
13.7.1 Results Overview Tab	
13.7.3 Spyware Tab	103 102
13.7.4 Warnings Tab	10J 103
13.7.5 KOOTKITS Tab	183 102
13.7.6 Information Tab	100
13.8 Virus Vault ·····	190
14. AVG Updates	
14.1 Update Levels ·····	192
14.2 Update Types ······	192



	A
	Tough on threats.
14.3 Update Process ······	192
 15. Event History	194
16. FAQ and Technical Support	195



1. Introduction

This user manual provides comprehensive documentation for **AVG 8.5 Internet Security**.

Congratulations on your purchase of AVG 8.5 Internet Security!

AVG 8.5 Internet Security is one of a range of award winning AVG products designed to provide you with peace of mind and total security for your PC. As with all AVG products **AVG 8.5 Internet Security** has been completely re-designed, from the ground up, to deliver AVG's renowned and accredited security protection in a new, more user friendly and efficient way.

Your new **AVG 8.5 Internet Security** product has a streamlined interface combined with more aggressive and faster scanning. More security features have been automated for your convenience, and new 'intelligent' user options have been included so that you can fit our security features to your way of life. No more compromising usability over security!

AVG has been designed and developed to protect your computing and networking activity. Enjoy the experience of full protection from AVG.



2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG 8.5 Internet Security is intended to protect workstations with the following operating systems:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64, all editions)

(and possibly higher service packs for specific operating systems).

2.2. Minimum Hardware Requirements

Minimum hardware requirements for **AVG 8.5 Internet Security** are as follows:

- Intel Pentium CPU 1,2 GHz
- 250 MB of free hard drive space (for installation purposes)
- 256 MB of RAM memory



3. AVG Installation Options

AVG can be installed either from the installation file available on your installation CD, or you can download the latest installation file from the <u>AVG website</u> (<u>www.avg.com</u>).

Before you start installing AVG, we strongly recommend that you visit the <u>AVG website</u> to check for a new installation file. This way you can be sure to install the latest available version of AVG 8.5 Internet Security.

We recommend you to try out our new <u>AVG Download Manager</u> tool that will help you select the proper installation file!

During the installation process you will be asked for your license/sales number. Please make sure you have it available before starting the installation. The sales number can be found on the CD packaging. If you purchased your copy of AVG on-line, your license number will have been delivered to you via e-mail.



4. AVG Download Manager

AVG Download Manager is a simple tool that helps you select the proper installation file for your AVG product. Based on your input data, the manager will select the specific product, license type, desired components, and language. Finally, **AVG Download Manager** will go on to download and launch the appropriate <u>installation process</u>.

Following please find a brief description of each single step you need to take within the **AVG Download Manager**:

AVG Download Manager	x
	Welcome to the AVG setup program
AVG	The following screens will guide you through the process of installing AVG protection on your computer. Click the Next button to begin the installation, or Exit button to quit.
	WARNING : This program is protected by laws and international treaties. Unauthorized reproduction or distribution of this program, or any part of it, may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent allowed by law.
0	
	Choose your setup language: English
0	<u>N</u> ext > <u>E</u> xit

4.1. Language Selection

In this first step of **AVG Download Manager** select the installation language from the roll-down menu. Note, that your language selection applies only to the installation process; after the installation you will be able to change the language directly from program settings. Then press the **Next** button to continue.

4.2. Connectivity Check

In the next step, **AVG Download Manager** will attempt to establish an Internet connection so that updates can be located. You will not be allowed to advance the download process until the **AVG Download Manager** is able to complete the connectivity test.



 If the test shows no connectivity, make sure you are really connected to Internet. Then click the *Retry* button

AVG Download Manager		x
AVG	Connection issue The AVG Download Manager is not able to detect a working Internet connection. Please check to make sure that you are connected to the Internet and click Retry . If you connect to the Internet through a proxy, please click on the Proxy Settings button below to specify your proxy information.	
	Proxy Setting Retry Exit	s

 If you are using a Proxy connection to the Internet, click the *Proxy Settings* button to specify your <u>proxy information</u>:



AVG Download Manager		x
AVG	Please specify your proxy s AVG setup was unable to identify your p Please specify them below.	ettings roxy settings.
	Server:	
	Port:	
	Use proxy authentication	
	Select authentication Any (defau	ult) 🔽
	Username:	
	Password:	
0	A	pply Cancel

• If the check has been successful, press the *Next* button to continue.

4.3. Proxy Settings

AVG Download Manager		×
AVG	Please specify your proxy settings AVG setup was unable to identify your proxy settings. Please specify them below.	
	Server: Port: Vuse proxy authentication Select authentication Any (default)	~
0	Username: Password: Apply Cancel	



If **AVG Download Manager** was not able to identify your Proxy settings you have to specify them manually. Please fill in the following data:

- Server enter a valid proxy server name or IP address
- Port provide the respective port number
- **Use proxy authentication** if your proxy server requires authentication, tick this check box.
- **Select authentication** from the drop-down menu select the authentication type. We strongly recommend that you keep to the default value (*the proxy server will then automatically convey its requirements to you*). However, if you are a skilled user, you can also choose Basic (*required by some servers*) or NTLM (*required by all ISA Servers*) option. Then, enter a valid **Username** and **Password** (optionally).

Confirm your settings by pressing the **Apply** button to follow to the next step of **AVG Download Manager**.



4.4. Select License Type

In this step you are prompted to choose the license type of the product you would like to download. The description provided will allow you to select the one that suits you



most:

- Full version i.e. AVG Anti-Virus, AVG Anti-Virus plus Firewall, or AVG Internet Security
- **Trial version** provides you an opportunity to use all the features of AVG full product for the limited time period of 30 days
- **Free version** provides protection to home users free of charge, however the application functions are limited! Also, the free version only includes some of the features available in the paid product.

x

4.5. Download Files to Install

Now, you have provided all information needed for the **AVG Download Manager** to start the installation package download, and launch the installation process. Further, advance to the <u>AVG Installation Process</u>.



5. AVG Installation Process

To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date.

Therefore we recommended getting the latest installation file online. You can download the file from the <u>AVG website</u> (at <u>www.avg.com</u>) / **Downloads** section. Or, you can make use of our new <u>AVG Download Manager</u> tool that helps you create and download the installation package you need, and launch the installation process.

The installation is a sequence of dialog windows with a brief description of what do at each step. In the following, we offer an explanation for each dialog window:

🛃 AVG 8.0 build 204 (10/10/2008)			
AVG	Welcome to the AVG Setup Program		
The following screens will guide you through the process of installing AVG protection on your computer. Click Next to begin th process or click Exit to quit.			
	Before you begin the process, you may find it useful to review the advice and recommendations we've prepared to help you set up the software to best meet your needs.		
	WARNING: This program is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent allowed by law.		
	Choose your setup language		
	Next > Exit		

5.1. Installation Launch

The installation process starts with the **Welcome to the AVG Setup Program** window. In here you select the language used for the installation process. In the lower part of the dialog window find the **Choose your setup language** item, and select the desired language from the drop down menu. Then press the **Next** button to confirm and continue to the next dialog.

Attention: Here, you are selecting the language for the installation process only. You are not selecting the language for the AVG application - that can be specified later on during the installation process!



5.2. License Agreement



The *License Agreement* dialog provides the full wording of the AVG license agreement. Please read it carefully and confirm that you have read, understood and accept the agreement by pressing the *Accept* button. If you do not agree with the license agreement press the *Don't accept* button, and the installation process will be terminated immediately.



5.3. Checking System Status

🞽 AVG 8.0 build 204 (10/13/2008)		
	Checking System Status	
📕 🕌 AVG	file Inglog.cfg: checking state	
	Cancel	

Having confirmed the license agreement, you will be redirected to the *Checking System Status* dialog. This dialog does not require any intervention; your system is being checked before the AVG installation can start. Please wait until the process has finished, then continue automatically to the following dialog.



5.4. Select Installation Type

🕌 AVG 8.0 build 204 (10/13/2008) 🛛 🛛 🔀	
	Select Installation Type
AVG 📲	© Standard Installation Choose this option to install the software in its standard configuration, which provides optimum protection for most users.
	Custom Installation Choose this option if you want to change some of the standard configuration attributes. This option is recommended for IT well-experienced users.
	< <u>B</u> ack <u>N</u> ext > <u>E</u> xit

The **Select Installation Type** dialog offers the choice of two installation options: **standard** and **custom** installation.

For most users, it is highly recommended to keep to the **standard installation** that installs AVG in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of resources. In the future, if the need arises to change the configuration, you will always have the possibility to do so directly in the AVG application.

Custom installation should only be used by experienced users who have a valid reason to install AVG with non-standard settings. E.g. to fit specific system requirements.

5.5. Activate your AVG License

In the **Activate your AVG License** dialog you have to fill in your registration data. Type in your name (**User Name** field) and the name of your organization (**Company Name** field).

Then enter your license/sales number into the *License/Sales Number* text field. The sales number can be found on the CD packaging in your AVG box. The license number will be in the confirmation email that you received after purchasing your AVG on-line. You must type in the number exactly as shown. If the digital form of the license



number is available (in the email), it is recommended to use the copy and paste method to insert it.

🕌 AVG 8.0 build 204 (10/13/2008)		
	Activate your AVG License	
📕 AVG	<u>U</u> ser name:	Name Surname
	<u>C</u> ompany name:	Company name
	License number:	
	If you purchased th been sent to you by cutting and pasting If you purchased th license number on I package. Take car	e software online, your license number will have ye-mail. To avoid typing errors, we recommend the number from the e-mail to this screen. e software in a retail store, you will find the he product registration card included with the e to copy the number correctly.
		< <u>B</u> ack <u>N</u> ext> <u>E</u> xit

Press the *Next* button to continue the installation process.

If in the previous step you have selected the standard installation, you will be redirected directly to the *Installation Summary* dialog. If custom installation was selected you will continue with the *Destination Folder* dialog.



5.6. Custom Installation - Destination Folder

🕌 AVG 8.0 build 204 (10/13/2008) 🛛 🛛 🔀	
	Destination Folder
AVG	The default destination folder is shown below. You can click Browse button to select a different folder, but we recommend using the default settings.
	Destination folder:
	C:\Program Files\AVG\AVG8
	Browse
	< Back Next > Exit

The **Destination Folder** dialog allows you to specify the location where AVG should be installed. By default, AVG will be installed to the program files folder located on drive C:. If you want to change this location, use the **Browse** button to display the drive structure, and select the respective folder. Press the **Next** button to confirm.



5.7. Custom Installation - Component Selection



The **Component Selection** dialog displays an overview of all AVG components that can be installed. If the default settings do not suit you, you can remove/add specific components.

However, you can only select from components that are included in your purchased AVG edition. Only those components will be offered to be installed within the Component Selection dialog!

Within the list of components to be installed, you can define which language(s) AVG should be installed in. Check the **Additional installed languages** item and then select the desired languages from the respective menu.

Click the *E-mail Scanner* item to open and decide on what plug-in is to be installed to guarantee your electronic mail security. By default, *Plugin for Microsoft Outlook* will be installed. Another specific option is the *Plugin for The Bat!* If you use any other e-mail client (*MS Exchange, Qualcomm Eudora, ...*), go for the *Personal E-mail Scanner* option to secure your e-mail communication automatically no matter what e-mail program you run.

Continue by pressing the *Next* button.



5.8. AVG Security Toolbar



In the **AVG Security Toolbar** dialog, decide whether you want to install the <u>AVG</u> <u>Security Toolbar</u> - if you do not change the default settings, this component will be installed automatically into your Internet browser; in conjunction with AVG 8.0 and AVG XPL technologies to provide you with comprehensive online protection while surfing the Internet.



5.9. Windows Firewall



The license number you have provided in one of the previous setup steps responds to **AVG 8.5 Internet Security** edition that includes AVG *Firewall*. AVG *Firewall* cannot run parallelly with another installed firewall. In this dialog please confirm you want to install AVG *Firewall*, and you wish to deactivate the Windows Firewall at the same time.

Press the **Next** button to continue.



5.10.Setup Summary



The **Setup Summary** dialog provides an overview of all parameters of the installation process. Please make sure all the information is correct. If so, press the **Finish** button to continue. Otherwise, you can use the **Back** button to return to the respective dialog and correct the information.

5.11.Application Termination

Before the installation process starts, you might be invited to terminate some of the currently running applications that might collide with the AVG installation process. In such a case, you will see the following **Application Termination** dialog. This dialog is only to inform you and does not require any intervention - if you agree to having closed the listed programs automatically, press **Next** to continue:



AVG 8.0 build 204 (10/1	3/2008)
	Applications Termination
AVG	The following applications must be terminated prior to installation. Press Next to terminate these applications, and begin installation. AVG PRODUCTS - Microsoft Outlook Dokument2 - Microsoft Word Microsoft Word mistnost u pani Svobodove - ?? - Zpráva (HTML) rctrl_renwnd32
	Kext Seck Next Sector S

Note: Please make sure you have saved all your data before you confirm you want to have the running application closed.

5.12.Installing AVG

The **Installing AVG** dialog shows the progress of the installation process, and does not require any intervention:

🛃 AVG 8.0 build 204 (10/13/2008)	
	Installing AVG
📕 AVG	file overlay.dtd: creating backup
	Cancel



Please wait until the installation is complete, then you will be redirected to the Installation Complete dialog.

5.13.Installation Complete

🕌 AVG 8.0 build 204 (10/13/2008)	
	Installation is complete!
AVG	AVG has been successfully installed
	If you have any questions or concerns, please refer to the help section in the software or visit <u>www.avq.com</u> .

The **Installation is complete!** dialog is the last step of the AVG installation process. AVG is now installed on your computer and fully functional. The program is running in the background in fully automatic mode.

After the installation, <u>AVG Basic Configuration Wizard</u> will be launched automatically and in a few steps will lead you through the **AVG 8.5 Internet Security** elementary configuration. Despite the fact the AVG configuration is accessible any time during AVG run, we deeply recommend to use this option and set up the basic configuration with the wizard's help.



6. AVG First Run Wizard

When you first install AVG on your computer, the **AVG Basic Configuration Wizard** pops up to help you with initial **AVG 8.5 Internet Security** settings. Though you can set all of the suggested parameters later on, it is recommended that you take the wizard's tour to secure your computer's protection simply and immediately. Follow the steps described in each of the wizard's windows:

6.1. Introducing the AVG First Run Wizard

😹 Configuring your AVG protection 🛛 🛛 🔀	
Step 1 of 7: Introd	ucing the AVG First Run Wizard
	Congratulations!
	AVG has been successfully installed on your computer.
Ins	A few simple steps remain to ensure optimum protection and ease of use. AVG First Run Wizard will guide you through the following:
	 Schedule regular scans and updates
	How you can help with our threat research
	 Configuring the AVG Security Toolbar
	Completing your first update
	Click Next to schedule your scans and updates.
Help	Next>

The **Introducing the AVG First Run Wizard** welcome window briefly summarizes the status of AVG on your computer, and suggests the steps to be taken to complete protection. Click on the **Next** button to continue.



6.2. Schedule regular scans and updates

🕌 Configuring your AVG protection	$\overline{\mathbf{X}}$
Step 2 of 7: Schedule regular scans and updates	
Updates: How often would you like your AVG protection to be updated?	
Scans: What time would you like your daily scan to take place? 12:00 💭 I Enable daily scanning (recommended) Click Next to see how you can help with AVG threat research	
Help	< Back Next >

In the **Schedule regular scans and updates** dialog set up the interval for new update files accessibility check-up, and define time when the <u>scheduled scan</u> should be launched. It is recommended to keep the default values. Press the **Next** button to continue.

6.3. Help us to identify new online threats

😹 AVG First Run Wizard	X
Step 3 of 7: Help us to identify new threats	
By checking this box, you give us permission to collect detected threats way you help us maintain the virus databases, and improve our service t	you might have encountered. This to you.
No personally-identifiable information is collected.	
Read AVG Privacy Policy	
Yes, I agree to provide information about potentially dange	erous websites to A¥G
Click Next to configure AVG Security Toolbar	
Help	< Back Next >



In the *Help us to identify new threats* dialog decide whether you want to activate the option of reporting of exploits and bad sites found by users either via *AVG Surf-Shield / AVG Search-Shield* features of the *LinkScanner* component to feed the database collecting information on malicious activity on the web. It is recommended to keep the default value and have the reporting activated. Press the *Next* button to continue.

6.4. Configure the AVG Security Toolbar

🕌 Configuring your AVG protection	$\overline{\mathbf{X}}$
Step 4 of 7: Configure the AVG Security Toolbar	
Yahoo! Search The AVG Security Toolbar includes Yahoo! search. If you installed the Too Yahoo! as your default (preferred) search engine, check the box below.	lbar and would like to set
Yes, change my default search engine to Yahoo!	
Click Next to update your AVG	
Help	< Back Next >

In the **Configure the AVG Security Toolbar** dialog you can tick the check box to define you want Yahoo! to become your default search engine.



6.5. Update AVG protection

😹 Configuring your AVG protection	×
Step 5 of 7: Update AVG protection	
New threats are appearing all the time, and it's very like downloaded the software. Both program updates and threat detection updates ar	ely new updates to AVG have been issued since you e included with your AVG license.
Click Next to check for the latest updates, or click Ski	${f p}$ to complete the AVG First Run Wizard.
Help	Skip < Back Next >

The **Update AVG protection** dialog will automatically check and download the latest <u>AVG updates</u>. Click on the **Next** button to download the latest update files and perform the update.

6.6. AVG Configuration finished

불 AVG First Run Wiza	ard 🛛 🔀
Step 7 of 7: The firs	st part of AVG configuration is finished.
K	The first part of AVG configuration is complete. We strongly recommend you proceed to the Firewall Configuration Wizard and complete the configuration, otherwise the component may not work properly. Please note that once you proceed to the Firewall Configuration Wizard you cannot go back to the first part of the AVG First Run Wizard! Click Next to proceed to the Firewall Configuration Wizard.
Help	< Back Next>



Now your **AVG 8.5 Internet Security** has been configured; press the **Finish** button to start working with AVG.



7. Firewall Configuration Wizard

Firewall Configuration Wizard launches automatically right after the AVG 8.5 Internet Security installation. Though you can <u>configure the component's</u> parameters later on, it is recommended that you take the wizard's tour to ensure the *Firewall* works properly.

Firewall Configuration Wizard can also be called directly from the <u>Firewall</u> <u>interface</u> by pressing the *Configuration wizard* button.

Firewall Configuration Wizard Network connection options How is your computer connected to the Internet? For maximum security, without disturbing the current network services that you access, it is necessary to select ALL connection types that you use to connect to the Internet. Available profiles Standalone computer Computer in domain Computer on the move Small home or office network Help Next >

7.1. Network Connection Options

In this dialog, the *Firewall Configuration Wizard* asks how your computer is connected to the Internet. For instance, your notebook, that connects to the Internet from many different locations (*airports, hotel rooms, etc.*) requires security rules that are stricter than those of a computer in a domain (*company network, etc.*). Based on the selected connection type the *Firewall* default rules will be defined with a different security level.

You have three options to select from:

- Standalone computer
- Computer in domain (company network)
- Computer on the move (typically a notebook)



• Small home or office network

In this dialog please choose the connection type(s), that suit your normal computer usage. You can tick more than one choice that corresponds to your current usage. Confirm your selection by pressing the **Next** button and proceed to the next dialog.

7.2. Scan for Internet Applications

불 Firewall Configuratio	n Wizard			×
Scan for Internet appli Which areas of your co	cations mputer shc	ould be scanned?		
To make sure your computer programs. The Firewall Config should be allowed to commun	will work corre guration Wizar icate over the	ctly it is necessary to d will now scan your c network.	allow network commu omputer and try to fi	unication for some nd applications that
Select scanning option:				
🔿 Quick search (take advani	age of curren	t settings for update)		
🔘 Complete scan (scan all lo	cal hard drives	of your computer)		
 Common directories (scan 	program and '	Windows directories)		
 Selected areas scan (scar 	selected harc	l drives)		
Drive Drive size	Free size	Drive label		
☑	57.2 GB			
Help			< Ba	ack Next >

To set the initial *Firewall* configuration it is necessary to scan your computer and define all applications and system services that need to communicate over the network. Initial *Firewall* rules should be created for all those applications and services.

Note: The wizard detects all generally known applications communicating over the network, and defines rules for these applications. However, it will not detect all such applications.

Within the **Scan for Internet applications** dialog you have to decide whether you want to run:

• **Quick search** - text this option is only active if you have configured the <u>Firewall</u> previously, and only applications that are currently saved within the existing <u>Firewall</u> configuration will be searched for. New default configuration (i.e. manufacturer recommended) will then be applied to these. Please note that no new applications will be detected! We recommend this option if you already have <u>Firewall</u> rules defined, and want to avoid repeating the whole scanning process.



- Complete scan scan all local hard drives of your computer
 - Common directories (by default) scan program and Windows directories only, scanning time is significantly shorter
 - Selected areas scan specify selected hard drives to be scanned

7.3. Select Profile to Activate

The **Select profile to activate** dialog informs you about the **<u>Firewall</u>** configuration set up in the previous dialogs.

Before closing the *Firewall Configuration Wizard* it is necessary that you select a profile you want to use on your computer. You can choose from up to three options (standalone computer, computer in domain, and computer on the move) based on the connection parameters you have specified in the first dialog (*Network Connection Options*) of this wizard. You can then later on switch between the pre-defined *Firewall* profiles according to the current state of your computer.

At the moment simply select the desired profile from the list and activate it by pressing the **Next** button:

🕌 Firewall Configuration Wizard			
Select profile to activate Automatic Firewall configuration has finis	hed successfully	SC	
Assign profile later by network area detection an	d automatic profile switch		
The Firewall Configuration Wizard has lead you throu created for selected system services and protocols, network.Press the Next button to save all settings.	igh the configuration proc and for selected application	ess.Initial rules have ons communicating over	been er the
Select the profile you would like to activate after o	ompleting the wizard		
Standalone computer			
Help		< Back	Next >

If you do not want to set up the profiles manually you can switch on the function of profile's automatic detection. In that case *Firewall* will automatically select the most appropriate profile based on where and how your computer currently connects to the network. The automatic profile selection guarantees maximum security! To select this option, tick the *Assign profile later by network area detection and automatic profile switch* item in the upper part of the dialog:



🛃 Firewall Configuration Wizard 🛛 🛛 🔯
Select profile to activate Automatic Firewall configuration has finished successfully
Assign profile later by network area detection and automatic profile switch
The Firewall Configuration Wizard has lead you through the configuration process. Initial rules have been created for selected system services and protocols, and for selected applications communicating over the network.Press the Next button to save all settings.
Select the profile you would like to activate after completing the wizard
Standalone computer
Help (Back Next >

This way the profile list will get deactivated and you just press the **Next** button to continue to the following wizard's dialog.

7.4. Configuration Review

Firewall Configuration Wizard	
Configuration Revie w Revie w the generated configuration	
You can review the newly generated configuration Firewall settings will be launched.	n by pressing the Open review button. Advanced en review
Нер	Back Finish Cancel

The **Configuration Review** dialog closes the **Firewall Configuration Wizard**. Press the **Finish** button to finalize the **Firewall**'s initial settings. If you would like to see a review of set up parameters, or to continue with the detailed configuration of the **Firewall** component press the **Open review** button to switch to the **Firewall** <u>Settings</u> editing interface.


8. After Installation

8.1. Product Registration

Having finished the **AVG 8.5 Internet Security** installation, please register you product online on the <u>AVG website</u>, **Registration** page (*follow the instruction provided directly in the page*). After the registration you will be able to gain full access to your AVG User account, the AVG Update newsletter, and other services provided exclusively for registered users.

8.2. Access to User Interface

The **<u>AVG User Interface</u>** is accessible in several ways:

- double-click the AVG icon on the system tray
- double-click the AVG icon on the desktop
- from the menu Start/All Programs/AVG 8.0/AVG User Interface

8.3. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG 8.5 Internet Security** installation. For this reason you should run a *Scan of the whole computer* to make sure there are no infections on your PC.

For instructions on running a <u>Scan of the whole computer</u> please consult the chapter <u>AVG Scanning</u>.

8.4. Eicar Test

To confirm that **AVG 8.5 Internet Security** has been installed correctly you can perform the EICAR test.

The EICAR test is a standard and absolutely safe method used to test antivirus system functioning. It is safe to pass around, because it is not an actual virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (*though they typically report it with an obvious name, such as "EICAR-AV-Test"*). You can download the EICAR virus from the EICAR website at <u>www.eicar.com</u>, and you will also find all necessary EICAR test information there.



Try to download the *eicar.com* file, and save it on your local disk. Immediately after you confirm downloading of the test file, the <u>Web Shield</u> will react to it with a warning. This <u>Web Shield</u> notice demonstrates that AVG is correctly installed on your computer.

🕌 Web Shie	ld alert		$\overline{\mathbf{X}}$		
Accessed F	ile is infected				
	threat de	etected!			
	File name:	www.eicar.org/download/eicar.com			
	threat name:	Virus identified EICAR_Test More information about this threat			
Close					
Show details					

If AVG fails to identify the EICAR test file as a virus, you should check the program configuration again!

8.5. AVG Default Configuration

The default configuration (*i.e. how the application is set up right after installation*) of **AVG 8.5 Internet Security** is set up by the software vendor so that all components and functions are tuned up to achieve optimum performance.

Unless you have a real reason to do so, do not change the AVG configuration! Changes to settings should only be performed by an experienced user.

Some minor editing of <u>AVG components</u> settings is accessible directly from the specific component user interface. If you feel you need to change the AVG configuration to better suit your your needs, go to <u>AVG Advanced Settings</u>: select the system menu item **Tools/Advanced settings** and edit the AVG configuration in the newly opened <u>AVG Advanced Settings</u> dialog.



9. AVG User Interface

AVG 8.5 Internet Security open with the main window:



The main window is divided into several sections:

- **System Menu** (top system line in the window) is the standard navigation that allows you to access all AVG components, services, and features <u>details >></u>
- **Security Status Info** (upper section of the window) provides you with information on the current status of your AVG program <u>details >></u>
- Quick Links (left section of the window) allow you to quickly access the most important and most frequently used AVG tasks - <u>details >></u>
- Components Overview (central section of the window) offer an overview of all installed AVG components - <u>details >></u>



- Statistics (left bottom section of the window) provide you with all statistical data regarding the programs operation <u>details >></u>
 - System Tray Icon (bottom right corner of the monitor, on the system tray) indicates the AVG current status - <u>details >></u>

9.1. System Menu

The **System menu** is the standard navigation used in all Windows applications. It is located horizontally in the very top part of the **AVG 8.5 Internet Security** main window. Use the system menu to access specific AVG components, feature, and services.

The system menu is divided into five main sections:

9.1.1. File

• *Exit* - closes the **AVG 8.5 Internet Security**'s user interface. However, the AVG application will continue running in the background and your computer will still be protected!

9.1.2. Components

The <u>*Components*</u> item of the system menu includes links to all installed AVG components, opening their default dialog page in the user interface:

- **System overview** switch to the default user interface dialog with the overview of all installed components and their status
- Anti-Virus opens the default page of the Anti-Virus component
- Anti-Rootkit opens the default page of the Anti-Rootkit component
- Anti-Spyware opens the default page of the Anti-Spyware component
- Firewall opens the default page of the Firewall component
- System Tools opens the default page of the System Tools
- Anti-Spam opens the default page of the Anti-Spam component
- *E-mail Scanner* opens the default page of the *E-mail Scanner* component
- License opens the default page of the License component



- *LinkScanner* opens the default page of the *LinkScanner* component
 - Web Shield opens the default page of the Web Shield component
 - Resident Shield opens the default page of the Resident Shield component
 - Update Manager opens the default page of the <u>Update Manager</u> component

9.1.3. History

- <u>Scan results</u> switches to the AVG testing interface, specifically to the <u>Scan</u> <u>Results Overview</u> dialog
- <u>Resident Shield Detection</u> open a dialog with an overview of threats detected by <u>Resident Shield</u>
- <u>E-mail Scanner Detection</u> open a dialog with an overview of mail messages attachments detected as dangerous by the <u>E-mail Scanner</u> component
- <u>Web Shield findings</u> open a dialog with an overview of threats detected by <u>Web Shield</u>
- <u>Virus Vault</u> opens the interface of the quarantine space (<u>Virus Vault</u>) to where AVG removes all detected infections that cannot be healed automatically for some reason. Inside this quarantine the infected files are isolated and your computer's security is guaranteed, and at the same time the infected files are stored for possible future repair.
- <u>Event History Log</u> opens the history log interface with an overview of all logged **AVG 8.5 Internet Security** actions.
- <u>Firewall</u> opens the Firewall settings interface on the <u>Logs</u> tab with a detailed overview of all Firewall actions

9.1.4. Tools

- <u>Scan computer</u> switches to the <u>AVG scanning interface</u> and launches a scan of the whole computer
- <u>Scan selected folder</u> switches to the <u>AVG scanning interface</u> and allows you to define within the tree structure of your computer which files and folders should be scanned



- Scan file allows you to run an on-demand test over a single file selected from the tree structure of your disk
 - <u>Update</u> automatically launches the update process of AVG 8.5 Internet Security
 - **Update from directory** runs the update process from the update files located in a specified folder on your local disk. However, this option is only recommended as an emergency, e.g. in situations where there is no connection to the Internet (*for example, your computer is infected and disconnected from the Internet; your computer is connected to a network with no access to the Internet, etc.*). In the newly opened window select the folder where you have previously placed the update file, and launch the update process.
 - <u>Advanced settings</u> opens the <u>AVG advanced settings</u> dialog where you can edit the AVG 8.5 Internet Security configuration. Generally, it is recommended to keep the default settings of the application as defined by the software vendor.
 - <u>Firewall settings</u> open a standalone dialog for advanced configuration of the <u>Firewall</u> component

9.1.5. Help

- Contents opens the AVG help files
- Get Help Online opens the <u>AVG</u> website at the customer support center page
- Your AVG Web opens the AVG homepage (at www.avg.com)
- About Viruses and Threats opens the online <u>Virus Encyclopedia</u> where you can look up detailed information on the identified virus
- **<u>Reactivate</u>** opens the **Activate AVG** dialog with the data you have entered in the <u>**Personalize AVG**</u> dialog of the <u>installation process</u>. Within this dialog you can enter your license number to either replace the sales number (*the number you have installed AVG with*), or to replace the old license number (*e. g. when upgrading to a new AVG product*).
- <u>**Register now</u>** connects to the registration website at <u>www.avg.com</u>. Please fill in your registration data; only customers who register their AVG product can receive free technical support.</u>



• **About AVG** - opens the **Information** dialog with five tabs providing data on program name, program and virus database version, system info, license agreement, and contact information of **AVG Technologies CZ**.

9.2. Security Status Info

The **Security Status Info** section is located in the upper part of the AVG main window. Within this section you will always find information on the current security status of your **AVG 8.5 Internet Security**. Please see an overview of icons possibly depicted in this section, and their meaning:

The green icon indicates that your AVG is fully functional. Your computer is completely protected, up to date and all installed components are working properly.



The orange icon warns that one or more components are incorrectly configured and you should pay attention to their properties/settings. There is no critical problem in AVG and you have probably decided to switch some component off for some reason. You are still protected by AVG. However, please pay attention to the problem component's settings! Its name will be provided in the **Security Status Info** section.

This icon also appears if for some reason you have decided to <u>ignore a</u> <u>component's error status</u> (the "**Ignore component state**" option is available from the context menu opened by a right-click over the respective component's icon in the component overview of the AVG main window). You may need to use this option in a specific situation but it is strictly recommended to switch off the "**Ignore component state**" option as soon as possible.



The red icon indicates that AVG is in critical status! One or more components does not work properly and AVG cannot protect your computer. Please pay immediate attention to fixing the reported problem. If you are not able to fix the error yourself, contact the <u>AVG technical support</u> team.

It is strongly recommended that you pay attention to **Security Status Info** and in case the report indicates any problem, go ahead and try to solve it immediately. Otherwise your computer is at risk!



Note: AVG status information can also be obtained at any moment from the <u>system</u> <u>tray icon</u>.

9.3. Quick Links

Quick links (in the left section of the <u>AVG User Interface</u>) allow you to immediately access the most important and most frequently used AVG features:

Overview
Computer scanner
Update now
Updating

- Overview use this link to switch from any currently opened AVG interface to the default one with an overview of all installed components - see chapter <u>Components Overview >></u>
- Computer scanner use this link to open the AVG scanning interface where you can run tests directly, schedule scans, or edit their parameters - see chapter <u>AVG Tests</u> >>
- Update now this link open the updating interface, and launches the AVG update process immediately - see chapter <u>AVG Updates</u> >>

These links are accessible from the user interface at all times. Once you use a quick link to run a specific process, the GUI will switch to a new dialog but the quick links are still available. Moreover, the running process is further graphically depicted - *see picture 2*.



9.4. Components Overview

The **Components Overview** section is located in the central part of the <u>AVG User</u> <u>Interface</u>. The section is divided into two parts:

- Overview of all installed components consisting of a panel with the component's icon and the information of whether the respective component is active or inactive
- Description of a selected component

Within the **AVG 8.5 Internet Security** the *Components Overview* section contains information on the following components:

- Anti-Virus ensures that your computer is protected from viruses trying to enter your computer - <u>details >></u>
- Anti-Spyware scans your applications in the background as you run them details >>
- Anti-Spam checks all incoming e-mail messages and marks unwanted e-mails as SPAM - <u>details >></u>
- Anti-Rootkit detects programs and technologies trying to camouflage malware - <u>details >></u>



- System Tools offers a detailed summary of the AVG environment details
 - Firewall controls how your computer exchanges data with other computers on the Internet or local network - <u>details >></u>
 - *E-mail Scanner* checks all incoming and outgoing mail for viruses <u>details</u>
 >>
 - License provides full wording of the AVG License Agreement details >>
 - LinkScanner checks the search results displayed in your internet browser details >>
 - Web Shield scans all data being downloaded by a web browser details >>
 - Resident Shield runs in the background and scans files as they are copied, opened or saved - <u>details >></u>
 - **Update Manager** controls all AVG updates <u>details >></u>

Single-click any component's icon to highlight it within the components overview. At the same time, the component's basic functionality description appears in the bottom part of the user interface. Double-click the icon to open the components own interface with a list of basic statistical data.

Right-click you mouse over a component's icon to expand a context menu: besides opening the component's graphic interface you can also select to **Ignore component state**. Select this option to express you are aware of the <u>component's error state</u> but for some reason you wish to keep your AVG so and you do not want to be warned by the grey color of the <u>system tray icon</u>.

9.5. Statistics

The **Statistics** section is located in the left bottom part of the <u>AVG User Interface</u>. It offers a list of information regarding the program's operation:

- Last scan provides the date when the last scan was performed
- Last update provides the date when the last update was launched
- **Virus DB** informs you about the currently installed version of the virus database



- **AVG version** informs you about the AVG version installed (the number is in the form of 8.0.xx, where 8.0 is the product line version, and xx stands for the number of the build)
 - License expires provides the date of your AVG license expiration

9.6. System Tray Icon

System Tray Icon (on your Windows taskbar) indicates the current status of your **AVG 8.5 Internet Security**. It is visible at all times on your system tray, no matter whether your AVG main window is opened or closed.

If in full color **System Tray Icon** indicates that all AVG components are active and fully functional. Also, AVG system tray icon can be displayed in full color if AVG is in error state but you are fully aware of this situation and you have deliberately decided to **Ignore the component state**.

A gray icon coloring with an exclamation mark an indicates a problem (inactive component, error status, etc.). Double-click the **System Tray Icon** to open the main window and edit a component.

The system tray icon further informs on current AVG activities and possible status changes in the program (*e.g. automatic launch of a scheduled scan or update, Firewall profile switch, a component's status change, error status occurrence, ...*) via a pop-up window opened from the AVG system tray icon:

2	Scan		×
	Scheduled scan was	s started.	
) s	17 🛞	10:38

The **System Tray Icon** can also be used as a quick link to access the AVG main window at any time - double click on the icon. By right-click on the **System Tray Icon** you open a brief context menu with the following options:

- Open AVG User Interface click to open the AVG User Interface
- Update launches an immediate update
- **Exit** click to close AVG (You only close the user interface, AVG continues to run in the background and your computer is still fully protected!)



10. AVG Components

10.1.Anti-Virus

10.1.1.Anti-Virus Principles

The antivirus software's scanning engine scans all files and file activity (opening/closing files, etc.) for known viruses. Any detected virus will be blocked from taking any action and will then be cleaned or quarantined. Most antivirus software also uses heuristic scanning, where files are scanned for typical virus characteristics, so called viral signatures. This means that the antivirus scanner can detect a new, unknown virus, if the new virus contains some typical characteristics of existing viruses.

The important feature of antivirus protection is that no known virus can run on the computer!

Where just a single technology might fall short of detecting or identifying a virus, **Anti-Virus** combines several technologies to ensure that your computer is protected from viruses:

- Scanning searching for character strings that are characteristic of a given virus
- Heuristic analysis dynamic emulation of the scanned object's instructions in a virtual computer environment
- Generic detection detection of instructions characteristic of the given virus/group of viruses

AVG is also able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system. We call such threats Potentially Unwanted Programs (various kinds of spyware, adware etc.). Furthermore, AVG scans your system registry for suspicious entries, temporary Internet files and tracking cookies, and allows you to treat all potentially harmful items in the same way as any other infection.



10.1.2.Anti-Virus Interface

🛃 AVG Internet Security 📃 🔲						
File Components History Tools He	elp					
AVG Internet Security	You are protect All security features	ed. are working correctly and are up to date.				
	Anti-Virus Component					
0verview	Anti-virus Component					
Anti Minus	Anti-Virus deter that could be pote	ts viruses, worms and trojans as well as executable files or DLL libraries entially unwanted within your system. Anti-Virus also holds the internal				
E Antrias	virus database, a up-to-date to mai	nd therefore it is crucial that you keep the Anti-Virus component ntain the maximum level of protection.				
Computer scanner						
📝 Update now	🛛 Anti-Virus component is act	ive.				
	Infection definitions:	1596338 22 října 2008, 9:23				
	Database version:	270.8.2/1739				
Statistics						
Last scan: 22.10.08, 12:00						
Last update: 22.10.08, 11:59 Virus DB: 270.8.2/1739						
AVG version: 8.0.206						
License expires: 1.1.2018		Back				
Show notification						

The **Anti-Virus** component's interface provides some basic information on the component's functionality, information on the component's current status (*Anti-Virus component is active.*), and a brief overview of **Anti-Virus** statistics:

- **Infection definitions** number provides the count of viruses defined in the up-to-date version of the virus database
- Latest database update specifies when and at what time the virus database was last updated
- **Database version** defines the number of the latest virus database version; and this number increases with every virus base update

There is just one operating button available within this component's interface (**Back**) - press the button to return to the default <u>AVG user interface</u> (components overview).

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.



10.2.Anti-Spyware

10.2.1.Anti-Spyware Principles

Spyware is usually defined as a type of malware, i.e. software, that gathers information from a user's computer without the user's knowledge or consent. Some spyware applications may also be installed on purpose and often contain advertisements, window pop-ups or different types of unpleasant software.

Currently, the most common source of infection is websites with potentially dangerous content. Other methods of transmission, such as via e-mail or transmission by worms and viruses are also prevalent. The most important protection is to use an always-on background scanner, *Anti-Spyware*, that works like a resident shield and scans your applications in the background as you run them.

There is also the potential risk that malware has been transmitted to your computer prior to AVG installation, or that you have neglected to keep your **AVG 8.5 Internet Security** up-to-date with the latest database and <u>program updates</u>. For this reason, AVG allows you to fully scan your computer for malware/spyware using the scanning feature. It also detects sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated.



10.2.2.Anti-Spyware Interface



The **Anti-Spyware** component's interface provides a brief overview on the component's functionality, information on the component's current status (*Anti-Spyware component is active.*), and some **Anti-Spyware** statistics:

- **Spyware definitions** number provides the count of spyware samples defined in the latest spyware database version
- Latest database update specifies when and at what time the spyware database was updated
- **Database version** defines the number of the latest spyware database version; and this number increases with every virus base update

There is just one operating button available within this component's interface (**Back**) - press the button to return to the default <u>AVG user interface</u> (components overview).

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.

10.3.Anti-Spam

10.3.1.Anti-Spam Principles

Spam refers to unsolicited e-mail, mostly advertising a product or service that is mass mailed to a huge number of e-mail addresses at a time, filling recipients' mail boxes. Spam does not refer to legitimate commercial e-mail for which consumers have given their consent. Spam is not only annoying, but also can often be a source of scams, viruses or offensive content.

Anti-Spam checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages.



10.3.2.Anti-Spam Interface

🚔 AVG Internet Security		_	
File Components History Tools H	əlp		
AVG Internet Security	You are protected All security features a	d. re working correctly and are up to date.	
	Anti-Snam Component		
0verview	· · · · · · · · · · · · · · · · · · ·		
	Anti-Spam checks uses several analyz	; all incoming e-mail messages and marks unwanted e-mails as SPAM ting methods offering maximum possible protection.	1. It
Anti-Spam		· · · · · · · · · · · · · · · · · · ·	
Computer scanner			
🕼 Update now	Anti-Spam component is activ	ve.	
	Database release:	22. října 2008, 3:14	
	Spamcatcher version:	5.1.0	
Statistics			
Last scan: 22.10.08, 12:00			
Virus DB: 270.8.2/1739			
AVG version: 8.0.206			
License expires: 1.1.2018		Back	
Show notification		Back	

In the **Anti-Spam** component's dialog you will find a brief text describing the component's functionality, information on its current status (*Anti-Spam component is active.*), and the following statistics:

- **Database release** specifies when and at what time the spam database was updated and published
- **Spamcatcher version** defines the number of the latest version of the antispam engine

There is just one operating button available within this component's interface (**Back**) - press the button to return to the default <u>AVG user interface</u> (components overview).

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.



10.4.Anti-Rootkit

10.4.1.Anti-Rootkit Principles

Anti-Rootkit is a specialized tool detecting and effectively removing dangerous rootkits, i.e. programs and technologies that can camouflage the presence of malicious software on your computer.

A rootkit is a program designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. Access to the hardware is rarely required as a rootkit is intended to seize control of the operating system running on the hardware. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. Often, they are also Trojans as well, thus fooling users into believing they are safe to run on their systems. Techniques used to accomplish this can include concealing running processes from monitoring programs, or hiding files or system data from the operating system.

10.4.2.Anti-Rootkit Interface

📬 AVG Internet Security				
File Components History Tools H	lelp			
AVG Internet Security	You are pro All security feat	lected. ures are working correctly and are up to date.		
Overview Overview Anti-Rootkit Computer scanner	Anti-Rootkit Compo Anti-Rootl dllibraries. administrato very well hic regular sec.	nent at component scans for dangerous rootkits hidden inside applications, drivers or A rootkit is usually a collection of malicious software that allows attacker to gain r-level access to a computer or possibly whole network. Rootkits are generally iden in an operating system which makes them hard to detect or remove by riv tools.		
📝 Update now	Anti-Rootkit component is active.			
	Last rootkit search:	Not yet scanned		
	Anti-Rootkit settings	ches not detect or remove rootkits. Therefore you should run a manual check		
Statistics Last scen: 22.10.08, 12:00 Last update: 22.10.08, 11:59 Virus DB: 270.8.2/1739 AVG version: 8.0.206 Linewse surface: 1.2019	with this component to ensure Scan applications Scan DLL libraries Scan drivers	no existing rootkits are installed on your system. Quick rootkit scan Full rootkit scan		
Show notification	Search for rootkits	Save changes Cancel		

The **Anti-Rootkit** user interface provides a brief description of the component's functionality, informs on the component's current status (*Anti-Rootkit component is active.*) and also brings information on the last time the **Anti-Rootkit** test was



launched.

In the bottom part of the dialog you can find the *Anti-Rootkit settings* section where you can set up some elementary functions of the rootkit presence scanning. First, mark up the respective check-boxes to specify objects that should be scanned:

- Scan applications
- Scan DLL libraries
- Scan drivers

Further you can pick the rootkit scanning mode:

- **Quick rootkit scan** scans only the system folder (*typically c:\Windows*)
- *Full rootkit scan* scans all accessible disks except for A: and B:

Control buttons available:

- Search for rootkits since the rootkit scan is not an implicit part of the Scan of the whole computer, you can run the rootkit scan directly from the Anti-Rootkit interface using this button
- Save changes press this button to save all changes made in this interface and to return to the default <u>AVG user interface</u> (components overview)
- Cancel press this button to return to the default <u>AVG user interface</u> (components overview) without having saved any changes you made

10.5.System Tools

System Tools refer to tools offering a detailed summary of the **AVG 8.5 Internet Security** environment. The component displays an overview of running processes, applications launched at operating system start up, active network connections, etc. Specific overviews can also be edited but this is only recommended for highly experienced users!



10.5.1.Processes

🖥 AVG Internet Security							
ile Components History Tools H	ielp	re protected					
Internet Security	All secu	rity features are working o	orrectly and are up to	date.			
-	Processes Network O	Connections Autostart Brow	vser Extensions LSP Viev	ver			
Dverview	Process name	Process path	Window	Internet	Service	PID	~
📃 💽 System Tools	Talo.exe	C:\WINDOWS\system		Yes	Yes	2512	
	avgam.exe	C:\PROGRA~1\AVG\A		Yes	No	328	
Computer scanner	avgcsrvx.exe	C:\Program Files\AVG\		No	No	3712	-
	avgcsrvx.exe	C:\Program Files\AVG\		No	No	2720	-
Update now	avgcsrvx.exe	C:\Program Files\AVG\		No	No	464	
	avgfws8.exe	C:\PROGRA~1\AVG\A		Yes	Yes	356	
	avgnsx.exe	C:\PROGRA~1\AVG\A		Yes	No	400	
	avgrsx.exe	C:\Program Files\AVG\		No	No	392	
	avgsystx.exe	C:\PROGRA~1\AVG\A		Yes	No	796	
	🛃 avgtray.exe	C:\PROGRA~1\AVG\A		Yes	No	2152	
	🛃 avgui.exe	C:\Program Files\AVG\	AVG Internet Security	Yes	No	3136	
Statistics	avgwdsvc.exe	C:\PROGRA~1\AVG\A		Yes	Yes	1800	
2210.00 12:00	csrss.exe	C:\WINDOWS\system		No	No	1320	V
Last update: 22.10.06, 11:59 Virus DB: 270.8,2/1739 AVG version: 8.0.206 License expires: 1.1.2018			e) Termi	nate Proce Back	:\$\$	
Show notification							

The **Processes** dialog contains a list of processes (*i.e. running applications*) that are currently active on your computer. The list is divided into several columns:

- Process name name of the running process
- Path physical path to the running process
- Window if applicable, indicates application Window name
- **Internet** indicates if the running process also connects to the Internet (Yes/No)
- **Service** shows if the running process is a service (*Yes/No*)
- **PID** process identification number is a unique Windows internal process identifier

You can select one or more applications and then terminate them by pressing the **Terminate Process** button. The **Back** button switches you back to the default <u>AVG</u> <u>user interface</u> (components overview).

We strongly suggest not to terminate any applications, unless you are absolutely sure that they represent a real threat!



🖥 AVG Internet Security					_	
ile Components History Tools H	elp					
AVG Internet Security	You are All security	protect	ed. are working correctly a	and are up to date.		
	Processes Network Cor	nections	Autostart Browser Exte	nsions LSP Viewer		
Overview						
	Application	Protocol	Local Address	Remote Address	State	^
📃 💽 System Tools	[System Process]	TCP	192.168.80.1:139	klarak.dev.grisoft.cz	Listening	
O contractor	[System Process]	TCP	klarak.dev.grisoft.cz	klarak.dev.grisoft.cz	Listening	=
Computer scanner	System Process]	TCP	klarak.dev.grisoft.cz	everest.dev.grisoft	Connected	
	System Process]	TCP	192.168.70.1:139	klarak.dev.grisoft.cz	Listening	
Update now	[System Process]	TCP	klarak.dev.grisoft.cz	medea2.app.grisoft	Connected	
	[System Process]	UDP	klarak.dev.grisoft.cz			
	[System Process]	UDP	192.168.80.1:137			
	[System Process]	UDP	klarak.dev.grisoft.cz			
	[System Process]	UDP	192.168.70.1:137			
	[System Process]	UDP	192.168.80.1:138			
	[System Process]	UDP	klarak.dev.grisoft.cz			
Statistics	[System Process]	UDP	192.168.70.1:138			
	alg.exe	TCP	localhost:1053	klarak.dev.grisoft.cz	Listening	~
Last scan: 22.10.06,12:00 Last update: 22.10.08,11:59 Virus DB: 270.8.2/1739 AVG version: 8.0.206 License expires: 1.1.2018	Hide local connections		🕈 Terminate connecti	on 🕅 Term	inate Process	
					Back	

10.5.2.Network Connections

The **Network Connections** dialog contains a list of currently active connections. The list is divided into the following columns:

- **Application** name of the application related to the connection. This information is only available on Windows XP.
- **Protocol** transmission protocol type used for the connection:
 - $_{\odot}$ TCP protocol used in conjunction with Internet Protocol (IP) to transmit information over the Internet
 - UDP alternative to TCP protocol
- Local address IP address of the local computer and the port number used
- **Remote address** IP address of the remote computer and the port number connected to. If possible, it will also look up the host name of the remote computer.
- **State** indicates the most probable current state (*Connected, Server should close, Listen, Active close finished, Passive close, Active close*)



To list only external connections, tick the *Hide local connections* checkbox.

The control buttons available are:

- Terminate Connection closes one or more connections selected in the list
- **Terminate Process** closes one or more applications related to connections selected in the list (*this button is only available on systems running Windows XP*)
- Back switch back to the default <u>AVG user interface</u> (components overview).

Sometimes it is possible to terminate only applications that are currently in the connected state. We strongly suggest not to terminate any connections, unless you are absolutely sure that they represent a real threat!

10.5.3.Autostart

🔰 I	🖌 AVG Internet Security 📃 🗖 🔯									
File	Components	History	Tools	Help						
	AVC Inter	G net Sec	urity			You are protec All security feature	ted. s are work	ing correctly and are	e up to dat	e.
					Processes	Network Connections	Autostart	Browser Extensions	LSP Viewer	
	🚺 Overvie	w			Name		Location		Path	
	System	Tools			Soundly	ια y	IDEGISTR'		"C:\Prog	ram Files) Analog Device
					B VMware	a batrav	IREGISTR'	VIMACHINE(SOFTW	"C:\Prog	ram Files) VMware) VMw
	Computer scanner					BEGISTRY MACHINE'SOFTW		C:\Progr	am Files\Analog Device	
					Shell		\REGISTR'	YMACHINE SOFTW	Explorer.	exe
	Vpdate	now			NvCplD	aemon	\REGISTR'	YMACHINE\SOFTW	RUNDLLS	2.EXE C:\WINDOWS\system32\r
					AVG8_1	TRAY	\REGISTR'	Y\MACHINE\SOFTW	C:\PROG	RA~1\AVG\AVG8\avgtr
					SC:\WIN	DOWS\system32\ms	\REGISTR'	Y\MACHINE\SOFTW	C:\WIND	OWS\system32\mshta
					🔊 ICQ		\REGISTR'	Y\USER\S-1-5-21-18	"C:\Prog	ram Files\ICQ6\ICQ.ex
					🔊 IETI		\REGISTR	Y\USER\.DEFAULT\S	C:\Progr-	am Files\Skype\Phone\I
					🔊 SHELL		\INI\syste	m.ini\BOOT\SHELL	SYS:Micro	osoft\Windows NT\Curr
					📝 ctfmon.	exe	\REGISTR'	Y\USER\S-1-5-21-18	C:\WIND	OWS\system32\ctfmon
S	tatistics				👏 Skype		\REGISTR'	Y\USER\S-1-5-21-18	"C:\Prog	ram Files\Skype\Phone\
	astecan: 22	10.08.12			👏 AppInit	_DLLs	\REGISTR'	Y\MACHINE\SOFTW	avgrsstx	.dl
La Vi A) Li	ast update: 22. rus DB: 270 /G version: 8.0. cense expires: 1	10.08, 11).8.2/173 .206 .1.2018	:59 9						۲	Remove selected Back
	∛ Show no	tificatio	n							

The **Autostart** dialog shows a list of all applications that are executed during Windows system start-up. Very often, several malware applications add themselves automatically to the start-up registry entry.

You can delete one or more entries by selecting them and pressing the *Remove*



selected button. The *Back* button switches you back to the default <u>AVG user</u> interface (components overview).

We strongly suggest not to delete any applications from the list, unless you are absolutely sure that they represent a real threat!

10.5.4.Browser Extensions

🛃 AVG Internet Security			_ 🗆 🔀		
File Components History Tools H	elp				
AVG All security features are working correctly and are up to date.					
	Processes Network Connection	Autostart Browser Extensions LSP Vie	wer		
🚺 Overview					
🛃 System Tools	AcroIEToolbarHelper Class	Type: Browser Helper Object	<u>^</u>		
Q Computer scanner	Skype add-on (button) SSVHelper Class	Other Extension Browser Helper Object			
📝 Update now	XTTBPos00 Class	Browser Helper Object Browser Helper Object	~		
Statistics Last scen: 22.10.08, 12:00 Last update: 22.10.08, 11:59 Virus DB: 270.8.2/1739 AVG version: 8.0.206 License expires: 1.1.2018	Name: XTTEPos0 Type: Browser I Type Description: Browser I Internal name: IE Toolba Description: IE Toolba Company: IE Toolba Copyright Copyright File name: Colbard Version: 2, 0, 20, Product Version: 2, 0, 20, Product Version: 2, 0, 20, CLSID: (055FD)	0 Class lelper Object lelper Objects are invisible components which 2001-2003. All rights reserved. # # Av1/LCQTOO-1(toolbaru.dll 11 11 XTTBPos00.1 %D-3A88-4e15-963D-DC8493744B1D)	Remove selected object		
Show notification			DIGUK		

The **Browser Extensions** dialog contains a list of plug-ins (*i.e. applications*) that are installed inside your Internet browser. This list may contain regular application plug-ins as well as potential malware programs. Click on an object in the list to obtain more information (*in the bottom section of the dialog*).

We strongly suggest not to delete any plug-ins from the list, unless you are absolutely sure that they represent a real threat!

The **Back** button switches you back to the default <u>**AVG** user interface</u> (components overview).



10.5.5.LSP Viewer

File Components History Tools H	elp	
AVG	You are protected. All security features are working correctly and are up to date.	
	Processes Network Connections Autostart Browser Extensions LSP Viewer	
Dverview		
System Tools	ID LSP 1001 MSAFD Tcoip [TCP/IP]	<u>^</u>
Q Computer scanner	1002 MSAFD Tcpip [UDP/IP] 1003 MSAFD Tcpip [RAW/IP] 1004 RSPU DD Service Provider	
📝 Update now	1005 RSVP TCP Service Provider	×
Statistics Last scan: 22.10.08, 12:00 Last update: 22.10.08, 11:59 Virus DB: 2708.2/1739 AVG version: 8.0.206 License expires: 1.1.2018 ▼ Show notification	Hide Windows LSP Name: MSAFD Tcpip [TCP/IP] Tetalog Di: 1001 File path: C:/WINDOWS\system32\nswsock.dll File name: mswsock.dll Wersion: 5.1.2600.3394 (rspsp.sp2_gdr.080620-1245). Copyright: @ Microsoft Corporation. All rights reserved. Product version: 5.1.2600.3394 Tetranal name: mswsock.dll File Description: Microsoft Corporation. All rights reserved. Remarks: Microsoft Windows Sockets 2.0 Service Provider.	

The *LSP Viewer* dialog shows a list of Layered Service Providers (LSP).

A **Layered Service Provider** (LSP) is a system driver linked into the networking services of the Windows operating system. It has access to all data entering and leaving the computer, including the ability to modify this data. Some LSPs are necessary to allow Windows to connect you to other computers, including the Internet. However, certain malware applications may also install themselves as an LSP, thus having access to all data your computer transmits. Therefore, this review may help you to check all possible LSP threats.

Under certain circumstances, it is also possible to repair broken LSPs (*for example when the file has been removed but the registry entries remain untouched*). A new button for fixing the issue is displayed once a repairable LSP is discovered.

To include Windows LSP in the list, uncheck the **Hide Windows LSP** checkbox. The **Back** button switches you back to the default <u>AVG user interface</u> (components overview).



10.6.Firewall

10.6.1.Firewall Principles

Firewall is a system that enforces an access control policy between two or more networks by blocking/permitting traffic. Firewall contains a set of rules that protect the internal network from attacks originating outside (typically from the Internet) and controls all communication on every single network port. The communication is evaluated according to the defined rules, and then either allowed or forbidden. If Firewall recognizes any intrusion attempts, it "blocks" the attempt and does not allow the intruder access to the computer.

Firewall is configured to allow or deny internal/external communication (both ways, in or out) through defined ports, and for defined software applications. For example, the firewall could be configured to only permit web data to flow in and out using Microsoft Explorer. Any attempt to transmit web data by any other browser would be blocked.

Firewall protects your personally-identifiable information from being sent from your computer without your permission. It controls how your computer exchanges data with other computers on the Internet or local network. Within an organization, the firewall also protects the single computer from attacks initiated by internal users on other computers in the network.

Note: AVG Firewall is not intended for server platforms!

How does AVG Firewall work

In AVG, the *Firewall* component controls all traffic on every network port of your computer. Based on the defined rules, the *Firewall* evaluates applications that are either running on your computer (and want to connect to the Internet/local network), or applications that approach your computer from outside trying to connect to your PC. For each of these applications the *Firewall* then either allows or forbids the communication on the network ports. By default, if the application is unknown (i.e. has no defined *Firewall* rules), the *Firewall* will ask you if you wish to allow or block the communication attempt.

What the Firewall can do:

 Allow or block communication attempts of known <u>applications</u> automatically, or ask you for confirmation



- Use complete profiles with predefined rules, according to your needs
 - Keep an archive of all defined profiles and settings
 - <u>Switch profiles</u> automatically when connecting to various networks, or using various network adapters

10.6.2. Firewall Profiles

The *Firewall* allows you to define specific security rules based on whether your computer is located in a domain, or it is a standalone computer, or even a notebook. Each of these options requires a different level of protection, and the levels are covered by the respective profiles. In short, a *Firewall* profile is a specific configuration of *Firewall* component, and you can use a number of such predefined configurations.

Available profiles

- **Allow all** a <u>Firewall</u> system profile that has been pre-set by the manufacturer and is always present. When this profile is activated, all network communication is allowed and no safety policy rules are applied, as if the <u>Firewall</u> protection was switched off (*i.e. all applications are allowed but packets are still being checked to completely disable any filtering you need to disable Firewall*). This system profile cannot be duplicated, deleted, and its settings cannot be modified.
- **Block all** a <u>Firewall</u> system profile that has been pre-set by the manufacturer and is always present. When this profile is activated, all network communication is blocked, and the computer is neither accessible from outer networks, nor can communicate outside. This system profile cannot be duplicated, deleted, and its settings cannot be modified.
- Custom profiles profiles generated through the <u>Firewall Configuration</u> <u>Wizard</u>. The maximum of three custom profiles can be generated through the Wizard:
 - Standalone computer suitable for common desktop home computers connected directly to the Internet.
 - Computer in domain suitable for computers in a local network, e.g. school or corporate network. It is assumed that the network is protected by some additional measures so that the security level can be lower than for a standalone computer.



- Small home or office network suitable for computers in a small network, e.g. at home or in a small business, typically only several computers connected together, without a "central" administrator.
- Computer on the move suitable for notebooks. It is supposed that, as a handheld travel computer, it connects to the Internet from various unknown and therefore totally insecure places (Internet café, hotel room etc.), and the highest security level is set.

Profile switching

The profile switching feature allows the *Firewall* to switch automatically to the defined profile when using a certain network adapter, or when connected to a certain type of network. If no profile has been assigned to a network area yet, then upon next connection to that area, the *Firewall* will display a dialog asking you to assign a profile.

You can assign profiles to all local network interfaces or areas and specify further settings in the <u>Areas and Adapters Profiles</u> dialog, where you can also disable the feature if you do not wish to use it (*then, for any kind of connection, the default profile will be used*).

Typically, users who have a notebook and use various types of connection will find this feature useful. If you have a desktop computer, and only ever use one type of connection (*e.g. cable connection to the Internet*), you do not have to bother with profile switching as most likely you will never use it.



10.6.3. Firewall Interface

File Components History Tools He	elp				
AVG Internet Security	You are protected. All security features are working of	correctly and are up to date.			
	Firewall Component				
🚺 Overview					
	Firewall defines rules that prote Internet, and control (allow/forbi	ect your computer from outside attacks, typically from the d) all communication on every network port. If Firewall			
E Firewall	recognizes an intrusion attempt,	it blocks it immediately and does not let the intruder access			
Q Computer scanner	to your PC.				
📝 Update now	Firewall is active and fully functional. You are protected against threats from external networks.				
	Firewall has been enabled for:	1 day(s) 20 hour(s) 55 minute(s) 32 second(s)			
	Blocked packets:	57440			
	Overall packets:	497669			
	For more detailed settings please select Tools / Fire	wall settings from the system menu.			
Statistics	Firowall optimes				
Last scan: 22.10.08.12:00	Colort Security				
Last update: 23.10.08, 9:47	Select Firewaii profile:	Firewall enabled			
Virus DB: 270.8.2/1740	Computer in domain 💌	Firewall disabled			
AVG version: 8.0.206	Enable gaming mode	Cimergency mode (block all Internet trarric)			
License expires: 1.1.2016					
Show polification	Configuration Wizard	The save changes Lancel			
· onen notification	1				

The *Firewall* component's interface provides some basic information on the component's functionality, and a brief overview of *Firewall* statistics:

- Firewall has been enabled for time elapsed since Firewall was last launched
- Blocked packets number of blocked packets from the entire amount of packets checked
- **Overall packets** number of all packets checked during the Firewall run

Firewall settings section

- Select Firewall profile from the roll-down menu select one of the defined profiles two profiles are available at all times (the *default profiles named* Allow all and Block all), other profiles were added as you went through the <u>Firewall Configuration Wizard</u> or by profile editing in the <u>Profiles</u> dialog in <u>Firewall Settings</u>.
- Firewall status:
 - Firewall enabled select this option to allow communication to those applications that are assigned as 'allowed' in the set of rules defined



within selected *Firewall* profile

- *Firewall disabled* this option switches *Firewall* off completely, all network traffic is allowed but not checked!
- *Emergency mode (block all internet traffic)* select this option to block all traffic on every single network port; *Firewall* is still running but all network traffic is stopped
- **Enable gaming mode** Check this option to ensure that when running full-screen applications (games, PowerPoint presentations etc.), the <u>Firewall</u> will not display dialogs asking you whether you want to allow or block communication for unknown applications. In case an unknown application tries to communicate over the network at that time, the <u>Firewall</u> will allow or block the attempt automatically according to settings in the current profile.

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change Firewall configuration, select the system menu item **File / Firewall settings** and edit the Firewall configuration in the newly opened **Firewall Settings** dialog.

Control buttons available are:

- <u>Configuration wizard</u> press the button to launch the <u>Firewall</u> <u>configuration wizard</u> that will lead you step by step through the <u>Firewall</u> component configuration
- **Save changes** press this button to save and apply any changes made in this dialog
- **Cancel** press this button to return to the default <u>AVG user interface</u> (*components overview*)

10.7.E-mail Scanner

10.7.1.E-mail Scanner Principles

One of the most common sources of viruses and trojans is via e-mail. Phishing and spam make e-mail an even greater source of risks. Free e-mail accounts are more likely to receive such malicious e-mails (as they rarely employ anti-spam technology), and home users rely quite heavily on such e-mail. Also home users, surfing unknown



sites and filling in online forms with personal data (such as their e-mail address) increase exposure to attacks via e-mail. Companies usually use corporate e-mail accounts and employ anti-spam filters etc, to reduce the risk.

The *E-mail Scanner* component checks every e-mail sent or received, providing much needed protection from e-mail borne threats. AVG supports all leading e-mail clients including MS Outlook, The bat!, Eudora and all other SMTP/POP3 based email clients such as Outlook Express. Encrypted connections using SSL are also supported.

Note: AVG E-mail Scanner is not intended for server platforms!

When detected, viruses are quarantined in <u>Virus Vault</u> immediately. Some e-mail clients may support messages with text certifying that sent and received e-mail has been scanned for viruses.

10.7.2.E-mail Scanner Interface



In the *E-mail Scanner* component's dialog you can find a brief text describing the component's functionality, information on its current status (*E-mail Scanner is active.*), and the following statistics:

• **Total e-mails scanned** - how many e-mail messages were scanned since the **E-mail Scanner** was last launched (*if needed, this value can be reset; e. g. for statistic purposes - Reset value*)



- Threats found and blocked provides the number of infections detected in e-mail messages since the last *E-mail Scanner* launch
 - **Installed e-mail protection** information about a specific e-mail protection plug-in referring to your default installed e-mail client

Basic component configuration

In the bottom part of the dialog you can find the section named *E-mail Scanner settings* where you can edit some elementary features of the component's functionality:

- **Scan incoming messages** check the item to specify that all e-mails delivered to your account should be scanned for viruses (*by default, this item is on, and it is recommended not to change this setting!*)
- **Scan outgoing messages** check the item to confirm all e-mail sent from your account should be scanned for viruses (*by default, this item is off*)
- **Display notification icon while E-mail is being scanned** during the scanning the <u>E-mail Scanner</u> component displays a notification dialog informing on an actual task the component is processing (*connecting to server, downloading a message, scanning the message, ...*)

The advanced configuration of the *E-mail Scanner* component is accessible via the *File/Advanced settings* item of the system menu; however advanced configuration is recommended for experienced users only!

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.

Control buttons

The control buttons available within the *E-mail Scanner* interface are as follows:

• **Save changes** - press this button to save and apply any changes made in this dialog



 Cancel - press this button to return to the default <u>AVG user interface</u> (components overview)

10.7.3.E-mail Scanner Detection

🖥 AVG Internet Security				
File Components History Tools	Help			
AVG Internet Security	You are protected. All security features are w	orking correctly	and are up to date.	
Overview	E-mail Scanner detection	Object	Result	Detection tin 🔨
Q Computer scapper	🗱 Virus identified EICAR_Test	eicar.com	Infected	7.5.2008, 15
Update now	Virus identified EICAR_Test	eicar.com eicar.com	Infected Infected	7.5.2008, 15
Statistics Last scan: 8.5.08, 11:10 Last update: 9.5.08, 10:52 Virus DB: 269.23.11/1422 AVG version: 8.0.103 License expires: 1.1.2018	Virus identified EICAR_Test Virus identified EICAR_Test Potentially harmful program Dialer.GSV Virus identified EICAR_Test Virus identified EICAR_Test There are 65 records in the list Additional actions: Export list to file, Empty list Refresh list	eicar.com eicar.com spyware.ex_ eicar.com spyware.ex_ eicar.com spyware.ex_ eicar.com spyware.ex_ eicar.com	Infected Infected Potentially dangerous object Infected Potentially dangerous object Infected Potentially dangerous object Infected	7.5.2008, 14 30.4.2008, 9 30.4.2008, 9
Show notification	nenesmist			DOUR

In the *E-mail Scanner detection* dialog (*accessible via system menu option History / E-mail Scanner detection*) you will be able to see a list of all findings detected by the *E-mail Scanner* component. For each detected object the following information is provided:

- Infection description (possibly even name) of the detected object
- Object object location
- Result action performed with the detected object
- Object Type type of the detected object

In the bottom part of the dialog, under the list, you will find information on total number of detected objects listed above. Further you can export the entire list of detected objects in a file (*Export list to file*) and delete all entries on detected objects (*Empty list*).



10.8.License

🛃 AVG Internet Security			
File Components History Tools He	alp		
AVG Internet Security	You are protected. All security features are working correctly and are up to date.		
Overview License Computer scanner	License Component The License Component manages your current license status. Your license number determines the specific version of AVG you have. Please make sure that you enter and activate your license correctly, otherwise your software will not get updated properly and we will not be able to provide you with technical support.		
🕼 Update now	License component is active. The installed product is AVG Internet Security.		
	License number: XXX-XXXXX-XXXXX-XXXXX-XXXXX License type: Full License expires: 1. ledna 2018 Number of seats: 1		
Statistics Last scan: 22:10.08, 12:00 Last update: 23:10.08, 9:47 Virus DB: 270.8.2/1740 AVG version: 8.0.206	License actions		
License expires: 1.1.2018	Buy now Re-activate Register Back		

In the *Licence* component interface you will find a brief text describing the component's functionality, information on its current status (*License component is active.*), and the following information:

- License number provides the exact form of your license number. When entering your license number, you have to be absolutely precise and type it exactly as shown. For your comfort, the License dialog offers the Copy license number button: press the button to copy the license number into the clipboard, and then you can simply paste it anywhere you like (CTRL+V).
- License type specifies the product edition defined by your license number.
- **License expires** this date determines the period of validity of your license. If you want to go on using AVG after this date you have to renew your license. The <u>license renewal can be performed online</u> on the AVG website.
- **Number of seats** how many workstations on which you are entitled to install your AVG.



Control buttons

- **Copy license number** press the button to insert the currently used license number into clipboard (*just like with CTRL+C*), and you can paste it wherever needed
- **Re-activate** opens the **Activate AVG** dialog with the data you have entered in the <u>Personalize AVG</u> dialog of the <u>installation process</u>. Within this dialog you can enter your license number to either replace the sales number (*the number you have installed AVG with*), or to replace the old license number (*e. g. when upgrading to a new AVG product*).
- **Register** connects to the registration website at <u>www.avg.com</u>. Please fill in your registration data; only customers who register their AVG product can receive free technical support.
- **Back** press this button to return to the default <u>AVG user interface</u> (components overview)

10.9.Link Scanner

10.9.1.Link Scanner Principles

LinkScanner consists of two features: <u>AVG Active Surf-Shield</u> and <u>AVG Search</u> <u>Shield</u>.

<u>AVG Active Surf-Shield</u> prevents you from accidentally becoming infected by driveby downloads and other exploits, ensuring the web pages you visit are safe at the only time that really matters - when you are about to click the link.

<u>AVG Search Shield</u> works with Google, Yahoo! and MSN search engines to deliver a real-time safety verdict on all search results, including search ads, displaying an icon to show the safety rating for each site.

Note: AVG Link Scanner is not intended for server platforms!



10.9.2.Link Scanner Interface

The *LinkScanner* component consists of two parts that you can switch on/off in the *LinkScanner component* interface:



- **Enable** <u>AVG Search-Shield</u> (on by default): advisory notifying icons on searches performed in Google, Yahoo or MSN having checked ahead the content of sites returned by the search engine.
- **Enable** <u>AVG Active Surf-Shield</u> (on by default): active (real-time) protection against exploitive sites as they are accessed. Known malicious site connections and their exploitive content is blocked as they are accessed by the user via a web browser (or any other application that uses HTTP).
- Back reporting of exploiting web sites mark this item to allow back reporting of exploits and bad sites found by users either via Safe Surf or Safe Search to feed the database collecting information on malicious activity on the web.

10.9.3.AVG Search-Shield

When searching Internet with the **AVG Search-Shield** on, all search results returned from the most popular search engines like Yahoo!, Google, MSN, etc. are evaluated for dangerous or suspicious links. By checking these links and marking the bad links, the <u>AVG Security Toolbar</u> warns you before you click on dangerous or suspicious



links, so you can ensure you only go to safe websites.

While a link is being evaluated on the search results page, you will see a graphic sign next to the link informing that the link verification is in progress. When the evaluation is complete, the respective informative icon will be displayed:

The linked page is safe (with Yahoo! search engine within <u>AVG Security</u> <u>Toolbar</u> this icon will not be displayed!).

The linked page does not contain threats but is somewhat suspicious (questionable in origin or motive, therefore not recommended for e-shopping etc.).

The linked page can be either safe itself, but containing further links to positively dangerous pages; or suspicious in code, though not directly employing any threats at the moment.

The linked page contains active threats! For your own safety, you will not be allowed to visit this page.

The linked page is not accessible, and so could not be scanned.

Hovering over an individual rating icon will display details about the particular link in question. Information include additional details of the threat (if any), the IP address of the link and when the page was scanned by AVG:



10.9.4.AVG Active Surf-Shield

This powerful protection will block malicious content of any webpage you try to open, and prevent it from being downloaded to your computer. With this feature enabled, clicking a link or typing in a URL to a dangerous site will automatically block you from opening the web page thus protecting you from inadvertently being infected. It is important to remember that exploited web pages can infect your computer simply by visiting the affected site, for this reason when you request a dangerous webpage



containing exploits or other serious threats, the <u>AVG Security Toolbar</u> will not allow your browser to display it.

If you do encounter a malicious web site, within your web browser the <u>AVG Security</u> <u>Toolbar</u> will warn you with a screen similar to:

MAVG
Danger: AVG Safe Search & Surf hat detected active threats on this page and has blocked access for your protection.
Risk Category: Exploit server
Explanation: The IP address of this web page belongs to a known malicious site. This is either not the true address of the URL you just clicked on or it is referenced, either intentionally or or unintentionally, by the site you were attempting to visit. AVG Safe Seach and Surf has prevented access to this IP address and its malicious content.
IP Adress: 66.xx.xxx.99
For additional information <u>click here</u>
Suggestions: Click the "Back" button on your browser to return to the previous page and choose another link (recommended) If you would like to ignore the warning and continue to the page, <u>click here</u> (not recommended)

If you still wish to visit the infected page, a link to the page is available on this screen, *but continuing to these pages in not recommended!*

10.1(Web Shield

10.10.1Web Shield Principles

Web Shield is a type of a real time resident protection; it scans the content of visited web pages (and possible files included in them) even before these are displayed in your web browser or downloaded to your computer.

Web Shield detects that the page you are about to visit includes some dangerous javascript, and prevents the page from being displayed. Also, it recognizes malware contained in a page and stops its downloading immediately so that it never gets to your computer.

Note: AVG Web Shield is not intended for server platforms!

10.10.2 Web Shield Interface

The **Web Shield** component's interface describes the behavior of this type of protection. Further you can find information on the component's current status (*Web Shield is active and fully functional.*). In the bottom part of the dialog you will then find the elementary editing options of this component's functionality.


Basic component configuration

First of all, you have the option to immediately switch on/off the **Web Shield** by checking the **Enable Web Shield** item. This option is enabled by default, and the **Web Shield** component is active. However, if you do not have a good reason to change this settings, we recommend to keep the component active. If the item is checked, and the **Web Shield** is running, more configuration options are available and editable on two tabs:

• **Web** - you can edit the component's configuration regarding the scan of the website content. The editing interface allows you to configure the following elementary options:

🕌 AVG Internet Security	
File Components History Tools H	elp
AVG Internet Security	You are protected. All security features are working correctly and are up to date.
Overview Image: Web Shield Image: Computer scanner	Web Shield Component Web Shield protects you against accidentally downloading infected files or exchanging infected files over instant messaging.
📝 Update now	🕼 Web Shield is active and fully functional.
	Web Shield
Statistics Last scar: 2310.08, 23:00 Last update: 24.10.08, 9.47 Virus DB: 270.8.2/1742 AVG version: 8.0.206 License expires: 1.1.2018	Basic web settings ✓ Web protection □ Check archives ✓ Scan Potentially Unwanted Programs and Spyware threats ✓ Use heuristic analysis Maximum part size of a file to be scanned 200 KB Save changes Cancel

- Web protection this option confirms that the Web Shield should perform scanning of the www pages content. Provided this option is on (by default), you can further switch on/off these items:
 - Check archives scan the content of archives possibly included in the www page to be displayed
 - Scan Potentially Unwanted Programs scan potentially unwanted programs (executable programs that can operate as spyware or adware) included in the www page to be displayed



Use heuristic analysis - scan the content of the page to be displayed using the heuristic analysis method (dynamic emulation of the scanned object's instructions in a virtual computer environment see chapter Anti-Virus Principles)

- Maximum file size to be scanned if included files are present in the displayed page you can also scan their content even before these are downloaded to your computer. However, scanning of large files takes quite some time and the web page download might be slowed significantly. You can use the slide bar to specify the maximum size of a file that is still to be scanned with **Web Shield**. Even if the downloaded file is bigger than specified, and therefore will not be scanned with **Web Shield**, you are still protected: in case the file is infected, the <u>Resident Shield</u> will detect it immediately.
- **Instant Messaging** allows you to edit the components settings referring to instant messaging (*e.g. ICQ, MSN Messenger, Yahoo ...*) scanning.



 Instant Messaging protection - check this item if you wish that the Web Shield verifies the on-line communication is virus free. Provided this option is on, you can further specify which instant messaging application you want to control - currently AVG 8.5 Internet Security supports the ICQ, MSN, and Yahoo applications.



Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.

Control buttons

The control buttons available within the **Web Shield** interface are as follows:

- Save changes press this button to save and apply any changes made in this dialog
- **Cancel** press this button to return to the default <u>AVG user interface</u> (*components overview*)

10.10.:Web Shield Detection

Web Shield scans the content of visited web pages and possible files included in them even before these are displayed in your web browser or downloaded to your computer. If a threat is detected, you will be warned immediately with the following dialog:



The suspect web page will not be opened, and the threat detection will be logged in the list of **Web Shield findings** (accessible via system menu History / Web Shield findings).



10.1 Resident Shield

10.11.:Resident Shield Principles

The **Resident Shield** scans files as they are copied, opened or saved. When the **Resident Shield** discovers a virus in a file that is accessed, it stops the operation currently being performed and does not allow the virus to activate itself. The **Resident Shield**, loaded in the memory of your computer during system startup, also provides vital protection for the system areas of your computer.

10.11. Resident Shield Interface



Besides an overview of the most important statistical data and the information on the component's current status (*Resident Shield is active and fully functional*), the **Resident Shield** interface offers some elementary component settings options, too. The statistics is as follows:

- Resident Shield has been active for provides the time since the latest component's launch
- **Threats detected and blocked** number of detected infections that were prevented from being run/opened (*if needed, this value can be reset; e.g. for statistic purposes Reset value*)



Basic component configuration

In the bottom part of the dialog window you will find the section called **Resident Shield settings** where you can edit some basic settings of the component's functionality (*detailed configuration, as with all other components, is available via the File/Advanced settings item of the system menu*).

The **Resident Shield is active** option allows you to easily switch on/off resident protection. By default, the function is on. With resident protection on you can further decide how the possibly detected infections should be treated (removed):

- o either automatically (*Remove all threats automatically*)
- o or only after the user's approval (*Ask me before removing threats*)

This choice has no impact on the security level, and it only reflects your preferences.

In both cases, you can still select whether you want to **Remove cookies automatically.** In specific cases you can switch this option on to achieve maximum security levels, however it is switched off by default. (*cookies = parcels of text sent by a server to a web browser and then sent back unchanged by the browser each time it accesses that server. HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*).

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.

Control buttons

The control buttons available within the **Resident Shield** interface are as follows:

- Manage exceptions opens the <u>Resident Shield Directory Excludes</u> dialog where you can define folders that should be left out from the <u>Resident</u> <u>Shield</u> scanning
- Save changes press this button to save and apply any changes made in this dialog



 Cancel - press this button to return to the default <u>AVG user interface</u> (components overview)

10.11.:Resident Shield Detection

Resident Shield scans files as they are copied, opened or saved. When a virus or any kind of threat is detected, you will be warned immediately via the following dialog:

🕌 Resident 🤅	Shield alert	$\overline{\mathbf{X}}$
Accessed F	ile is infected	
	threat d	etected!
	File name:	C:\KLARA\eicar.com
	threat name:	Virus identified EICAR_Test
		Detected on open.
		More information about this threat
Re	move threat as Pou	wer User
0	_ <u>H</u> eal	Move to Vault Ignore
Show (details	

The dialog provides information on the threat detected, and it invites you to decide what action should be taken now:

- *Heal* if a cure is available, AVG will heal the infected file automatically; this option is the recommended action to be taken
- Move to Vault the virus will be moved to AVG Virus Vault
- **Ignore** we strictly recommend NOT TO use this option unless you have a very good reason to do so!



AVG Internet Security File Components History Tools He	elp You are pro All security fea	tected. tures are working corre	ctly and are up to date	
Overview Computer scanner Update now	Resident Shield de Infection	tection Object C:\KLARA\eicar.com	Result Moved to Virus Vault	Detection time C 23.10.2008, 11:16:10 Fi
Statistics Last scan: 22.10.08, 12:00 Last update: 23.10.08, 9.47 Virus DB: 270.8.2/1740 AVG version: 8.0.206 License expires: 1.1.2018 Image: Show notification 20.8.2/10	There are 1 records in the list Additional actions: Export list to Refresh list	III file, Empty list		Back

The **Resident Shield detection** offers an overview of objects that were detected by the **<u>Resident Shield</u>**, evaluated as dangerous and either cured or moved to the **<u>Virus Vault</u>**. For each detected object the following information is provided:

- Infection description (possibly even name) of the detected object
- **Object** object location
- Result action performed with the detected object
- **Object Type** type of the detected object
- **Process** what action was performed to call out the potentially dangerous object so that it could be detected

In the bottom part of the dialog, under the list, you will find information on total number of detected objects listed above. Further you can export the entire list of detected objects in a file (*Export list to file*) and delete all entries on detected objects (*Empty list*). The *Refresh list* button will update the list of finding detected by *Resident Shield*. The *Back* button switches you back to the default <u>AVG user interface</u> (components overview).



10.1:Update Manager

10.12. Update Manager Principles

No security software can guarantee true protection from various types of threats unless it is regularly updated! Virus writers are always looking for new flaws that they can exploit in both software and operating systems. New viruses, new malware, new hacking attacks appear daily. For this reason, software vendors are continually issuing updates and security patches, to fix any security holes that are discovered.

It is crucial to update your AVG regularly!

The **Update Manager** helps you to control regular updating. Within this component you can schedule automatic downloads of update files either from the Internet, or the local network. Essential virus definition updates should be daily if possible. Less urgent program updates can be weekly.

Note: Please pay attention to the <u>AVG Updates</u> chapter for more information on update types and levels!

aVG Internet Security		
File Components History Tools H	elp	
AVG Internet Security	You are protected. All security features are working	g correctly and are up to date.
	Update Manager Component	
Overview Overview	Update Manager manages make sure you always get the update schedule that checks fr i.e. at least once a day. Updat protection against viruses.	automatic AVG updates from the Internet or a local network. To latest version of update files it is recommended to create an or critical updates directly from the Internet at regular intervals, ing your AVG is vital if you want to preserve maximum
📝 Update now	🛛 Update Manager component is active.	
	Latest update:	23. října 2008, 12:02
	Virus database version:	270.8.2/1741
	Next scheduled update:	23. října 2008, 15:59
	For more detailed settings please select Tools / A	dvanced settings from the system menu.
Statistics	Update Manager settings	
Last scan: 23.10.08, 12:00	Start automatic updates	
Last update: 23.10.08, 12:02	Periodically	At a specific time interval
Virus DB: 270.8.2/1741	Every 4 A Hour(s)	Every day
License expires: 1.1.2018		
Show notification	Update now	🕐 Save changes Cancel

10.12. Update Manager Interface

The Update Manager's interface displays information about the component's



functionality and its current status (*Update manager is active.*), and provides the relevant statistical data:

- Latest update specifies when and at what time the database was updated
- **Virus database version** defines the number of the latest virus database version; and this number increases with every virus base update

Basic component configuration

In the bottom part of the dialog you can find the **Update Manager settings** section where you can perform some changes to the rules of the update process launch. You can define whether you wish the update files to be downloaded automatically (**Start automatic updates**) or just on demand. By default, the **Start automatic updates** option is switched on and we recommend to keep it that way! Regular download of the latest update files is crucial for proper functionality of any security software!

Further you can define when the update should be launched:

- *Periodically* define the time interval
- At a specific time define the exact day and time

By default, the update is set for every 4 hours. It is highly recommended to keep this setting unless you have a true reason to change it!

Please note: The software vendor has set up all AVG components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change AVG configuration, select the system menu item **Tools / Advanced settings** and edit the AVG configuration in the newly opened <u>AVG</u> <u>Advanced Settings</u> dialog.

Control buttons

The control buttons available within the **Update Manager** interface are as follows:

- Update now launches an immediate update on demand
- **Save changes** press this button to save and apply any changes made in this dialog



 Cancel - press this button to return to the default <u>AVG user interface</u> (components overview)

10.1:AVG Security Toolbar

The **AVG Security Toolbar** is designed to work with **MS Internet Explorer** (version 6.0 or greater) and **Mozilla Firefox** (version 1.5 or greater).

Note: AVG Security Toolbar is not intended for server platforms!

Once installed the **AVG Security Toolbar** will by default be located just under your browsers address bar:

🛃 AVG 🔻 🛛 powered by 🏹 HOO!, SEARCH 💌 Search 🔶 🎒 Active Surf-Shield 🚳 Search-Shield 🖏 AVG Info 🔻

The **AVG Security Toolbar** consists of the following:

- AVG logo button provides access to general toolbar items. Click the logo button to get redirected to the AVG website (<u>www.avg.com</u>). Clicking the pointer next to the AVG icon will open the following:
 - Toolbar Info link to the AVG Security Toolbar home page with detailed information on the toolbar's protection
 - o Launch AVG 8.0 opens the AVG 8 user interface
 - Options opens a configuration dialog where you can adjust your AVG Security Toolbar settings to suit your needs; the dialog is divided into two tabs:
 - General on this tab you can find two sections named Buttons and Ratings.

The **Buttons** section allows you to configure which buttons are visible or hidden on the **AVG Security Toolbar**. By default all buttons are visible.

The **Ratings** section allows you to determine what type of ratings do you want to be displayed for your search results. By default all ratings are visible but you may hide some of them (*when searching from the Yahoo! search box, only safe results are displayed*).



Options		
General	Advanced	
Button	s	
Custon	nize which buttons are show	vn on AVG Toolbar:
🗹 Sur	f Safe	
🔽 Sea	arch Shield	
🗹 AVI	G Info	
Get	More!	
- Rating:	3	
Custon search	nize which type of ratings S results pages:	earch Shield will show on the
🗹 Saf	e (Green)	
🔽 Que	estionable (Yellow)	
🗹 Ris	ky (Orange)	
🔽 Uni	known (Gray)	Learn more
	ОК	Cancel

Advanced - on this tab you can edit the AVG Security Toolbar protection features. By default, both the <u>AVG Search-Shield</u> and <u>AVG Active Surf-Shield</u> features are enabled.

Options			×
General	Advanced		
Advan	ced options -		h
Select from th	the protectior e listed below	ns you would like to use within the Toolbar :	
	AVG Search-	Shield	
	AVG Active S	iurf-Shield	
<u>Learn r</u>	nore	OK Cancel	

- Update checks for new updates for your AVG Security Toolbar
- *Help* provides options to open the help file, contact <u>AVG technical</u> <u>support</u>, or view the details of the current version of the toolbar
- Yahoo! powered search box easy and safe way to search the web using



Yahoo! search. Enter a word or phrase into the search box press **Search** to start the search on the Yahoo! server directly, no matter what page is currently displayed. The search box also lists your search history. Searches done through the search box are analyzed using the <u>AVG Search-Shield</u> protection.

- AVG Active Surf-Shield button on/off button controls the status of the <u>AVG Active Surf-Shield</u> protection
- AVG Search-Shield button on/off button controls the status of the <u>AVG</u> <u>Search-Shield</u> protection
- AVG Info button provides links to important security information located on the AVG website (<u>www.avg.com</u>)



11. AVG Advanced Settings

The advanced configuration dialog of **AVG 8.5 Internet Security** opens in a new window named **Advanced AVG Settings**. The window is divided into two sections: the left part offers a tree-arranged navigation to the program configuration options. Select the component you want to change the configuration of (*or its specific part*) to open the editing dialog in the right-hand section of the window.

11.1.Appearance

The first item of the navigation tree, *Appearance*, refers to the general settings of the <u>AVG user interface</u> and a few elementary options of the application's behavior:

🕌 Advanced AVG Settings		- 🗆 🗙
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Schedules E-mail Scanner Resident Shield Anti-Rootkit Update	age selection tation must be restarted to apply language changes. t user interface language: ish n tray notifications splay system tray notifications Display tray notifications about update. Display tray notifications about scanning. Display Resident Shield related tray notifications (automatic action). Display Splay Firewall related tray notifications. Display Firewall related tray notifications. Display E-mail Scanner related tray notifications.	
Default	Cancel 😿 A	pply .:

Language selection

In the *Language selection* section you can chose your desired language from the drop-down menu; the language will then be used for the entire <u>AVG user interface</u>. The drop-down menu only offers those languages you have previously selected to be installed during the <u>installation process</u> (see chapter <u>Custom Installation - Component Selection</u>). However, to finish switching the application to another language you have



to restart the user interface; follow these steps:

- Select the desired language of the application and confirm your selection by pressing the *Apply* button (right-hand bottom corner)
- Press the **OK** button to close the **Advanced AVG Settings** editing dialog
- Close the <u>AVG user interface</u> via the <u>system menu</u> item option <u>File/Exit</u>
- Re-open the <u>AVG user interface</u> by one of these options: double-click the <u>AVG</u> system tray icon, double-click the AVG icon on your desktop, or via the menu **Start/All Programs/AVG 8.0/AVG User Interface** (see chapter <u>Access to</u> <u>User Interface</u>). The user interface will then be displayed in the newly selected language.

Balloon tray notifications

Within this section you can suppress display of system tray balloon notifications on the status of the application. By default, the balloon notifications are allowed to be displayed, and it is recommended to keep this configuration! The balloon notifications typically inform on some AVG component's status change, and you should pay attention to them!

However, if for some reason you decide you do not wish these notifications to be displayed, or you would like only certain notifications (related to a specific AVG component) to be displayed, you can define and specify your preferences by checking/unchecking the following options:

- **Display system tray notifications** by default, this item is checked (*switched on*), and notifications are displayed. Uncheck this item to completely turn off the display of all balloon notifications. When turned on, you can further select what specific notifications should be displayed:
 - Display tray notifications about <u>update</u> decide whether information regarding AVG update process launch, progress, and finalization should be displayed;
 - Display tray notifications about <u>scanning</u> decide whether information upon automatic launch of the scheduled scan, its progress and results should be displayed;
 - Display <u>Resident Shield</u> related tray notifications decide whether information regarding file saving, copying, and opening processes



should be displayed or suppressed;

- Display components state change notifications decide whether information regarding component's activity/inactivity or its possible problem should be displayed. When reporting a component's fault status, this option equals to the informative function of the system tray icon (color changing) reporting a problem in any AVG component.
- Display <u>Firewall</u> related tray notifications decide whether information concerning Firewall status and processes, e.g. component's activation/deactivation warnings, possible traffic blocking etc. should be displayed;
- Display <u>E-mail Scanner</u> related tray notifications decide whether information upon scanning of all incoming and outgoing e-mail messages should be displayed.

11.2.Ignore Faulty Conditions

In the *Ignore faulty components conditions* dialog you can tick those components that you do not want to get informed about:

🕌 Advanced AVG Settings		- 🗆 🛛
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Veb Shield LinkScanner Scans E-mail Scanner E-mail Scanner Resident Shield Anti-Rootkit Update	Ignore faulty components conditions Error or warning status of the selected components will be ignored. Component Anti-Rootkit Anti-Spam Anti-Spyware Anti-Virus E-mail Scanner Firewall License LinkScanner Resident Shield System Tools Update Manager Web Shield	
Default	🕐 OK Cancel 🕅	Apply



By default, no component is selected in this list. It means that if any component get to an error status, you will be informed about it immediately via:

- <u>system tray icon</u> while all parts of AVG are working properly, the icon is displayed in four colors; however, if an error occurs, the icon appears with a yellow exclamation mark,
- text description of the existing problem in the <u>Security Status Info</u> section of the AVG main window

There might be a situation that for some reason you need to switch a component off temporarily (*this is not recommended, you should try to keep all components permanently on and in default configuration, but it may be happen*). In that case the system tray icon automatically reports the component's error status. However, in this very case we cannot talk about an actual error since you have deliberately induced it yourself, and you are aware of the potential risk. At the same time, once being displayed in grey color, the icon cannot actually report any possible further error that might appear.

For this situation, within the above dialog you can select components that may be in an error state (*or switched off*) and you do not wish to get informed about it. The same option of **Ignoring component state** is also available for specific components directly from the <u>components overview in the AVG main window</u>.



11.3.Virus Vault

🕌 Advanced AVG Settings	
 Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Schedules E-mail Scanner Resident Shield Anti-Rootkit Update 	Virus Vault maintenance ✓ Limit Virus Vault Size ✓ Limit Virus Vault Size ✓ Automatic file deletion Delete files older than @ @ day(s) Maximum number of files to be stored: 1000 @
Default	OK Cancel Reply

The **Virus Vault maintenance** dialog allows you to define several parameters regarding the administration of objects stored in the <u>Virus Vault</u>:

- Limit Virus vault size use the slider to set up the maximum size of the <u>Virus Vault</u>. The size is specified proportionally compared to the size of your local disk.
- Automatic file deletion in this section define the maximum length of time that objects should be stored in the <u>Virus Vault</u> (Delete files older than ... days), and the maximum number of files to be stored in the <u>Virus Vault</u> (Maximum number of files to be stored)

11.4.PUP Exceptions

AVG is able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system. In some cases the user may wish to keep certain unwanted programs on the computer, (programs that were installed on purpose). Some programs, especially free ones, include adware. Such adware might be detected and reported by AVG as a **potentially unwanted program**. If you wish



to keep such a program on your computer, you can define it as a potentially unwanted program exception:

🕌 Advanced AVG Settings		
Appearance	Potentially Unwanted Programs Exceptions	
 Virus Vault PLP Exceptions Anti-Spam Web Shield LinkScanner Scans Construction Schedules E-mail Scanner Resident Shield Anti-Rootkit Update 	File File Path Checksum Image: Im	
Default	😵 OK Cancel 💽 Apply	

The **Potentially Unwanted Programs Exceptions** dialog displays a list of already defined and currently valid exceptions from potentially unwanted programs. You edit, delete, or add new exception.

Control buttons

- **Edit** opens an editing dialog (*identical with the dialog for new exception definition, see below*) of an already defined exception, where you can change the exception's parameters
- Remove deletes the selected item from the list of exceptions
- **Add exception** open an editing dialog where you can define parameters of the new exception to be created:



🕌 Exception Defi	inition 🛛
File:	
Checksum:	
File Info:	Extended file information not available.
0	Add Cancel

- *File* type the full path to the file that you want to mark as an exception
- Checksum displays the unique 'signature' of the chosen file. This checksum is an automatically generated string of characters, which allows AVG to unequivocally distinguish the chosen file from other files. The checksum is generated and displayed after successful addition of the file.
- *File Info* displays any additional information available about the file (*license/version information etc.*)
- Any location do not use full path if you want to define this file as an exception only for the specific location, then leave this checkbox unchecked

11.5.Anti-Spam



Advanced AVG Settings		
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Settings Performance RBL Whitelist Blacklist UnkScanner Scans Cons E-mail Scanner Resident Shield Anti-Rootkit Update Remote Administration	Anti-Spam basic settings Turn on Anti-Spam protection Mark message as SPAM if score is greater than: More Aggressive Le More Aggressive Le Move message to the junk folder (Microsoft Outlook plugin only) Add recipients of sent e-mails to whitelist Modify subject for messages marked as SPAM [SPAM] Train Anti-Spam	70 v
2 Default	😵 OK Cancel 🦉	Apply

In the *Engine performance settings* dialog you can check the *Turn on Anti-Spam protection* checkbox to allow/forbid the anti-spam scanning of e-mail communication.

In this dialog you can also select more or less aggressive scoring measures. The **Anti-***Spam* filter assigns each message a score (*i.e. how similar the message content is to SPAM*) based on several dynamic scanning techniques. You can adjust the **Mark***message as spam if score is greater than* setting by either typing the value (0 to 100) or by moving the slider left or right (*using the slider, the range of values is limited to* 50-90).

Generally we recommended setting the threshold between 50-90, or if you are really unsure, to 90. Here is a general review of the scoring threshold:

- **Value 90-99** Most incoming e-mail messages will be delivered normally (without being marked as <u>spam</u>). The most easily identified <u>spam</u> will be filtered out, but a significant amount of <u>spam</u> may still be allowed through.
- **Value 80-89** E-mail messages likely to be <u>spam</u> will be filtered out. Some non-spam messages may be incorrectly filtered as well.



- Value 60-79 Considered as a quite aggressive configuration. E-mail messages that are possibly <u>spam</u> will be filtered out. Non-spam messages are likely to be caught as well.
 - **Value 1-59** Very aggressive configuration. Non-spam e-mail messages are as likely to be caught as real <u>spam</u> messages. This threshold range is not recommended for normal use.
 - Value 0 In this mode, you will only receive e-mail messages from senders in your <u>Whitelist</u>. Any other e-mail messages will be considered as <u>spam</u>. This threshold range is not recommended for normal use.

In the **Engine performance settings** dialog you can further define how the detected <u>spam</u> e-mail messages should be treated:

- **Move message to junk folder** mark this check box to specify that each detected spam message should be automatically moved to the specific junk folder within your e-mail client;
- Add recipients of sent e-mails to <u>whitelist</u> tick this check box to confirm that all recipients of sent e-mails can be trusted, and all e-mail messages coming from their e-mail accounts can be delivered;
 - Modify subject for messages marked as spam tick this check box if you would like all messages detected as <u>spam</u> to be marked with a specific word or character in the e-mail subject field; the desired text can be typed in the activated text field.

Control buttons

Train Anti-Spam button open the <u>Anti-Spam training wizard</u> described in details in the <u>next chapter</u>.

The first dialog of the **Anti-Spam Training Wizard** asks you to select the source of e-mail messages you want to use for training. Usually, you will want to use either e-mails that have been incorrectly marked as SPAM, or spam messages that have not been recognized.



Anti-Spam training wizard		
Please choose a source training set. Folders with EML files Microsoft Office Outlook Windows Mail (Outlook Express) The Bat! Mozilla Thunderbird		
Heip	Cancel	Next

There are the following options to choose from:

- **A specific e-mail client** if you use one of the listed e-mail clients (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), simply select the respective option
- **Folder with EML files** if you use any other e-mail program, you should first save the messages to a specific folder (in *.eml format*), or make sure that you know the location of your e-mail client message folders. Then select **Folder with EML files**, which will enable you to locate the desired folder in the next step

For faster and easier training process, it is a good idea to sort the e-mails in the folders beforehand, so that the folder you will use for training contains only the training messages (either wanted, or unwanted). However, it is not necessary, as you will be able to filter the e-mails later on.

Select the appropriate option and click *Next* to continue the wizard.

Dialog displayed in this step depends on your previous selection.

Folders with EML files



A1	nti-Spam training wizar	d		
Folde Unso Pleas	rs contain: plicited e-mails (SPAM) e select folders for training.			
				Add folder Remove folder
	Heb		Cancel	Nevt

In this dialog, please select the folder with the messages you want to use for training. Press the *Add folder* button to locate the folder with the .eml files (*saved e-mail messages*). The selected folder will then be displayed in the dialog.

In the **Folders contain** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. You can also remove unwanted selected folders from the list by clicking the **Remove folder** button.

When done, click *Next* and proceed to *Message filtering options*.

Specific e-mail client

Once you confirm one of the options, new dialog will appear.



📕 Anti-Spam training wizard		\mathbf{X}
Folder contains:		
Unsolicited e-mails (SPAM)		v
Please select a folder for training.		
Deleted Items Drafts Inbox Outbox Sent Items		
Help	Cancel	Next

Note: In case of Microsoft Office Outlook, you will be prompted to select the MS Office Outlook profile first.

In the **Folders contain** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. A navigation tree of the selected e-mail client is already displayed in the main section of the dialog. Please locate the desired folder in the tree and highlight it with your mouse.

When done, click *Next* and proceed to <u>Message filtering options</u>.



📕 Anti-Spam training wizard		
Please select the type of filtering for messa	ges	
 All messages (no filtering) 		
🔘 Use filter		
Subject contains:		
From contains:		
O Ask for each message		
Help	Cancel	Next

In this dialog, you can set filtering of the e-mail messages.

If you are sure that the selected folder contains only messages you want to use for training, select the *All messages (no filtering)* option.

If you are unsure about the messages contained in the folder, and you want the wizard to ask you about every single message (so that you can determine whether to use it for training or not), select the **Ask for each message** option.

For more advanced filtering, select the **Use filter** option. You can fill in a word (*name*), part of a word, or phrase to be searched for in the e-mail subject and/or the sender's field. All messages matching exactly the entered criteria will be used for the training, without further prompting.

Attention!: When you fill in both text fields, addresses that match just one of the two conditions will be used, too!

When the appropriate option has been selected, click **Next**. The following dialog will be informative only, telling you that the wizard is ready to process the messages. To start training, click the **Next** button again. Training will then start according to previously selected conditions.



11.5.2.Performance

🕌 Advanced AVG Settings	_ 🗆 🖾
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Ignore faulty conditions Figure Anti-Spam Ignore RBL Ignore RBL Ignore Blacklist Ignore Figure Advanced Settings	Engine performance settings Use basic and advanced rules and the on-line check. Basic and advanced rules and training data are used to identify spam. All messages are checked on-line. This option is recommended.
Web Shield LinkScanner Scans Schedules E-mail Scanner Resident Shield Jore Resident Shield Jore Quarte Remote Administration	✓ Enable on-line checking If enabled, the Anti-Spam engine will communicate with the Mailshell SpamLabs servers to determine better scoring.
Default	Cancel Cancel

The **Engine performance settings** dialog (*linked to via the* **Performance** *item of the left navigation*) offers the **Anti-Spam** component performance settings. Move the slider left or right to change the level of scanning performance ranging between **Low memory** / **High performance** modes.

- **Low memory** during the scanning process to identify <u>spam</u>, no rules will be used. Only training data will be used for identification. This mode is not recommended for common use, unless the computer hardware is really poor.
- **High performance** this mode will consume large amount of memory. During the scanning process to identify <u>spam</u>, the following features will be used: rules and <u>spam</u> database cache, basic and advanced rules, spammer IP addresses and spammer databases.

The **Enable on-line checking** item is on by default. It results in more precise <u>spam</u> detection via communication with the <u>Mailshell</u> servers, i.e. the scanned data will be compared with <u>Mailshell</u> databases online.

Generally it is recommended to keep the default settings and only change them if you have a valid reason to do so. Any changes to this configuration



should only be done by expert users!

11.5.3.RBL

The **RBL** item open an editing dialog called **Realtime Blackhole Lists**:

불 Advanced AVG Settings		
 Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Settings Performance Whitelist Blacklist Blacklist UnkScanner Scans Schedules E-mail Scanner Resident Shield Anti-Rootkit Update Remote Administration 	Realtime Blackhole Lists Query RBL servers RBL servers list Specifies a list of Realtime Blackhole List (RBL) servers to query when analyzing messages. Default server format is servername:response:offset and servers are separated by comma.	
Default	Cancel	Apply .::

In this dialog you can switch on/off the **Query RBL servers** function.

The RBL (*Realtime Blackhole List*) server is a DNS server with an extensive database of known spam senders. When this feature is switched on, all e-mail messages will be verified against the RBL server database and marked as <u>spam</u> if identical to any of the database entries. The RBL servers databases contain the latest up-to-the-minute spam fingerprints, to provide the very best and most accurate <u>spam</u> detection. This feature is especially useful for users who receive large amounts of spam that is not being normally detected by the <u>Anti-Spam</u> engine.

The **RBL servers list** allows you to define specific RBL server locations.

Note: Enabling this feature may, on some systems and configurations, slow down the e-mail receiving process, as every single message must be verified against the RBL server database.



No personal data is sent to the server!

11.5.4.Whitelist

The **Whitelist** item opens a dialog with a global list of approved sender e-mail addresses and domain names whose messages will never be marked as <u>spam</u>.

🛃 Advanced AVG Settings		. 🗆 🗙
Auvanced Avo Settings Appearance	Approved e-mail senders list Approved e-mail senders list Edit	
Default	😵 OK Cancel 🕅 App	y

In the editing interface you can compile a list of senders that you are sure will never send you unwanted messages (<u>spam</u>). You can also compile a list of full domain names (e.g. *avg.com*), that you know do not generate spam messages.

Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once. The following control buttons are available:

- *Edit* press this button to open a dialog, where you can manually enter a list of addresses (you can also use *copy and paste*). Insert one item (sender, domain name) per line.
- **Import** if you already have a text file of email addresses/domain names prepared, you can simply import it by selecting this button. The input file



must be in plain text format, and the content must contain only one item (address, domain name) per line.

• **Export** - if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.

11.5.5.Blacklist

The **Blacklist** item opens a dialog with a global list of blocked sender e-mail addresses and domain names whose messages will always be marked as <u>spam</u>.

🛃 Advanced AVG Settings		_ 🗆 🔀
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Settings Performance RBL Whitelist Blacklist Whitelist Elacklist Elac	Blocked e-mail senders list Blocked e-mail senders list Elocked e-mail senders list Edit Export	Import
Default	Cancel	Apply

In the editing interface you can compile a list of senders that you expect to send you unwanted messages (<u>spam</u>). You can also compile a list of full domain names (e.g. *spammingcompany.com*), that you expect or receive spam messages from. All e-mail from the listed addresses/domains will be identified as spam.

Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once. The following control buttons are available:

• Edit - press this button to open a dialog, where you can manually enter a list



of addresses (you can also use *copy and paste*). Insert one item (sender, domain name) per line.

- **Import** if you already have a text file of email addresses/domain names prepared, you can simply import it by selecting this button. The input file must be in plain text format, and the content must contain only one item (address, domain name) per line.
- **Export** if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.

11.5.6.Advanced Settings

Typically it is recommended to keep the default settings and only change them if you have a valid reason to do so. Any changes to configuration should only be done by expert users!

If you still believe you need to change the <u>Anti-Spam</u> configuration at the very advanced level, please follow the instructions provided directly in the user interface. Generally, in each dialog you will find one single specific feature and you can edit it - its description is always included in the dialog itself:

- Cache fingerprint, domain reputation, LegitRepute
- **Training** word training, score history, score offset, maximum word entries, auto training threshold, weight, write buffer
- *Filtering* language list, country list, approved IPs, blocked IPs, blocked countries, blocked charsets, spoofed senders
- **RBL** RBL servers, multihit, threshold, timeout, maximum IPs
- Netcheck netcheck threshold
- Internet connection timeout



11.6.Web Shield

불 Advanced AVG Settings	
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield UnkScanner Scans Chick Schedules E-mail Scanner Resident Shield Anti-Rootkit Update	Web Shield You need to restart your web browser after you enable Web Shield. Once you disable Web Shield it is necessary to refresh the viewed web page. Threat notification mode Standard pop-up dialog (recommended) Tray balloon notification Tray icon signalization
Default	Cancel 🚱 Apply

The **Web Protection** dialog allows you to activate/deactivate the entire <u>Web Shield</u> component (*activated by default*). For further advanced settings of this component please continue to the subsequent dialogs as listed in the tree navigation.

In the bottom section of the dialog, select in which way you wish to be informed about possible detected threat: via standard pop-up dialog, via tray balloon notification, or via tray icon signalization.



Advanced AVG Settings	
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield Web Protection Instant Messaging LinkScanner Scans E-mail Scanner Resident Shield Anti-Rootkit Update	Web Protection Image: Check archives Image: Check archives Image: Scan Potentially Unwanted Programs and Spyware threats Image: Use heuristic analysis Ports to be scanned 80, 8080, 3128 Image: Maximum part size of a file to be scanned Image: Check analysis Image: Check analysis
Default	🕐 OK Cancel 🔗 Apply

11.6.1.Web Protection

In the **Web Protection** dialog you can edit the component's configuration regarding the scan of the website content. The editing interface allows you to configure the following elementary options:

- **Web protection** this option confirms that the <u>Web Shield</u> should perform scanning of the www pages content. Provided this option is on (*by default*), you can further switch on/off these items:
 - $_{\odot}$ **Check archives** scan the content of archives possibly included in the www page to be displayed .
 - Scan Potentially Unwanted Programs and Spyware threats scan potentially unwanted programs (*executable programs that can operate as spyware or adware*) included in the www page to be displayed, and <u>spyware</u> infections.
 - Use heuristic analysis scan the content of the page to be displayed using the <u>heuristic analysis</u> method (*dynamic emulation of the scanned* object's instructions in a virtual computer environment).



- *Ports to be scanned* this field lists the standard http communication port numbers. If your computer configuration differs, you can change the port numbers as needed.
- Maximum file size to be scanned if included files are present in the displayed page you can also scan their content even before these are downloaded to your computer. However, scanning of large files takes quite some time and the web page download might be slowed significantly. You can use the slide bar to specify the maximum size of a file that is still to be scanned with <u>Web Shield</u>. Even if the downloaded file is bigger than specified, and therefore will not be scanned with Web Shield, you are still protected: in case the file is infected, the <u>Resident Shield</u> will detect it immediately.
- Exclude host/IP/domain into the text field you can type the exact name of a server (host, IP address, IP address with mask, or URL) or a domain that should not be scanned by <u>Web Shield</u>. Therefore exclude only host that you can be absolutely sure would never provide dangerous website content.

🕌 Advanced AVG Settings		- 🗆 🗙
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield Web Protection LinkScanner Scans Constant Messaging LinkScanner Resident Shield Anti-Rootkit Update	Instant Messaging Shield ✓ Enable Instant Messaging Shield ✓ ICQ protection ✓ MSN protection	
Default	😵 OK Cancel 😵 Ar	pply

11.6.2.Instant Messaging



In the **Instant Messaging Shield** dialog you can edit the <u>Web Shield</u> components settings referring to instant messaging scanning. Currently the following three instant messaging programs are supported: **ICQ**, **MSN**, and **Yahoo** - tick the respective item for each of them if you want the Web Shield to verify the on-line communication is virus free.

For further specification of allowed/blocked users you can see and edit the respective dialog (*Advanced ICQ*, *Advanced MSN*) and specify the *Whitelist* (*list of users that will be allowed to communicate with you*) and *Blacklist* (*users that should be blocked*).

불 Advanced AVG Settings			×
 Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield UnkScanner Scans Scans Schedules E-mail Scanner Resident Shield Anti-Rootkit Update 	 LinkScanner settings ✓ Enable AVG Search-Shield (need web browser restart) ✓ Enable AVG Active Surf-Shield ✓ Enable reporting of detected threats to AVG 		
Default	👻 OK Cancel 👻	Apply	

11.7.Link Scanner

The *LinkScanner settings* dialog allows you to switch on/off the two elementary features of the *LinkScanner*:

- **Enable Safe Search** (on by default): advisory notifying icons on searches performed in Google, Yahoo, MSN or Baidu having checked ahead the content of sites returned by the search engine.
- Enable Safe Surf (on by default): active (real-time) protection against



exploitive sites as they are accessed. Known malicious site connections and their exploitive content is blocked as they are accessed by the user via a web browser (*or any other application that uses HTTP*).

• **Enable reporting to AVG of exploited websites** - (on by default): mark this item to allow back reporting of exploits and bad sites found by users either via **Safe Surf** or **Safe Search** to feed the database collecting information on malicious activity on the web.

11.8.Scans

The advanced scan settings is divided into three categories referring to specific scan types as defined by the software vendor:

- <u>Scan Whole Computer</u> standard predefined scan of the entire computer
- <u>Shell Extension Scan</u> specific scanning of a selected object directly from the Windows Explorer environment
- <u>Scan Specific Files or Folders</u> standard predefined scan of selected areas of your computer
- <u>Removable Device Scan</u> specific scanning of removable devices attached to your computer



11.8.1.Scan Whole Computer

The **Scan whole computer** option allows you to edit parameters of one of the scans predefined by the software vendor, **Scan of the whole computer**:

불 Advanced AVG Settings		_ 🗆 🗙
 Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Scans becific files or folders Schedules E-mail Scanner Resident Shield Anti-Rootkit Update 	Scan settings Automatically heal/remove infections Scan Potentially Unwanted Programs and Spyware threats Scan for Tracking Cookies Scan inside archives Use Heuristics Scan system environment Scan for rootkits Scan infectable files only Scan media files Scan process priority Automatic scan Set additional scan reports	
Default	😵 OK Cancel 🕅	Apply

Scan settings

The **Scan settings** section offers a list of scanning parameters that can be optionally switched on/off:

- **Automatically heal/remove infection** if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, or if you decide to switch off this option, you will be notified upon a virus detection and will have to decide what to do with the detected infection. The recommended method is to remove the infected file to the <u>Virus Vault</u>.
- **Scan Potentially Unwanted Programs** this parameter controls the <u>Anti-Virus</u> functionality that allows <u>detection of potentially unwanted programs</u> (*executable files that can run as spyware or adware*) and these can then be


blocked, or removed;

- **Scan for cookies** this parameter of the <u>Anti-Spyware</u> component defines that cookies should be detected; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)
- **Scan inside archives** this parameters defines that scanning should check all files even those stored inside archives, e.g. ZIP, RAR, ...
- **Use Heuristics** heuristic analysis (*dynamic emulation of the scanned object' s instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;
- Scan system environment scanning will also check the system areas of your computer;
- Scan for rootkits tick this item if you want to include the rootkit detection into scanning of the entire computer. The rootkit detection is also available on its own within the <u>Anti-Rootkit</u> component;
- **Scan infectable files only** with this option switched on, files that cannot get infected will not be scanned. These can be for instance some plain text files, or some other non-executable files.
 - Scan media files check to scan media files (Video, Audio etc.). If you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus.

Scan process priority

Within the **Scan process priority** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but system resources usage will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease system resources usage by extending the scanning duration.

Set additional scan reports ...



Click the *Set additional scan reports* ... link to open a standalone dialog window called *Scan reports* where you can tick several items to define what scan findings should be reported:

📕 Scan reports 🛛 🔀
Scan reports
Report password protected archives
Report password protected documents
Report locked files
Report files containing macro
Report hidden extensions
Save Cancel

11.8.2.Shell Extension Scan

Similar to the previous <u>Scan whole computer</u> item, this item named **Shell** extension scan also offers several options for editing the scan predefined by the software vendor. This time the configuration is related to <u>scanning of specific objects</u> <u>launched directly from the Windows Explorer</u> environment (*shell extension*), see chapter <u>Scanning in Windows Explorer</u>:

불 Advanced AVG Settings		
 Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Scans Scans Scan specific files or folders Removable device scan Schedules E-mail Scanner Resident Shield Anti-Rootkit Update 	Scan settings Automatically heal/remove infections Scan Potentially Unwanted Programs and Spyware threats Scan for Tracking Cookies Scan inside archives Use Heuristics Scan system environment Scan for rootkits Scan infectable files only Scan process priority Automatic scan Set additional scan reports	
Default	🕐 OK Cancel 🕅	Apply



The list of parameters is identical to those available for the <u>Scan of the whole</u> <u>computer</u>. However, the default settings differ: with the **Scan of the Whole Computer** most parameters are selected while for the **Shell extension scan** (<u>Scanning in Windows Explorer</u>) only the relevant parameters are switched on.

11.8.3.Scan Specific Files or Folders

The editing interface for *Scan specific files or folders* is identical to the <u>*Scan*</u> <u>*Whole Computer*</u> editing dialog. All configuration options are the same; however, the default settings are more strict for the <u>*Scan of the whole computer*</u>:

🕌 Advanced AVG Settings		- 🗆 🔀
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Scan whole computer Scan specific files or folders Removable device scan E-mail Scanner Resident Shield Anti-Rootkit Update	Scan settings Automatically heal/remove infections Scan Potentially Unwanted Programs and Spyware threats Scan for Tracking Cookies Scan inside archives Use Heuristics Scan system environment Scan for rootkits Scan media files Scan process priority Automatic scan Set additional scan reports	
Default	Cancel	Apply

All parameters set up in this configuration dialog apply only to the areas selected for scanning with the <u>Scan of specific files or folders</u>! If you tick the **Scan for rootkits** option within this configuration dialog, only a quick rootkit test will be performed, i.e. rootkit scanning of selected areas only.

Note: For a description of specific parameters please consult the chapter <u>AVG</u> <u>Advanced Settings / Scans / Scan Whole Computer</u>.



11.8.4.Removable Device Scan

The editing interface for **Removable device scan** is also very similar to the <u>Scan</u> <u>Whole Computer</u> editing dialog:

불 Advanced AVG Settings		_ 🗆 🔀
 Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Scan whole computer Scan shell extension scan Scan specific files or folders Schedules E-mail Scanner Resident Shield Anti-Rootkit Update 	Enable Removable device scan Scan settings Automatically heal/remove infections Scan Potentially Unwanted Programs and Spyware threats Scan for Tracking Cookies Scan inside archives Scan inside archives Use Heuristics Scan media files Scan process priority Automatic scan Set additional scan reports	
Default	Cancel	Apply

The **Removable device scan** is launched automatically once you attach any removable device to your computer. By default, this scanning is switched off. However, it is crucial to scan removable devices for potential threats since these are a major source of infection. To have this scanning ready and launched automatically when needed, mark the **Enable Removable device scan** option.

Note: For a description of specific parameters please consult the chapter <u>AVG</u> <u>Advanced Settings / Scans / Scan Whole Computer</u>.

11.9.Schedules

In the **Schedules** section you can edit the default settings of:

- Whole computer scan schedule
- Virus database update schedule



- Program update schedule
 - Anti-Spam update schedule

11.9.1.Scheduled Scan

Parameters of the scheduled scan can be edited (*or a new schedule set up*) on three tabs:

🕌 Advanced AVG Settings		
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Comparison Comp	Schedule settings How to scan What to scan Name Schedule this task Name Schedule running Run every: 1 Hour(s) Run at a specific time interval: Every day Cation based: On computer startup Action based: On computer startup Advanced schedule options Run on computer is in low power mode Delay this task if a full-screen application is running	
Default	🕐 OK Cancel 🕅 Apply	

On the **Schedule settings** tab you can first check/uncheck the **Enable this task** item to simply deactivate the scheduled test temporarily, and switch it on again as the need arises.

Next, give a name to the scan you are about to create and schedule. Type the name into the text field by the **Name** item. Try to use brief, descriptive and apt names for scans to make it easier to later recognize the scan from others.

Example: It is not appropriate to call the scan by the name of "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System areas scan" etc. Also it is not necessary to specify in the scan's name whether it is the scan of the whole of



the computer or just a scan of selected files or folders - your own scans will always be a specific version of the <u>scan of selected files or folders</u>.

In this dialog you can further define the following parameters of the scan:

- Schedule running specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time (*Run every ...*) or by defining an exact date and time (*Run at specific time ...*), or possibly by defining an event that the scan launch should be associated with (*Action based on computer startup*).
- **Advanced schedule options** this section allows you to define under which conditions the scan should/should not be launched if the computer is in low power mode or switched off completely.

Once the scheduled scan is launched in the time you have specified, you will be informed on this fact via a pop-up window opened over the <u>AVG system tray icon</u>:

불 Scan		×
Scheduled scan was started.		
) s	17 88	10:38

A new <u>AVG system tray icon</u> then appears (*in full color with a white arrow - see picture above*) informing a scheduled scan is running. Right-click on the running scan AVG icon to open a context menu where you can decide to pause or even stop the running scan:

Scheduled scan	•		<u>×</u>
		- a	- Bi:
Pause all scans			
Stop all scans			
20		. 77 - 1	11:11



불 Advanced AVG Settings		_ 🗆 🗙
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Schedules Schedules Forgram update schedule Anti-Spam update schedule Anti-Spam update schedule E-mail Scanner Resident Shield Anti-Rootkit Update	Schedule settings How to scan What to scan Automatically heal/remove infections Scan Potentially Unwanted Programs and Spyware threats Scan for Tracking Cookies Scan for Tracking Cookies Scan inside archives Scan system environment Scan for rootkits Scan infectable files only Scan media files Scan process priority Automatic scan Set additional scan reports Additional scan settings	
Default	Image: Cancel Image: Cancel Image: Cancel	Apply

On the **How to scan** tab you will find a list of scanning parameters that can be optionally switched on/off. By default, most parameters are switched on and the functionality will be applied during scanning. Unless you have a valid reason to change these settings we recommend to keep the predefined configuration:

- **Automatically heal/remove infection** (*switched on, by default*): if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, or if you decide to switch off this option, you will be notified upon virus detection and will have to decide what to do with the detected infection. The recommended action is to remove the infected file to the <u>Virus Vault</u>.
- Scan Potentially Unwanted Programs (switched on, by default): this parameter controls the <u>Anti-Virus</u> functionality that allows <u>detection of</u> <u>potentially unwanted programs</u> (executable files that can run as spyware or adware) and these can then be blocked, or removed;
- Scan for cookies (switched on, by default): this parameter of the <u>Anti-Spyware</u> component defines that cookies should be detected during scanning ; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their*



electronic shopping carts)

- **Scan inside archives** (*switched on, by default*): this parameter defines the scanning should check all files even if they are stored inside an archive, e.g. ZIP, RAR, ...
- **Use Heuristics** (switched on, by default): heuristic analysis (dynamic emulation of the scanned object's instructions in a virtual computer environment) will be one of the methods used for virus detection during scanning;
- **Scan system environment** (*switched on, by default*): scanning will also check the system areas of your computer;
- Scan for rootkits tick this item if you want to include the rootkit detection into scanning of the entire computer. The rootkit detection is also available on its own within the <u>Anti-Rootkit</u> component;
- **Scan infectable files only** (*switched off, by default*): with this option switched on, scanning will not be applied to files that cannot get infected. These can be for instance some plain text files, or some other non-executable files.

Within the **Scan process priority** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but the system resources usage will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease the system resources usage by extending the scanning duration.

Click the **Set additional scan reports** ... link to open a standalone dialog window called **Scan reports** where you can tick several items to define what scan findings should be reported:

Scan reports
Scan reports
Report password protected archives
Report password protected documents
Report locked files
Report files containing macro
Report hidden extensions
Save Cancel



Click the **Additional scan settings** ... to open a new **Computer shutdown options** dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option activates that allows the computer to shut down even if it is currently locked (**Force shutdown is computer is locked**).

📕 Additional scan settings 🛛 🔀
Computer shutdown options
Shutdown computer upon scan completion
Force shutdown if computer is locked
OK Cancel

🕌 Advanced AVG Settings		- 🗆 🛛
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield	Schedule settings How to scan What to scan Constraint Scan whole computer Constraint Scan specific files or folders	
 LinkScanner Scans Schedules Scheduled scan Virus database update schedule Program update schedule E-mail Scanner E-mail Scanner Resident Shield Anti-Rootkit Update 	Cesktop Gesktop Gesktop	
Default	Cancel 👻	Apply

On the **What to scan** tab you can define whether you want to schedule <u>scanning of</u> the whole computer or <u>scanning of specific files or folders</u>. If you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify the folders to be scanned.



불 Advanced AVG Settings		
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Schedules Schedules Kordules Virus database update schedule Anti-Spam update schedule Anti-Spam update schedule Anti-Spam update schedule Anti-Spam update schedule Anti-Rootkit Update	Schedule settings Image: Enable this task Name Virus database update schedule Schedule running Image: Run every: 4 Image: Run every: 17:00 Image: Run every: 17:00 Image: Run every: 17:00 Image: Run even if computer startup if task has been missed Image: Run even if computer is in low power mode Image: Delay this task if a full-screen application is running Other update settings Image: Run the update again as soon as the internet connection is available.	
Default	Cancel 👻 Appl	y,

11.9.2.Virus Database Update Schedule

On the **Schedule settings** tab you can first check/uncheck the **Enable this task** item to simply deactivate the scheduled virus database update temporarily, and switch it on again as the need arises.

The basic virus database update scheduling is covered within the <u>Update Manager</u> component. Within this dialog you can set up some detailed parameters of the virus database update schedule:

Give a name to the virus database update schedule you are about to create. Type the name into the text field by the **Name** item. Try to use brief, descriptive and appropriate names of update schedules to make it easier to recognize the schedule among others later.

• **Schedule running** - specify the time intervals for the newly scheduled virus database update launch. The timing can either be defined by the repeated update launch after a certain period of time (**Run every** ...) or by defining an exact date and time (**Run at specific time** ...), or possibly by defining an event that the update launch should be associated with (**Action based on**



computer startup).

- **Advanced schedule options** this section allows you to define under which conditions the virus database update should/should not be launched if the computer is in low power mode or switched off completely.
- **Other update settings** check this option to make sure than if the internet connection gets corrupted and the update process fails, it will be launched again immediately after the internet connection is restored.

Once the scheduled scan is launched in the time you have specified, you will be informed on this fact via a pop-up window opened over the <u>AVG system tray icon</u> (*provided that you have kept the default configuration of the the <u>Advanced Settings/</u><u>Appearance</u> dialog).*

11.9.3.Program Update Schedule

😹 Advanced AVG Settings				-	
Appearance Ignore faulty conditions	Schedule settings				
PUP Exceptions Anti-Spam Let Web Shield	V Enable this task	Program update sched	ule		
LinkScanner LinkScanner Scans Scans	Schedule running ORun every:	12 🗘 Hour(s)		*	
Credules Scheduled scan Virus database update schedule Program update schedule	Run at a specific time interval: Action based:	Every day	▼ 8:00	minutes delav	∃
Anti-Spam update schedule 	Advanced schedule options	<pre>chas been missed</pre>	×	V	
E_ Anti-Rootkit ⊕E_ Update	Run even if computer is in low power mode Delay this task if a full-screen application is running				
	Other update settings	as the internet connectio	n is available.		~
Default		👻 ОК	Cano	cel 🕜 App	ly

On the **Schedule settings** tab you can first check/uncheck the **Enable this task** item to simply deactivate the scheduled program update temporarily, and switch it on again as the need arises.



Next, give a name to the program update schedule you are about to create. Type the name into the text field by the **Name** item. Try to use brief, descriptive and appropriate names of update schedules to make it easier to recognize the schedule among others later.

- Schedule running specify the time intervals for the newly scheduled program update launch. The timing can either be defined by the repeated update launch after a certain period of time (*Run every ...*) or by defining an exact date and time (*Run at specific time ...*), or possibly by defining an event that the update launch should be associated with (*Action based on computer startup*).
- **Advanced schedule options** this section allows you to define under which conditions the program update should/should not be launched if the computer is in low power mode or switched off completely.
- **Other update settings** check this option to make sure than if the internet connection gets corrupted and the update process fails, it will be launched again immediately after the internet connection is restored.

Once the scheduled scan is launched in the time you have specified, you will be informed on this fact via a pop-up window opened over the <u>AVG system tray icon</u> (*provided that you have kept the default configuration of the the <u>Advanced Settings/</u><u>Appearance</u> dialog).*



🕌 Advanced AVG Settings			
Appearance Ignore faulty conditions	Schedule settings		
	✓ Enable this task Name	Anti-Spam update schedule	
InkScanner Scans Schedules	Schedule running Run every:	2 🕞 Hour(s)	
- R Scheduled scan - R Virus database update schedule - R Program update schedule	Run at a specific time interval:	Every day 9:00 \$ 10:00 \$	∃
Anti-Spam update schedule E-mail Scanner E-mail Scanner E [] Resident Shield	Advanced schedule options	khas been missed	
⊕ ∰ Update	✓ Run even if computer is in low p Delay this task if a full-screen a	power mode pplication is running	
	Other update settings Run the update again as soon a	as the internet connection is available.	~
Default		🕐 OK Cancel 🕅 App	ly

11.9.4.Anti-Spam Update Schedule

On the **Schedule settings** tab you can first check/uncheck the **Enable this task** item to simply deactivate the scheduled <u>Anti-Spam</u> update temporarily, and switch it on again as the need arises.

Basic <u>Anti-Spam</u> update scheduling is covered within the <u>Update Manager</u> component. Within this dialog you can set up some detailed parameters of the update schedule:

Next, give a name to the <u>Anti-Spam</u> update schedule you are about to create. Type the name into the text field by the **Name** item. Try to use brief, descriptive and appropriate names of update schedules to make it easier to recognize the schedule among others later.

Schedule running - specify the time intervals for the newly scheduled <u>Anti-Spam</u> update launch. The timing can either be defined by the repeated <u>Anti-Spam</u> update launch after a certain period of time (*Run every ...*) or by defining an exact date and time (*Run at specific time ...*), or possibly by defining an event that the update launch should be associated with (*Action*)



based on computer startup).

- **Advanced schedule options** this section allows you to define under which conditions the <u>Anti-Spam</u> update should/should not be launched if the computer is in low power mode or switched off completely.
- Task settings in this section you can uncheck the Enable this task item to simply deactivate the scheduled <u>Anti-Spam</u> update temporarily, and switch it on again as the need arises.
- Other update settings check this option to make sure than if the internet connection gets corrupted and the <u>Anti-Spam</u> update process fails, it will be launched again immediately after the internet connection is restored.

Once the scheduled scan is launched in the time you have specified, you will be informed on this fact via a pop-up window opened over the <u>AVG system tray icon</u> (*provided that you have kept the default configuration of the the <u>Advanced Settings/</u><u>Appearance</u> dialog).*

11.1(E-mail Scanner

불 Advanced AVG Settings	
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Certification Mail Filtering Logs and Results Servers Resident Shield Anti-Rootkit Update Remote Administration	E-mail scanning Check incoming e-mail Certify e-mail With attachments only Modify subject of virus infected messages ***VIRUS**** Scanning properties Vuse Heuristics Scan Potentially Unwanted Programs and Spyware threats Scan inside archives E-mail attachments reporting Report password protected achives Report password protected documents Report files containing macro Report hidden extensions Move reported attachments to Virus Vault (incoming e-mails only)
Default	Tancel Reply



The *E-mail Scanner* dialog is divided into three sections:

- *E-mail scanning* in this section select whether you want to scan the incoming/outgoing e-mail messages and whether all e-mails should be certified or only e-mails with attachments (e-*mail virus-free certification is not supported in HTML/RTF format*). Additionally you can choose if you want AVG to modify the subject for messages that contain potential viruses. Tick the *Modify subject of virus infected messages* checkbox and change the text respectively (*default value is ***VIRUS****).
- Scanning properties specify whether the <u>heuristic analysis</u> method should be used during scanning (Use heuristic), whether you want to check for the presence of <u>potentially unwanted programs</u> (Scan Potentially Unwanted Programs), and whether archives should be scanned too (Scan inside archives).
- **E-mail attachments reporting** specify whether you wish to be notified via e-mail about password protected archives, password protected documents, macro containing files and/or files with hidden extension detected as an attachment of the scanned e-mail message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the <u>Virus Vault</u>.



11.10.:Certification

불 Advanced AVG Settings		
Appearance Ignore faulty conditions Urus Vault PUP Exceptions Anti-Spam	Incoming e-mail Incoming e-mail certification text: No virus found in this incoming message.	<
🕀 📳 Web Shield	Language used for the incoming e-mail certification text:	
InkScanner InkScanner InkScanner	Default install language	~
Creating Schedules E-mail Scanner Certification Mail Filtering Logs and Results Servers Resident Shield Anti-Rootkit Update Remote Administration	Outgoing e-mail Outgoing e-mail certification text: No virus found in this outgoing message. Language used for the outgoing e-mail certification text: Default install language	
Default	😵 OK Cancel 😵 A	pply

In the *Certification* dialog you can specify exactly what text the certification note should contain, and in what language. This should be specified separately for *Incoming mail* and *Outgoing mail*.



🕌 Advanced AVG Settings		_ 🗆 🛛
Appearance Ignore Faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield IinkScanner Scans Certification Mail Filtering Logs and Results Exervers Resident Shield Anti-Rootkit Update Remote Administration	Attachment filter Remove attachments Remove all executable files Remove files with these comma separated extensions:	
Default	🛞 OK Cancel 🕅	Apply

11.10.2 Mail Filtering

The **Attachment filter** dialog allows you to set up parameters for e-mail messages attachment scanning. By default, the **Remove attachments** option is switched off. If you decide to activate it, all e-mail message attachments detected as infectious or potentially dangerous will be removed automatically. If you want to define specific types of attachments that should be removed, select the respective option:

- Remove all executable files all *.exe files will be deleted
- Remove all documents all *.doc files will be deleted
- Remove files with these extensions will remove all files with the defined extensions



🛃 Advanced AVG Settings		_ 🗆 🔀
Advanced AvG settings	Logs Maintenance Monthly logs Weekly logs Daily logs Automatic logs Maximum log file size: Umatic logs Medium Folder used to store log files C:\Documents and Settings\All Users\Application Data\avg8\Emc\Log	MB
Default	🕐 OK Cancel 🔮	Apply

11.10.:Logs and Results

The dialog opened via the *Logs and Results* navigation item allows you to specify parameters for e-mail scanning results maintenance. The dialog is divided into several sections:

- **Logs Maintenance** define whether you want to log e-mail scanning information daily, weekly, monthly, ... ; and also specify the maximum size of the log file (*in MB*)
- **Log level threshold** the medium level is set up by default you can select a lower level (*logging elementary connection information*) or higher level (*logging of all traffic*)
- Folder used to store log files define where the log file should be located

11.10.4Servers

In the **Servers** section you can edit parameters of the <u>**E-mail Scanner**</u> component servers, or set up a new server fusing the **Add new server** button.



ver Name			_
server settings (used in e-mail client): POP when available n: ant POP3 server settin	Regula		10110
	I settings t (used in e-mail client): POP when available on: ent POP3 server settir ent POP3 server activ ate this server and use it fo	I settings t (used in e-mail client): POP when available on: Regula ent POP3 server settings ent POP3 server activation ate this server and use it for receiving e-mail	I settings t (used in e-mail client): POP when available on: Regular ent POP3 server settings ent POP3 server activation ate this server and use it for receiving e-mail

In this dialog (opened via **Servers / POP3**) you can set up a new <u>**E-mail Scanner**</u> server using the POP3 protocol for incoming mail:

- **POP3 Server Name** type in the name of the server or keep the AutoPOP3 default name
- **Type of login** defines the method for determining the mail server used for incoming mail:
 - $_{\odot}$ Automatic Login will be carried out automatically, according to your e-mail client settings.
 - USER/COMPUTER the simplest and the most frequently used method for determining the destination mail server is the proxy method. To use this method, specify the name or address (or also the port) as part of the login user name for the given mail server, separating them with the / character. For example, for the account user1 on the server pop.acme.com and the port 8200 you would use user1/pop.acme.com:8200 for the login name.



- Fixed host In this case, the program will always use the server specified here. Please specify the address or name of your mail server. The login name remains unchanged. For a name, you may use a domain name (for example, pop.acme.com) as well as an IP address (for example, 123.45.67.89). If the mail server uses a non-standard port, you can specify this port after the server name by using a colon as the delimiter (for example, pop.acme.com:8200). The standard port for POP3 communication is 110.
- Additional settings specifies more detailed parameters:

- Local port specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for POP3 communication.
- Use APOP when available this option provides more secure mail server login. This makes sure that the <u>*E-mail Scanner*</u> uses an alternative method of forwarding the user account password for login, sending the password to the server not in an open, but in an encrypted format using a variable chain received from the server. Naturally, this feature is available only when the destination mail server supports it.
- Connection in the drop-down menu, you can specify which kind of connection to use (regular/SSL/SSL default). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
- *E-mail client POP3 server activation* provides brief information on the configuration settings required to correctly configure your e-mail client (so that the *E-mail Scanner* will check all incoming mail). This is a summary based on the corresponding parameters specified in this dialog and other related dialogs.



불 Advanced AVG Settings		
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Certification Mail Filtering Logs and Results Servers POP3 AutoPOP3:10110 SMTP AutoSMTP:10025 Resident Shield Anti-Rootkit Update Remote Administration	SMTP Server Name AutoSMTP Relay Host Automatic Fixed host Additional settings Local port (used in e-mail client): Queue processing: Automatic Manual Connection: Administrative server Send administrative messages to server port: E-mail client SMTP server settings Original E-mail client SMTP server activation Image: Activate this server and use it for sending e-mail	10025 Regular AutoPOP3:10110
Default	📀 ОК	Cancel 💽 Apply

In this dialog (opened via *Servers / SMTP*) you can set up a new *E-mail Scanner* server using the SMTP protocol for outgoing mail:

- SMTP Server Name type in the name of the server or keep the AutoSMTP default name
- **Relay Host** defines the method for determining the mail server used for outgoing mail:
 - $_{\odot}$ Automatic login will be carried out automatically, according to your e-mail client settings
 - Fixed host in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (for example, smtp.acme.com) as well as an IP address (for example, 123.45.67.89) for a name. If the mail server



uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (for example, smtp.acme.com:8200). The standard port for SMTP communication is 25.

• Additional settings - specifies more detailed parameters:

- $_{\odot}$ Local port specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for SMTP communication.
 - Queue processing determines the behavior of the <u>*E-mail Scanner*</u> when processing the requirements for sending mail messages:
 - Automatic the outgoing mail is immediately delivered (sent) to the target mail server
 - Manual the message is inserted into the queue of outgoing messages and sent later
 - Connection in this drop-down menu, you can specify which kind of connection to use (regular/SSL/SSL default). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is available only when the destination mail server supports it.
 - **Administrative server** shows the number of the port of the server that will be used for the reverse delivery of administration reports. These messages are generated, for example, when the target mail server rejects the outgoing message or when this mail server is not available.
 - *E-mail client SMTP server settings* provides information on how to configure the client mail application so that outgoing mail messages are checked using the currently modified server for checking the outgoing mail. This is a summary based on the corresponding parameters specified in this dialog and other related dialogs.



11.1 Resident Shield

The **<u>Resident Shield</u>** component performs live protection of files and folders against viruses, spyware and other malware.

불 Advanced AVG Settings		
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Veb Shield InkScanner Scans E-mail Scanner E-mail Scanner Resident Shield E-mail Scanner Advanced Settings Exceptions Anti-Rootkit Update Remote Administration	Resident Shield Scan for Tracking Cookies Scan Fortulally Unwanted Programs and Spyware threats Scan files on close Scan boot sector of removable media Use Heuristics Auto-heal	
Default	👻 OK Cancel 👻	Apply

In the **Resident Shield Settings** dialog you can activate or deactivate the <u>Resident</u> <u>Shield</u> protection completely by checking/unchecking the **Enable Resident Shield** item (*this option is switched on by default*). In addition you can select which <u>Resident Shield</u> features should be activated:

- **Scan cookies** this parameter defines that cookies should be detected during scanning. (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)
- Scan Potentially Unwanted Programs (switched on by default) scanning for <u>potentially unwanted programs</u> (executable applications that can behave as various types of spyware or adware)
- **Scan on process closing** on-close scanning ensures that AVG scans active objects (e.g. applications, documents ...) when they are being opened, and



also when they are being closed; this feature helps you protect your computer against some types of sophisticated virus

- Scan boot sector of removable media (switched on by default)
- **Use Heuristics** (switched on by default) <u>heuristic analysis</u> will be used for detection (dynamic emulation of the scanned object's instructions in a virtual computer environment)
- Auto-heal any detected infection will be healed automatically if there is a cure available

11.11.1Advanced Settings

In the *Files scanned by the Resident Shield* dialog it is possible to configure which files will be scanned (*by specific extensions*):

🕌 Advanced AVG Settings	
Appearance Grant Grant	Files scanned by the Resident Shield Scan all files Scan all files Scan infectable files and selected types of documents Exclude files with the following extensions from scanning: Always scan files with the following extensions: 386;ASP;BAT;BIN;BMP;BOO;CHM;CLA;CLAS*;CMD;CNM;COM;CPL;DEV;DLL;DO*;DRV;EML;E: Always scan files without extensions The Resident Shield will scan Resident Shield will scan files with following extensions: 386;ASP;BAT;BIN;BMP;BOO;CHM;CLA;CLAS*;CMD;CNM;COM;CPL;DEV;DLL;DO*;DRV;EML;E: xextensions The Resident Shield will scan Resident Shield will scan files with following extensions: 386;ASP;BAT;BIN;BMP;BOO;CHM;CLA;CLAS*;CMD;CNM;COM;CPL;DEV;DLL;DO*;DRV;EML;E: Scanning files without extension is on.
Default	🕐 OK Cancel 🕅 Apply

Decide whether you want all files to be scanned or just infectable files - if so, you can further specify a list of extensions defining files that should be excluded from scanning, and also a list of file extensions defining files that must be scanned under



all circumstances.

11.11. Exceptions

🕌 Advanced AVG Settings	
Appearance J Ignore faulty conditions	Resident Shield - Directory Excludes
PUP Exceptions Anti-Spam Make Skield	Add Path Add List
E LinkScanner	Edit Path
🕀 🕼 Schedules 🖶 🚛 E-mail Scanner 🖨 🚛 Resident Shield	E dit List
Exceptions	Remove Path
E Update E Remote Administration	
Default	Cancel Reply

The **Resident Shield - Directory Excludes** dialog offers the possibility of defining folders that should be excluded from the <u>Resident Shield</u> scanning. If this is not essential, we strongly recommend not excluding any directories!

The dialog provides the following control buttons:

- **Add path** specify directories to be excluded from the scanning by selecting them one by one from the local disk navigation tree
- Add list allows you to enter a whole list of directories to be excluded from the <u>Resident Shield</u> scanning
- *Edit path* allows you to edit the specified path to a selected folder
- Edit list allows you to edit the list of folders
- Remove path allows you to delete the path to a selected folder from the list



11.1:Anti-Rootkit

In this dialog you can edit the *<u>Anti-Rootkit</u>* component's configuration:



Editing of all functions of the <u>Anti-Rootkit</u> component as provided within this dialog is also accessible directly from the <u>Anti-Rootkit component's interface</u>.

Mark up the respective check-boxes to specify objects that should be scanned:

- Scan applications
- Scan DLL libraries
- Scan drivers

Further you can pick the rootkit scanning mode:

- Quick rootkit scan scans only the system folder (typically c:\Windows)
- Full rootkit scan scans all accessible disks except for A: and B:



11.1:Update

🕌 Advanced AVG Settings	
Appearance Ignore faulty conditions Virus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans E-mail Scanner Resident Shield Anti-Rootkit Update Proxy Dial-up URL Manage Remote Administration	When to update files ○ Update upon next computer restart. (Updated files will be prepared, and the update will be completed after the computer restart.) ③ Update immediately If computer restart is required: ④ Require confirmation from the user ○ Restart immediately ○ Complete at next computer restart Additional update options ✓ Build new system restore point after each program update. ✓ Use DNS update ✓ Require confirmation to close running applications. AVG may require the closing of some running applications (for example MS Outlook). ✓ Check computer time Display notification if time set on computer differs from the correct time more than 24 ➡ hours
Default	Cancel 👻 Apply

The **Update** navigation item opens a new dialog where you can specify general parameters regarding the <u>AVG update</u>:

When to update files

In this section you can select between two alternative options: <u>update</u> can be scheduled for the next PC restart or you can launch the <u>update</u> immediately. By default, the immediate update option is selected since this way AVG can secure the maximum safety level. Scheduling an update for the next PC restart can only be recommended if you are sure the computer gets restarted regularly, at least daily.

If you decide to keep the default configuration and launch the update process immediately, you can specify the circumstances under which a possible required restart should be performed:

Require confirmation from the user - you will be asked to approve a PC restart needed to finalize the <u>update process</u>



- Restart immediately the computer will be restarted automatically immediately after the <u>update process</u> has finished, and your approval will not be required
 - **Complete at next computer restart** the <u>update process</u> finalization will be postponed until the next computer restart again, please keep in mind that this option is only recommended if you can be sure the computer gets restarted regularly, at least daily

Additional update options

- **Build new system restore point after each program update** before each AVG program update launch, a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS in its original configuration from this point. This option is accessible via Start / All Programs / Accessories / System tools / System Restore, but any changes can be recommended to experienced users only! Keep this check-box ticked if you want to make use of this functionality.
- Use DNS update mark this check box to confirm you want to use the update files detection method that eliminates data amount íê-åëÑÉêÉÇ-ÄÉíï ÉÉå í. É= . Ç~íÉ=Éê Éê-åÇ= . . = . . Éåí.
- **Require confirmation to close running applications item** (*switched on by default*) will help you make sure no currently running applications will be closed without your permission if required for the update process to be finalized;
- **Check computer time** mark this option to declare you wish to have notification displayed in case the computer time differs from the correct time more than specified number of hours.



Interest and the second	Update settings - Proxy		
📳 Virus Vault	Try connection using proxy and i	f it fails, connect directly	[
PUP Exceptions			
📳 Anti-Spam	Manual		
📳 Web Shield	Server:	Port:	3128
🔄 LinkScanner	Use PROXY authentication		
🖳 Scans		A ((
	Authentication type:	Any (derault)	
E-mail Scanner	Username:		
E Apti-Readtit	Password:		
Proxy	c 💽 Auto		
📕 Dial-up		Teheveek Evelevev	
📲 URL	- From browser		
	From script		
📳 Remote Administration	 Autodetect 		

The proxy server is a stand-alone server or a service running on a PC that guarantees safer connection to the Internet. According to the specified network rules you can then access the Internet either directly or via the proxy server; both possibilities can also be allowed at the same time. Then, in the first item of the **Update settings** - **Proxy** dialog you have to select from the combo box menu whether you want to:

• Use proxy

12 Drown

- Do not use proxy server
- Try connection using proxy and if it fails, connect directly default settings

If you select any option using proxy server, you will have to specify some further data. The server settings can be configured either manually or automatically.

Manual configuration



If you select manual configuration (check *the* **Manual** option to activate the respective dialog section) you have to specify the following items:

- Server specify the server's IP address or the name of the server
- **Port** specify the number of the port that enables Internet access (*by default, this number is set to 3128 but can be set differently if you are not sure, contact your network administrator*)

The proxy server can also have configured specific rules for each user. If your proxy server is set up this way, check the **Use PROXY authentication** option to verify that your user name and password are valid for connecting to the Internet via the proxy server.

Automatic configuration

If you select automatic configuration (*mark the* **Auto** *option to activate the respective dialog section*) then please select where the proxy configuration should be taken from:

- **From browser** the configuration will be read from your default internet browser
- **From script** the configuration will be read from a downloaded script with the function returning the proxy address
- Autodetect the configuration will be detected automatically directly from the proxy server



11.13.2Dial-up

불 Advanced AVG Settings		- 🗆 🗙
Appearance Ignore faulty conditions Virus Vaul PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Cs Schedules E-mail Scanner Resident Shield Anti-Rootkit Update Proxy Dial-up URL Manage Remote Administration	Update settings - Dial-up connection ✓ Use dial-up connections Automatically open this connection Ask before connection ✓ Close dial-up connection when finished	
Default	Cancel	Apply

All parameters optionally defined in the **Update settings - Dial-Up connection** dialog refer to the dial-up connection to the Internet. The dialog's fields are inactive until you check the **Use dial-up connections** option that activates the fields.

Specify whether you want to connect to the Internet automatically (*Automatically open this connection*) or you wish to confirm the connection manually every time (*Ask before connection*). For automatic connection you should further select whether the connection should be closed after the update is finished (*Close dial-up connection when finished*).



	Update settings - URL		
Yirus Vault Vurus Vault PUP Exceptions Anti-Spam Web Shield LinkScanner Scans Schedules E-mail Scanner Resident Shield Anti-Rootkit Update Proxy Dial-up URL Manage	Name Image: output Image: output	URL http://update.avg.com/softw/80/update/ http://backup.avg.cz/softw/80/update/	Edit Delete Move up
Remote Administration			

The **URL** dialog offers a list of Internet addresses from which the update files can be downloaded. The list and its items can be modified using the following control buttons:

- Add opens a dialog where you can specify a new URL to be added to the list
- Edit opens a dialog where you can edit the selected URL parameters
- Delete deletes the selected URL from the list
- Default returns to the default list of URLs

- Move Up moves the selected URL one position up in the list
- Move Down moves the selected URL one position down in the list



11.13.4Manage

The *Manage* dialog offers two options accessible via two buttons:

- **Delete temporary update files** press this button to delete all redundant update files from your hard disk (*by default, these files are being saved for 30 days*)
- **Revert virus database to previous version** press this button to delete the latest virus base version from your hard disk, and to return to the previously saved version (*new virus base version will be a part of the following update*)

11.14Remote Administration

불 Advanced AVG Settings			_ 🗆 🗙
Advanced AVG Settings	Remote Administration Server: Port: Login name: Password: Port for incoming messages:	4158 6051 Test connection	
Default	?	OK Cancel 🔗 A	Apply

The **Remote Administration** settings refer to connecting the AVG client station to the remote administration system. If you plan to connect the respective station to remote administration please specify the following parameters:

 Server - server name (or server IP address) where the AVG Admin Server is installed



- **Port** provide the number of the port on which the AVG client communicates with the AVG Admin Server (*port number 4158 is considered as default if you use this port number you do not have to specify it explicitly*)
 - **Login** if communication between the AVG client and the AVG Admin Server is defined as secured, provide your username ...
 - Password ... and your password
 - **Port for incoming messages** number of the port on which the AVG client accepts incoming messages from the AVG Admin Server

The **Test connection** button helps you to verify that all above stated data are valid and can be used to successfully connect to DataCenter.

Note: For a detailed description on remote administration please consult the AVG Network Edition documentation.



12. Firewall Settings

The *Firewall* configuration opens in a new window where in several dialogs can set up very advanced parameters of the component. The advanced configuration editing is only intended for experts and experienced users. To all other users we highly recommend to keep to the configuration set up via the *Firewall Configuration Wizard*.

12.1.General

🕌 Firewall settings	
General Security Areas and Adapters profiles Logs Profiles Hock All Standalone computer Computer in domain Computer on the move Small home or office network	General information This dialog allows you to change Firewall advanced settings, in particular, edit Firewall profiles and assign these to the network adapters or areas to take full advantage of automatic profile switching. Also, you can edit access rights here, and save the complete Firewall settings to the archive.
	Settings management Export Exports rules and configuration from all profiles into the backup files (e.g. for transferring to another computer). Import Imports rules and configuration for all profiles from backup file.
Help	OK Cancel Apply

In the *General information* you can export/import, or store *Firewall* configuration:

- **Export / Import** export the defined <u>Firewall</u> rules and settings to the back-up files, or on the other hand to import the entire back up file.
- **Archive** after every *Firewall* configuration change, the whole original configuration is saved into an archive. Archived configurations can be then accessed using the **Settings archive** button. If the archive is empty it means that no change has been done since the *Firewall* was installed. The maximum number of stored records is 10; if you try to save more records, the oldest records will be over-written.



12.2.Security

🕌 Firewall settings	
General Security Areas and Adapters profiles Cogs Profiles Allow all Block All Computer in domain Computer on the move Small home or office network	Security settings Permit settings modification to: Administrator Administrator and Power User All Users Show confirmation dialogs for: Administrator Administrator Administrator Administrator Administrator Administrator and Power User Show critical errors Show warnings Show information
Help	OK Cancel Apply

In the **Security settings** dialog you can define general rules of <u>**Firewall**</u>'s behavior regardless the selected profile:

- Permit settings modification to specify who is allowed to change the <u>Firewall</u>'s configuration
- Show confirmation dialog for specify to whom the confirmation dialogs (dialogs asking for decision in situation that is not covered by a defined <u>Firewall</u> rule) should be displayed

In both cases you can assign the specific right to one of the following user groups:

- Administrator controls the PC completely and has the right of assigning every user into groups with specifically defined authorities
- Administrator and Power User the administrator can assign any user into a specified group (Power User) and define authorities of the group members
- $_{\odot}$ **All Users** other users not assigned into any specific group
- Firewall information message decide what Firewall information


messages should be displayed - it is recommended to have the critical errors and warnings displayed at all times, and decide voluntarily about the information messages

12.3.Areas and Adapters Profiles

불 Firewall settings			
General Security Areas and Adapters profiles Logs Profiles Alews all	Adapters and network areas settings Disable area detection and automatic profile switch The following list contains adapters, areas and assigned profiles		×
 Block All Standalone computer Computer in domain 	Adapters and Areas Adapters and Areas All available adapters on the computer Adapters connected to safe networks Adapters RTL8168/8111 PCI-E Gigabit Ethernet NIC - Packet Scheduler Miniport	Assigned profile Cdit Are Unassigned Delete A	rea 📃 🗏
 € Computer on the move € E Small home or office network 	Wiware Virtual Ethernet Adapter for VMnet1 - AVG miniport driver Wiware Virtual Ethernet Adapter for VMnet8 - AVG miniport driver All network areas Av praci	Unassigned Unassigned Allow all Block All Standalone computer	
	Advanced settings Disable dialog for assigning new area	Computer in domain Computer on the move Small home or office network	
	Disable displaying information about areas and profile changes		
😢 Help			

In the **Adapters and network areas settings** dialogs you can edit setting related to assigning of defined profiles to specific adapters and referring and respective networks:

- **Disable area detection and automatic profile switch** one of the defined profiles can be assigned to each network interface type, respectively to each area. If you do not wish to define specific profiles, one common profile defined during the *Firewall Configuration Wizard* will be used. However, if you decide to distinguish profiles and assign them to specific adapters and areas, and later on for some reason you want to switch this arrangement temporarily, tick the *Disable area detection and automatic profile switch* option.
- List of adapters, areas and assigned profiles in this list you can find an overview of detected adapters and areas. To each of them you can assign a specific profile from the menu of defined profiles (all profiles are primarily defined within the Firewall Configuration Wizard, or later you can create new profiles in the Profiles dialog of the Firewall Settings). To open this menu, click the respective item in the list of adapters, and select the profile.



Advanced settings - ticking the respective option will deactivate the feature of displaying an information message

12.4.Logs

🔰 Firewall settings			_ 🗆 🔀
General Security Areas and Adapters profiles	Logs Event time	Application	Log action
Profiles Allow all Block All Computer in domain Computer on the move Small home or office network	 18.11.2008, 11:24:27 18.11.2008, 11:24:08 	C:\WINDOWS\SYSTEM32\LSASS.EXE C:\WINDOWS\SYSTEM32\LSASS.EXE	Block
2 Help		ок с	ancel Apply

The **Logs** dialog allows you to review the list of all logged <u>Firewall</u> actions and events with a detailed description of relevant parameters:

- Event time exact date and time when the event was encountered
- **Application** name of the process to which the logged event refers
- Action type of action performed

The following control buttons are available:

- *Help* opens the dialog related help files.
- **Show details** if you find the provided parameters insufficient, and want to see more, use this button to switch to the advanced log file overview with additional information (on user, PID, direction, protocol, remote/local port, remote/local IP address).



- Refresh list all logged parameters can be arranged according to the selected attribute: chronologically (*dates*) or alphabetically (*other columns*) just click the respective column header. Use the Refresh list button to update the currently displayed information.
 - *Empty list* delete all entries in the chart.

12.5.Profiles

In the **Profiles' settings** dialog you can find a list of all profiles available.

🕌 Firewall settings		X
 General Security Areas and Adapters profiles Logs Profiles Allow all Block All Standalone computer Computer in domain Computer on the move 	Profiles' settings Firewall profile is a set of security rules applied to the computer based on how it is connected to the Internet (through a corporate network, independently, or in variable manner). Within a profile, each application can be assigned rules related to the network communication Description of the currently active profile Allow all communication to and from the computer	<
⊕ 📳 Small home or office network	Profile name Activate profile Allow all Duplicate profile Block All Duplicate profile Standalone computer Rename profile Computer in domain Delete profile Small home or office network Exception	III
	Import profile	
	"Allow all" is a basic system profile. When activated, it allows all communication to and from any network, on any port. No communication is blocked, as if the Firewall was deactivated.	
	OK Cancel Apply	:

All other then system <u>profiles</u> can then be edited right in this dialog using the following control buttons:

• Activate profile - this button sets the selected profile as active, which means



the selected profile configuration will be used by *Firewall* to control the network traffic

- **Duplicate profile** creates an identical copy of the selected profile; later you can edit and rename the copy to create a new profile based on the duplicated original one
- Rename profile allows you to define a new new for a selected profile
- Delete profile deletes the selected profile from the list
- **Export profile** records the selected profile's configuration into a file that will be saved for possible further use
- **Import profile** configures the selected profile's settings based on the data exported from the backup configuration file
- Help opens the dialog related help file

In the bottom section of the dialog please find the description of a profile that is currently selected in the above list.

Based on the number of defined profiles that are mentioned in the list within the **Profile** dialog, the left navigation menu structure will change accordingly. Each defined profile creates a specific branch under the **Profile** item. Specific profiles can then be edited in the following dialogs (*that are identical for all profiles*):



🕌 Firewall settings	
 General Security Areas and Adapters profiles Logs Profiles Allow all Block All Standalone computer Computer in domain Defined adapters Defined networks Defined services Applications System services Computer on the move Small home or office network 	Profile information The navigation tree (left) displays all currently defined profiles. System profiles "Allow all" and "Block all" are always present. Custom profiles can be generated through the Firewall configuration wizard. Any listed profile can be edited here; click the relevant plus symbol to expand and display detailed setting options. Enable Virtual Machines Bridged networking Gaming mode settings Disable Firewall notification when playing games Do this action when gaming mode is enabled: Allow for all
Help	OK Cancel Apply

12.5.1.Profile Information

The **Profile information** dialog is the first dialog of a section where you can edit configuration of each profile in separate dialogs referring to specific parameters of the profile.

Enable Virtual Machines Bridget networking - tick this item to allow virtual machines in WMware to connect directly to the network

Gaming mode settings

In the **Gaming mode settings** section you can decide and confirm by ticking the respective item whether you want to have *Firewall* information messages displayed even while a full-screen application is running on your computer (*typically these are games, but applies to any full-screen applications, e.g. PPT presentations*). Since the information messages can be somewhat disruptive, the feature is switched off by default.

If you tick the **Enable Firewall notifications when playing games** item, in the roll-down menu then select what action is to be taken in case a new application with no rules specified yet tries to communicate over the network (*applications that would normally result in an ask dialog*) all these applications can be either allowed or blocked.



🕌 Firewall settings				
 General Security Areas and Adapters profiles Logs Profiles Allow all Block All Standalone computer Computer in domain Defined adapters Defined anetworks Defined networks Defined services System services Computer on the move Small home or office network 	Defined adapters Adapters All available adapters on the computer Adapters Adapters <td< td=""><td>Interface safety Safe Safe Safe Unsafe Unsafe</td><td>IP address range 192.168.195.68/24</td><td>Mark as Safe</td></td<>	Interface safety Safe Safe Safe Unsafe Unsafe	IP address range 192.168.195.68/24	Mark as Safe
😢 Help		ОК	Cancel	Apply

12.5.2. Defined Adapters

The **Defined adapters** dialog offers a list of all adapters that were detected on your computer. A specific network refers to each adapter - for list of all networks consult the **Defined Networks** dialog.

The following information is provided on every detected adapter:

- Adapters name list of all detected adapters that your computer uses to connect to specific networks
- **Interface safety** by default, all adapters and are considered unsafe, and only if you are sure the respective adapter (and the respective network) is safe, you can assign it so (*click the list item referring to the respective adapter and select Safe from the context menu, or use the* **Mark as safe** *button*) - all safe adapters and respective networks will then be included into the group of those that the application can communicate over with the application rule set to <u>Allow for safe</u>
- **IP** address range each network (referring to a specific adapter) range will be detected automatically and specified in the form of IP addresses range



불 Firewall settings				_ 🗆 🔀
General Security Areas and Adapters profiles Logs Profiles Block All Block All Computer in domain Computer in domain Defined adapters Defined services Computer solutions System services System services Small home or office network	Defined networks Networks All Networks Safe networks Classfe All IPv4 Networks All IPv4 Networks All IPv6 Networks Vou can add, edit, or delete ret	Network safety	IP address range 0.0.0.0 - 255.255.255.255, :: - ffff:ff 0.0.0.0 - 255.255.255.255, :: - ffff:ff 0.0.0.0 - 255.255.255 :: - ffff:ffff:ffff:ffff:ffff:ffff:ffff	Add network Edit network Delete network Mark as Safe
e Help			OK Cancel	Apply

12.5.3.Defined Networks

The **Defined networks** dialog offers a list of all networks that your computer is connected to. Each network refers to a specific adapter - for list of all adapters see the **<u>Defined Adapters</u>** dialog.

The following information is provided on every detected network:

- Networks name list of all networks that the computer is connected to
- **Network safety** by default, all networks are considered unsafe, and only if you are sure the respective network is safe, you can assign it so (*click the list item referring to the respective network and select Safe from the context menu*) all safe networks will then be included into the group of those that the application can communicate over with the application rule set to <u>Allow</u> for safe
- **IP address range** each network will be detected automatically and specified in the form of IP addresses range

Control buttons

• **Add network** - opens the **Network properties** dialog window where you can edit parameters of the newly defined network:



Network properties		\mathbf{X}
Network properties		
Network name		
New network		
Network description		
Network is safe		
IP address range		Add IP
		Edit IP
		Editii
		Delete IP
Advanced IPs range representation		
		Verify
() Help	ОК	Cancel

Within this dialog, you can specify the **Network name**, provide the **Network description** and possibly assign the network as safe. The new network can be either defined manually in a standalone dialog opened via the **Add IP** button (alternatively **Edit IP** / **Delete IP**), within this dialog you can specify the network by providing its IP range or mask.

For large number of networks that should be defined as parts of the newly created network you can use the option of **Advance IP range representation**: enter the list of all networks into the respective text field (*any standard format is supported*) and press the **Verify** button to make sure the format can be recognized. Then press **OK** to confirm and save the data.

- *Edit network* opens the *Network properties* dialog window (*see above*) where you can edit parameters of an already defined network (*the dialog is identical with the dialog for adding new network, see the description in the previous paragraph*)
- Delete network removes the note of a selected network from the list of



networks

- **Mark as safe** by default, all networks are considered unsafe, and only if you are sure the respective network is safe, you can use this button to assign it so
- Help opens the dialog related help file

12.5.4.Defined Services

👬 Firewall settings			
📳 General	Defined services		
Areas and Adapters profiles Logs Profiles Allow all Block All Computer in domain Computer in domain Defined adapters Defined services Explications	Service name All Traffic ActiveSync AH_Proto (Authentication Header) Destination_Unreachable DHCP DNS DNS_Server ECHO_IN ECHO_OUT ESP_Proto FTP GRE_Proto HTTD You can add, edit, or delete service definition	Ports preview ▲ P: 0: L: 0 - 65535 R: 0 - 65535 P: 6: L: 990 R: 0 - 65535 P: 6: P: 51: L: 0 - 65535 R: 0 - 65535 P: 17: L: 3 R: 0 - 65535 P: 58: P: 17: L: 0 - 65535 R: 67; P: 17 P: 17: L: 0 - 65535 R: 67; P: 17 P: 17: L: 0 - 65535 R: 63; P: 17: L: 8 R: 0 - 65535; P: 17: L: 8 R: 0 - 65535; P: 11: L: 8 R: 0 - 65535; P: 11: L: 8 R: 0 - 65535; P: 12: L: 8 R: 0 - 65535; P: 11: L: 8 R: 0 - 65535; P: 12: L: 8 R: 0 - 65535; P: 12: L: 8 R: 0 - 65535; P: 14: L: 0 - 65535 R: 21; P: 6; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553; P: 47: L: 0 - 65535 R: 0 - 6553;	Add service E dit service Delete service
Help		OK Cancel	Apply

The **Defined services** dialog opens a list of all services defined for the application in the default configuration, and services that have already been defined by the user. The dialog is divided into two columns:

- Service name provides the name of the service
- **Ports preview** arrows assign incoming/outgoing communication; further provided you will find the number or name of the protocol used (P), and the number or range of local (L) / remote (R) ports used

You can add, edit, and/or delete specific services.

Control buttons



Add service - opens a new Service items editor dialog window where you define the parameters of the service that is being added:

dervice	items editor			
Service item	name			
New service				ок
Service item	description			Cancel
Service items	; list			
Direction	Protocol number	Local ports	Remote ports	Add
				E dit
				Delete
<	11	1	>	😢 Help

Within the dialog you can specify **Service item name** and provide a brief **Service item description**. In the **Service items list** section you can then add (*and also edit or delete*) service items by specifying the following parameters:

- Direction incoming, outgoing, both ways
- Protocol number protocol type (select from the menu)
- *Local ports* local ports list of ranges
- o *Remote ports* remote ports list of ranges
- *Edit service* opens the *Service items editor* dialog (*see above*) where you can edit parameters of an already defined service (*the dialog is identical with the dialog for adding new service, see the description in the previous paragraph*)
- Delete service removes the note of a selected service from the list
- Help opens the dialog related help file



12.5.5.Applications

🕌 Firewall settings	
General Security Areas and Adapters profiles Cogs Profiles Standalone computer Computer in domain Defined adapters Defined adapters Defined networks Computer on the move System services System services Small home or office network	Applications information The list displays applications installed on this computer that might need to communicate over the network. Each application can be assigned a specific rule for communication over networks: allow / block / ask for permission. You can apply advanced rules.
	Application name Add Priority Application Rules Edit Application Layer Gateway service Edit AVG Admin Console Edit AVG Admin Server Deployment Wizard Edit AVG Admin Server Deployment Wizard Edit AVG Admin Server Monitor AVG Admin Server Monitor AVG Admin Station Remover AVG Admin Station Remover AVG Computer scanner AVG Computer scanner AVG Computer scanner AVG Computer scanner
Help	OK Cancel Apply

In the *Applications information* dialog you can find an overview of all applications communicating over the network that were detected on your computer either during the *Firewall Configuration Wizard*'s search within the *Scan for Internet Applications* dialog, or at any time later. The list can be edited using the following control buttons:

- Add opens the dialog for defining new application's rule set
- Edit opens the dialog for editing of an existing application's rule set
- Delete removes the selected application from the list
- Help opens the dialog related help file



🧯 Firewall settings				_ 🗆 🔀
Remote Desktor RunDLL32	Page actions		Delete this rule	
Skype Skype Extras M Felnet Tracert Userinit Logon A Various System Windows Explor Windows Genuit	Application basic information Name Description Path Application action	New application		
WMI Provider H New application Other Applicatic System services Computer on the move Small home or office netwo	Log rule occurrences			
		OK	Cancel	Apply

The dialog for defining new application's rule set opens using the **Add** button from the **<u>Applications</u>** dialog within the <u>**Firewall Settings**</u>:

Within this dialog you can define:

- **Application basic information** name of application, its brief description and a path to its location on the disk
- **Application action** from the drop-down menu select a rule that should be applied to the application's behavior:
 - Advanced settings this option allows you to edit the rule set in details in the bottom part of this dialog; for description of this section please see the <u>Edit Application</u> chapter
 - Allow for all any communication attempt of the application will be allowed
 - Allow for safe the application will only be allowed to communicate over safe networks (for instance, communication to the protected company network will be allowed while communication to the Internet will be blocked); for an overview and description of safe networks please see the <u>Networks</u> dialog



- Ask any time th application attempts to communicate over the network, you will be asked to decide whether the communication should be allowed or blocked
- > **Block** all communication attempts of the application will be blocked
- **Log rule occurrences** tick this option to confirm you wish to have logged all *Firewall* actions regarding the application that you have been configuring the rule set for. The respective log entries can then be found in the *Logs* dialog.



The dialog for editing an existing application's rule set opens using the *Edit* button from the *<u>Applications</u>* dialog in the *<u>Firewall Settings</u>*:

🕌 Firewall settings			X
Applications Application Application Application Application Application Application Application Application	Page actions	Delete this rule	^
AVG Admin Server	Application basic information - Name	Priority Application Rules	
AVG Admin Server	Description Path	Preferential to rules of specific applications SYSTEM	
AVG Alert Manage AVG Computer sca AVG Computer sca AVG Computer sca AVG Computer sca AVG Computer sca AVG Diagnostics 8 AVG Firewall	Application action Advanced settings Log rule occurrences Application detail rules		
AVG Network Inst. AVG Personal E-m. AVG Personal E-m. AVG Prevalence R AVG Scan Action E AVG Scan Action E AVG Scan Action E AVG Update AVG Update down AVG Update down AVG User Interfac AVG WatchDog AVG Web Shield	Details	Add Remove Move up Move down	III
AVG web Shield AVG web Shield (f AVG web Shield (f Dr. Watson Windc Firefox FTP ICQ Local Security Aut Microsoft Feeds S' MS Internet Explo MS Registration W MS Sync Manager Office Source Eng Outlook Express ping Prov Cle Marking	Defined services Defined n Service name Intraffic AH_Proto (Authentic ActiveSync DHCP DNS DNS_Server Destination_Unreach ECHO_IN ECHO_OUT ESP_Proto FTP GRE_Proto Intraffic	Inetworks Defined adapters Ports preview	
1 Help		OK Cancel Apply	

Within this dialog you can edit all application's parameters:

• Application basic information - name of application, its brief description



and a path to its location on the disk

- **Application action** from the drop-down menu select a rule that should be applied to the application's behavior:
 - Advanced settings this option allows you to edit the rule set in details in the bottom part of this dialog
 - Allow for all any communication attempt of the application will be allowed
 - Allow for safe the application will only be allowed to communicate over safe networks (for instance, communication to the protected company network will be allowed while communication to the Internet will be blocked); for an overview and description of safe networks please see the <u>Networks</u> dialog
 - Ask any time th application attempts to communicate over the network, you will be asked to decide whether the communication should be allowed or blocked
 - > Block all communication attempts of the application will be blocked
- **Log rule occurrences** tick this option to confirm you wish to have logged all *Firewall* actions regarding the application that you have been configuring the rule set for. The respective log entries can then be found in the *Logs* dialog.
- **Application detail rules** this section opens for editing only if you have previously selected the option of **Advanced settings** from the **Application action** roll-down menu. All detail settings (listed in the **Details** column) can be edited using these control buttons:
 - Add use the button to create a new detailed rule for a specific application. In the **Details** tab a new entry appears, and you will have to specify its parameters by selecting the respective networks that the application can communicate with (**Networks** tab), adapters that the application can use (**Adapters** tab), and services the application can employ (**Service name** tab).
 - > Remove removes the selected entry on a detail rule from the list
 - Move up / Move down detail rules are ordered based on their priority. If you want to change the rule's priority, use the Move up and Move down buttons to arrange the detailed settings as needed.



Each detailed settings further specifies what **Defined services / Defined** networks / Defined adapters will be used.

12.5.6.System Services

Any editing within the System services and protocols dialog is recommended to experienced users only!

불 Firewall settings	
General Security Areas and Adapters profiles Logs Profiles Allow all Standalone computer Computer in domain Computer in domain Computer in domain Defined adapters Defined adapters Defined retworks Defined retworks Standalone computer Computer in domain Standalone computer Standalone computer Computer in domain Standalone computer Standalone computer Computer in domain Standalone computer Standalone computer Computer in domain Standalone computer Standalone computer Computer on the move Standalone computer on the move Standalone computer in the move	System services and protocols The list displays most of Windows system services. System services can be assigned simple rules for network communication only: allow or block. List of system services and protocols System services and protocols System services and protocols Add Destination unreachable OHCP Client Delete ESP protocol Log unknown incoming traffic Log unknown outgoing traffic
2 Help	OK Cancel Apply

The **System services and protocols** dialog opens an overview of system services and protocols communicating over the network. Underneath the list you can find two options: check/uncheck them to confirm you want to <u>have logged</u> all unknown traffic in both directions (*incoming or outgoing*).

Control buttons

• **Add / Edit** - both buttons open the same dialog in where you can edit the system service parameters. The **Add** button opens an empty dialog and in the basic mode (*no advanced settings section; but this section can be opened by selecting the advanced settings for the application action*); the **Edit** button opens the same dialog with already entered data referring to the selected system service:



🕌 Firewall settings	
Areas and Adapters profiles	Page actions
Profiles Allow all Block All Standalone computer Computer in domain Defined adapters	System rule basic information Name DHCP Client Description The Dynamic Host Configuration Protocol - dynamically allocates network ad
Defined networks Defined services Applications System services AH protocol (Au	System rule details Allow for all Log rule occurrences
	System rule action Details Add 1 DHCP traffic
GRE protocol	Move up
ICMPv6 Multica ICMPv6 Neighb	Defined services Defined networks Defined adapters
ICMPv6 Router	Service name Ports preview DHCP P: 17: L: 0 - 65535 R: 67; P: 17: L: 68 R: 0 - 65535;
L2TP VPN	Add service Edit service
PPTP VPN	

- Application basic information name of application and its brief description
- Application action from the drop-down menu select a rule that should be applied to the system service's behavior (*compared to applications, there are only three actions available for the system services*):
 - Block all communication attempts of the system service will be blocked
 - Allow for safe the system service will only be allowed to communicate over safe networks (for instance, communication to the protected company network will be allowed while communication to the Internet will be blocked); for an overview and description of safe networks please see the <u>Networks</u> dialog



- Allow for all any communication attempt of the system service will be allowed
- Log rule occurrences tick this option to confirm you wish to have logged all <u>Firewall</u> actions regarding the system service that you have been configuring the rule set for. The respective log entries can then be found in the <u>Logs</u> dialog.
- Application detail rules for each system service you can further specify detailed rules within the Application detail rules section. All detail settings (listed in the Details tab) can be edited using these control buttons:
 - Add use the button to create a new detailed rule for a specific system service. In the **Details** tab a new entry appears, and you will have to specify its parameters by selecting the respective networks that the system service can communicate with (**Networks** tab), adapters that the system service can use (**Adapters** tab), and services the system service can employ (**Service name** tab).
 - > **Remove** removes the selected entry on a detail rule from the list
 - Move up / Move down detail rules are ordered based on their priority. If you want to change the rule's priority, use the Move up and Move down buttons to arrange the detailed settings as needed.

Each detailed settings further specifies what **Defined services / Defined networks / Defined adapters** will be used.

- **Delete** removes the selected entry on a system services from the list above
- Help opens the dialog related help file



13. AVG Scanning

Scanning is a crucial part of **AVG 8.5 Internet Security** functionality. You can run on-demand tests or <u>schedule them to run periodically</u> at convenient times.

13.1.Scanning Interface

🛃 AVG Internet Security Network Edition 📃 🗆 🔯			
File Components History Tools H	lp		
AVG Internet Security	You are protected. All security features are working correctly and are up to date.		
	Sean for threate		
Overview	Scartor meats		
Q Computer scanner	Scan whole computer Change scan settings Change scan settings Change scan settings		
📝 Update now			
	Schedule scans		
	Name Next scheduled run Scheduled cran 6, 11, 2008, 23:00:00		
Statistics Last scar: 5.11.08, 23.00 Last update: 6.11.08, 10.04 Virus DB: 270.9.01770 AVG version: 8.0.209	Add scan schedule Edit scan schedule		
License expires: Not activated	Scan history View Virus Vault		

The AVG scanning interface is accessible via the *Computer Scanner* <u>quick link</u>. Click this link to switch to the *Scan for threats* dialog. In this dialog you will find the following:

- overview of <u>predefined scans</u> two types of test (defined by the software vendor) are ready to be used immediately on demand or scheduled;
- <u>scan scheduling</u> section where you can define new tests and create new schedules as needed.

Control buttons

Control buttons available within the testing interface are the following:

 Scan history - displays the <u>Scan results overview</u> dialog with the entire history of scanning



View Virus Vault - opens a new window with the <u>Virus Vault</u> - a space where detected infections are quarantined

13.2.Predefined Scans

One of the main features of AVG is on-demand scanning. On-demand tests are designed to scan various parts of your computer whenever suspicion of possible virus infection arises. Anyway, it is strongly recommended to carry out such tests regularly even if you think that no virus can be found on your computer.

In the **AVG 8.5 Internet Security** you will find two types of scanning predefined by the software vendor:

13.2.1.Scan Whole Computer

Scan whole computer - scans your entire computer for possible infections and/or potentially unwanted programs. This test will scan all hard drives of your computer, will detect and heal any virus found, or remove the detected infection to the <u>Virus</u> <u>Vault</u>. Scanning of the whole of your computer should be scheduled on a workstation at least once a week.

Scan launch

The **Scan of a whole computer** can be launched directly from the <u>scanning interface</u> by clicking on the scan's icon. No further specific settings have to be configured for this type of scan, the scanning will start immediately within the **Scan is running** dialog (*see screenshot*). The scanning can be temporarily interrupted (**Pause**) or canceled (**Cancel**) if needed.



AVG Internet Security Netwo File Components History Tools He AVG Internet Security	rk Edition #p You are protected. All security features are working correctly and are up to date.	
Image: Computer scanner Image: Computer scanner	Scan is running File Result/Infect Image: Scan is running Processes Current boject: C:\WINDOW5\system32\ShimEng.dll Additional scan settings Pause	on

Scan configuration editing

You have the option of editing the predefined default settings of the *Scan of the whole computer*. Press the *Change scan settings* link to get to the *Change scan settings for Scan whole computer* dialog. *It is recommended to keep to the default settings unless you have a valid reason to change them!*



File Component	et Security Network Edition s History Tools Help /G ernet Security	You are protected. All security features are worki	ng correctly and are up to	date.
 Overv Comp Updat 	riew Autom v Autom v Scan F v Scan F v Scan fi v Scan fi	e scan settings for Sca atically heal/remove infections otentially Unwanted Programs and Sj or Tracking Cookies side archives autistics	n whole computer	
	♥ Scan s Scan f ♥ Scan i Scan i Scan proc Scan proc	ystem environment or rootkiks in media files only ess priority Automatic scan		
Statistics Last scann & Last update: & Virus DB: AVG version & License expires Show	Set addition Set additional sc 11.08, 11:46 Additional sc 11.08, 10:04 30.209 : Not activated Image: Compare the science of the science o	al scan reports an settings refault	Start s	Save the current settings

- **Scanning parameters** in the list of scanning parameters you can switch on/off specific parameters as needed. By default, most of the parameters are switched on and these will be used automatically during scanning.
- Scan process priority you can use the slider to change the scanning process priority. By default, the priority is set to medium level (*Automatic scan*) that optimizes the scanning process speed and the use of system resources. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).
- Set additional scan reports the link opens a new Scan Reports dialog where you can select what types of possible findings should be reported:

📕 Scan reports 🛛 🔀		
Scan reports		
Report password protected archives		
Report password protected documents		
Report locked files		
Report files containing macro		
Report hidden extensions		
OK Cancel		



 Additional scan settings - the link opens a new Computer shutdown options dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (Shutdown computer upon scan completion), a new option activates that allows the computer to shut down even if it is currently locked (Force shutdown is computer is locked).

📕 Additional scan settings 🛛 🔀		
Computer shutdown options		
Shutdown computer upon scan completion		
Force shutdown if computer is locked		
0K Cancel		

Warning: These scan settings are identical to the parameters of a newly defined scan - as described in the chapter <u>AVG Scanning / Scan scheduling / How to Scan</u>.

Should you decide to change the default configuration of the **Scan the whole computer** you can then save your new setting as the default configuration to be used for all further scans of the whole computer.

13.2.2.Scan Specific Files or Folders

Scan specific files or folders - scans only those areas of your computer that you have selected to be scanned (selected folders, hard disks, floppy discs, CDs, etc.). The scanning progress in case of virus detection and its treatment is the same as with the scan of the whole computer: any virus found is healed or removed to the <u>Virus</u> <u>Vault</u>. Specific files or folders scanning can be used to set up your own tests and their scheduling based on your needs.

Scan launch

The **Scan of specific files or folders** can be launched directly from the <u>scanning</u> <u>interface</u> by clicking on the scan's icon. A new dialog called **Select specific files or folders for scanning** opens. In the tree structure of your computer select those folders you want to have scanned. The path to each selected folder will generate automatically and appear in the text box in the upper part of this dialog.

There is also a possibility of having a specific folder scanned while all its subfolders are excluded from this scanning; to do that write a minus sign "-" in front of the automatically generated path (*see screenshot*). To exclude the entire folder from



scanning use the "!" parameter.

Finally, to launch the scanning, press the **Start scan** button; the scanning process itself is basically identical to the <u>scan of a whole computer</u>.

🛃 AVG Internet Security Network Edition 📃 🗆 🔀		
File Components History Tools He	ql	
AVG Internet Security	You are protected. All security features are working correctly and are up to date.	
	Select specific files or folders for scanning	
Overview		~
Q Computer scanner	Computer	
📝 Update now		
Statistics Last scan: 6,11,08,11:46 Last update: 6,11,08,10,04 Virus DB: 270,9,0/1770 AVG version: 8,0209 License expires: Not activated	Port Port	
Show notification	Automatic scan Start scan	Cancel

Scan configuration editing

You have the option of editing the predefined default settings of the *Scan of specific files or folders*. Press the *Change scan settings* link to get to the *Change scan settings for Scan of specific files or folders* dialog. *It is recommended to keep to the default settings unless you have a valid reason to change them!*



AVG Internet Security Network	ork Edition
File Components History Tools F	You are protected.
Internet Security	All security features are working correctly and are up to date.
Overview	Change scan settings for Scan specific files of folders
Computer scanner	Addimitationary rearrentiate in each of the end of
Update now	Scan inside archives
	Scan system environment
	Scan infectable files only
	Scan media files
	Automatic scan
Statistics	Set additional scan reports
Last scan: 6.11.08, 11:46 Last update: 6.11.08, 10:04	Additional scan settings
Virus DB: 270.9.0/1770 AVG version: 8.0.209	Save the current settings
License expires: Not activated	
Show notification	Default Cancel

- **Scanning parameters** in the list of scanning parameters you can switch on/off specific parameters as needed (*for detailed description of this settings please consult chapter <u>AVG Advanced Settings / Scans / Scan Specific Files or Folders</u>).*
- Scan process priority you can use the slider to change the scanning process priority. By default, the priority is set to medium level (*Automatic scan*) that optimizes the scanning process speed and the use of system resources. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).
- **Set additional scan reports** the link opens a new **Scan Reports** dialog where you can select what types of possible findings should be reported:

📕 Scan reports 🛛 🔀		
Scan reports		
Report password protected archives		
Report password protected documents		
Report locked files		
Report files containing macro		
Report hidden extensions		
OK Cancel		



 Additional scan settings - the link opens a new Computer shutdown options dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (Shutdown computer upon scan completion), a new option activates that allows the computer to shut down even if it is currently locked (Force shutdown is computer is locked).

Additional scan settings	X	
Computer shutdown options	_	
Shutdown computer upon scan completion		
Force shutdown if computer is locked		
OK Canad		

Warning: These scan settings are identical to the parameters of a newly defined scan - as described in the chapter <u>AVG Scanning / Scan scheduling / How to Scan</u>.

Should you decide to change the default configuration of the **Scan specific files or folders** you can then save your new setting as the default configuration to be used for all further scans of specific files or folders. Also, this configuration will be used as a template for all of your newly scheduled scans (<u>all customized scans are based on</u> <u>the current configuration of the Scan of selected files or folders</u>).

13.3.Scanning in Windows Explorer

Besides the pre-defined scans launched for the entire computer or its selected areas, AVG also offers the option of quick scanning of a specific object directly in the Windows Explorer environment. If you want to open an unknown file and you cannot be sure of its content, you may want to have it checked on demand. Follow these steps:





- Within Windows Explorer highlight the file (or folder) you want to check
- Right-click your mouse over the object to open the context menu
- Select the Scan with AVG option to have the file scanned with AVG

13.4.Command Line Scanning

Within **AVG 8.5 Internet Security** there is the option of running the scan from the command line. You can use this option for instance on servers, or when creating a batch script to be launched automatically after the computer boot. From the command line, you can launch the scanning with most parameters as offered in AVG graphical user interface.

To launch AVG scan from the command line, run the following command within the folder where AVG is installed:

- avgscanx for 32 bits OS
- avgscana for 64 bits OS

Syntax of the command



The syntax of the command follows:

- avgscanx /parameter ... e.g. avgscanx /comp for scanning the whole computer
- **avgscanx /parameter /parameter** .. with multiple parameters these should be lined in a row and separated by a space and a slash character
- if a parameters requires specific value to be provided (e.g. the /scan parameter that requires information on what are the selected areas of your computer that are to be scanned, and you have to provide an exact path to the selected section), the values are divided by commas, for instance: avgscanx /scan=C:\,D:\

Scanning parameters

To display a complete overview of available parameters, type the respective command together with the parameter /? or /HELP (e.g. **avgscanx /?**). The only obligatory parameter is /SCAN to specify what areas of the computer should be scanned. For a more detailed explanation of the options, see the <u>command line</u> <u>parameters overview</u>.

To run the scan press *Enter*. During scanning you can stop the process by *Ctrl+C* or *Ctrl+Pause*.

CMD scanning launched from graphic interface

When you run your computer in Windows Safe Mode, there is also a possibility to launch the command line scan from the graphic user interface. The scan itself will be launched from the command line, the **Command Line Composer** dialog only allows you to specify most scanning parameters in the comfortable graphic interface.

Since this dialog is only accessible within the Windows Safe Mode, for detailed description of this dialog please consult the help file opened directly from the dialog.

13.4.1.CMD Scan Parameters

Following please find a list of all parameters available for the command line scanning:

• /SCAN Scan specific files or folders /SCAN=path;path (e.g. /SCAN=C:\;D:\)



• /COMP	Scan whole computer
• /HEUR	Use <u>heuristic analyse</u>
• /EXCLUDE	Exclude path or files from scan
• /@	Command file /file name/
• /EXT	Scan these extensions /for example EXT=EXE,DLL/
• /NOEXT	Do not scan these extensions /for example NOEXT=JPG/
• /ARC	Scan archives
• /CLEAN	Clean automatically
• /TRASH	Move infected files to the Virus Vault
• / QT Qui	ck test
• /MACROW	Report macros
• /PWDW	Report password-protected files
• /IGNLOCKED	Ignore locked files
• /REPORT	Report to file /file name/
• /REPAPPEND	Append to the report file
• /REPOK	Report uninfected files as OK
• /NOBREAK	Do not allow CTRL-BREAK to abort
• <i>/BOOT</i>	Enable MBR/BOOT check
• /PROC	Scan active processes
• /PUP	Report "Potentially unwanted programs"
• /REG	Scan registry
• /COO	Scan cookies
• /?	Display help on this topic



- /HELP Display help on this topic
 - **/PRIORITY** Set scan priority /Low, Auto, High/ (see <u>Advanced</u> <u>settings / Scans</u>)
 - /SHUTDOWN Shutdown computer upon scan completion
 - /FORCESHUTDOWN Force computer shutdown upon scan completion
 - **/ADS** Scan Alternate Data Streams (NTFS only)

13.5.Scan Scheduling

With **AVG 8.5 Internet Security** you can run scanning on demand (for instance when you suspect an infection has been dragged to your computer) or based on a scheduled plan. It is highly recommended to run the scans based on a schedule: this way you can make sure your computer is protected from any possibility of getting infected, and you will not have to worry about if and when to launch the scan.

You should launch the <u>Scan whole computer</u> regularly, at least once a week. However, if possible, launch the scan of your entire computer daily - as set up in the scan schedule default configuration. If the computer is "always on" then you can schedule scans out of working hours. If the computer is sometimes switched off, then schedule scans to occur <u>on a computer start-up when the task has been missed</u>.

To create new scan schedules, see the <u>AVG scanning interface</u> and find the bottom section called **Schedule scans**:



🛃 AVG Internet Security Netwo	rk Edition
File Components History Tools H	elp
AVG Internet Security	You are protected. All security features are working correctly and are up to date.
0verview	Scan for threats
Computer scanner	Scan whole computer Change scan settings Scan specific files or folders Change scan settings
Update now	Schedule scans
	Name Next scheduled run
	Scheduled scan 6.11.2008, 23:00:00
Statistics Last scan: 5.11.08, 23.00 Last update: 6.11.08, 10.04 Virus DB: 270.3.0/1770 AVG version: 8.0.209 License expires: Not activated	Add scan schedule Edit scan schedule @Delete scan schedule
× Show notification	Scan history View Virus Vault

Control buttons for the scan scheduling

Within the editing section you can find the following control buttons:

- Add scan schedule the button opens the Settings for scheduled scan dialog, <u>Schedule settings</u> tab. In this dialog you can specify the parameters of the newly defined test.
- *Edit scan schedule* this button can only be used if you have already previously selected an existing test from the list of scheduled tests. In that case the button appears as active and you can click it to switch to the *Settings for scheduled scan* dialog, *Schedule settings* tab. Parameters of the selected test are already specified in here and can be edited.
- **Delete scan schedule** this button is also active if you have already previously selected an existing test from the list of scheduled tests. This test can then be deleted from the list by pressing the control button. However, you can only remove your own tests; the **Whole computer scan schedule** pre-defined within the default settings can never be deleted.



13.5.1.Schedule Settings

If you wish to schedule a new test and its regular launch, enter the **Settings for scheduled test** dialog. The dialog is divided into three tabs: **Schedule settings** see picture below (the default tab that you will be automatically redirected to), <u>How</u> <u>to scan</u> and <u>What to scan</u>.

불 AVG Internet Security Netwo	rk Edition		
File Components History Tools He	łp		
AVG Internet Security	You are protected. All security features are	working correctly and are up to date.	
	Settings for scheduled sc	an	
0verview	Schedule settings How to scan What t	o scan	
Q Computer scanner	🗹 Enable this task		
📝 Update now	Name	New scheduled task	
	Schedule running		
	ORun every:	1 Hour(s)	
	Run at a specific time interval:	Every day 23:00	
Statistics	Action based:	On computer startup	
Last scan: 6.11.08, 11:46 Last update: 6.11.08, 10:04	Advanced schedule options		
Virus DB: 270.9.0/1770	Run on computer startup if task has been missed		
License expires: Not activated	Run even if computer is in low power mode		
		💓 Save Cancel	
Show notification			

On the **Schedule settings** tab you can first check/uncheck the **Enable this task** item to simply deactivate the scheduled test temporarily, and switch it on again as the need arises.

Next, give a name to the scan you are about to create and schedule. Type the name into the text field by the **Name** item. Try to use brief, descriptive and apt names for scans to make it easier to later recognize the scan from others.

Example: It is not appropriate to call the scan by the name of "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System areas scan" etc. Also it is not necessary to specify in the scan's name whether it is the scan of the whole of the computer or just a scan of selected files or folders - your own scans will always be a specific version of the scan of selected files or folders.

In this dialog you can further define the following parameters of the scan:

• Schedule running - specify the time intervals for the newly scheduled scan



launch. The timing can either be defined by the repeated scan launch after a certain period of time (*Run every* ...) or by defining an exact date and time (*Run at specific time* ...), or possibly by defining an event that the scan launch should be associated with (*Action based on computer startup*).

• **Advanced schedule options** - this section allows you to define under which conditions the scan should/should not be launched if the computer is in low power mode or switched off completely.

Control buttons of the Settings for scheduled scan dialog

There are two control buttons available on all three tabs of the **Settings for scheduled scan** dialog (**Schedule settings**, <u>How to scan</u> and <u>What to scan</u>) and these have the same functionality no matter on which tab you currently are:

- **Save** saves all changes you have performed on this tab or on any other tab of this dialog and switches back to the <u>AVG scanning interface default dialog</u>. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.
- **Cancel** cancels any changes you have performed on this tab or on any other tab of this dialog and switches back to the <u>AVG scanning interface default</u> <u>dialog</u>.



13.5.2. How to Scan

🛃 AVG Internet Security Network Edition 📃		
File Components History Tools He	lp	
AVG Internet Security	You are protected. All security features are working correctly and are up to date.	
	Settings for scheduled scan	-
Overview	Schedule settings How to scan What to scan	_
Computer scanner	✓ Automatically heal/remove infections	
📝 Update now	Scan Potentially Unwanted Programs and Spyware threats Scan for Tracking Cookies	
	✓ Scan inside archives ✓ Use Heuristics	
	Scan system environment	
	Scan for rootkits	
	Scan infectable files only	
	✓ Scan media files	
	Scan process priority	
Statistics	Automatic scan	
Last scan: 6.11.08, 11:46	· ·	
Last update: 6.11.06,12:04 Virus DB: 270.9.0/1770	Set additional scan reports	
AVG version: 8.0.209	Additional scan settings	
License expires: Not activated		_
	🐑 Save Cancel	
Show notification		_

On the **How to scan** tab you will find a list of scanning parameters that can be optionally switched on/off. By default, most parameters are switched on and the functionality will be applied during scanning. Unless you have a valid reason to change these settings we recommend to keep to the pre-defined configuration:

- **Automatically heal/remove infection** (*switched on, by default*): if a virus is identified during scanning it can be healed automatically if a cure is available. In case the infected file cannot be healed automatically, or if you decide to switch off this option, you will be notified upon a virus detection and will have to decide what to do with the detected infection. The recommended action is to remove the infected file to the <u>Virus Vault</u>.
- Scan Potentially Unwanted Programs (switched on, by default): this parameter controls the <u>Anti-Virus</u> functionality that allows <u>detection of</u> <u>potentially unwanted programs</u> (executable files that can run as spyware or adware) and these can then be blocked, or removed;
- Scan for Tracking Cookies (switched on, by default): this parameter of the <u>Anti-Spyware</u> component defines that cookies should be detected during scanning (*HTTP cookies are used for authenticating, tracking, and maintaining* specific information about users, such as site preferences or the contents of their electronic shopping carts);



- Scan inside archives (switched on, by default): this parameters defines that the scanning should check all files even if these are packed inside some type of archive, e.g. ZIP, RAR, ...
 - **Use Heuristics** (switched on, by default): heuristic analysis (dynamic emulation of the scanned object's instructions in a virtual computer environment) will be one of the methods used for virus detection during scanning;
 - **Scan system environment** (*switched on, by default*): scanning will also check the system areas of your computer;
 - Scan for rootkits tick this item if you want to include the rootkit detection into scanning of the entire computer. The rootkit detection is also available on its own within the <u>Anti-Rootkit</u> component;
 - Scan infectable files only (switched off, by default): with this option switched on, scanning will not be applied to files that cannot get infected. These can be for instance some plain text files, or some other non-executable files.

Within the *Scan process priority* section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but system resources usage will increase significantly during its run, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease system resources usage by extending the scanning duration.

Note: By default, the scanning configuration is set up for optimum performance. Unless you have a valid reason to change the scanning settings it is highly recommended to stick to the predefined configuration. Any configuration changes should be performed by experienced users only. For further scanning configuration options see the <u>Advanced settings</u> dialog accessible via the **File / Advanced setting** system menu item.

Control buttons of the Settings for scheduled scan dialog

There are two control buttons available on all three tabs of the **Settings for scheduled scan** dialog (<u>Schedule settings</u>, **How to scan** and <u>What to scan</u>) and these have the same functionality no matter on which tab you currently are:



- Save saves all changes you have performed on this tab or on any other tab
 of this dialog and switches back to the <u>AVG scanning interface default dialog</u>.
 Therefore if you wish to configure the test parameters on all tabs, press the
 button to save them only after you have specified all your requirements.
 - Cancel cancels any changes you have performed on this tab or on any other tab of this dialog and switches back to the <u>AVG scanning interface default</u> <u>dialog</u>.

13.5.3.What to Scan

불 AVG Internet Security Netwo	rk Edition	_ 🗆 🖂
File Components History Tools He	lp	
AVG Internet Security	You are protected. All security features are working correctly and are up to date.	
	Settings for scheduled scan	
🚺 Overview	Schedule settings How to scan What to scan	
Q Computer scanner	Scan whole computer	
🕼 Update now	Scan specific files or folders	
Statistics Last scar: 6.11.08, 11:46 Last update: 6.11.08, 12:04 Virus DB: 270.9.0/1770 AVG version: 8.0.209 License expires: Not activated Show notification	Gesktop My Conputer My Conputer General Attack Ge	Cancel

On the **What to scan** tab you can define whether you want to schedule <u>scanning of</u> the whole computer or <u>scanning of specific files or folders</u>. In case you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify folders to be scanned.

Control buttons of the Settings for scheduled scan dialog

There are two control buttons available on all three tabs of the **Settings for scheduled scan** dialog (<u>Schedule settings</u>, <u>How to scan</u> and **What to scan**) and these have the same functionality no matter on which tab you currently are:

• Save - saves all changes you have performed on this tab or on any other tab


of this dialog and switches back to the <u>AVG scanning interface default dialog</u>. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.

> Cancel - cancels any changes you have performed on this tab or on any other tab of this dialog and switches back to the <u>AVG scanning interface default</u> <u>dialog</u>.

13.6.Scan Results Overview

🛃 AVG Internet Security Netwo	rk Edition				_	
File Components History Tools He	lp					
AVG Internet Security	You are All security	protected. features are workir	ng correctly and are	up to date.		
	Scan results ove	rview				
0verview	Name	Start time	End time	Tested objects	Infections	Spyv
Q Computer scanner	Scan whole computer	6.11.2008, 11:46 5.11.2008, 23:00	6.11.2008, 11:46 6.11.2008, 1:09	165 778558	0/0 0/0	0/0 0/0
Vpdate now	Scheduled scan	4.11.2008, 23:00	5.11.2008, 1:07	777652	0/0	0/0
Statistics Last scan: 6.11.08, 11:46 Last update: 6.11.08, 12:04 Virus DB: 270.9.0/1770 AVG version: 8.0.209 License exprises Nd activated	٢)	101				>
Show notification	View details	Delete result			Back	

The **Scan results overview** dialog is accessible from the <u>AVG scanning interface</u> via the **Scan history** button. The dialog provides a list of all previously launched scans and information of their results:

- **Name** scan designation; it can either be the name of one of the <u>predefined</u> <u>scans</u>, or a name you have given to your <u>own scheduled scan</u>. Every name includes an icon indicating the scan result:
 - l green icon informs there was no infection detected during the scan

local - blue icon announces there was an infection detected during the scan but the infected object was removed automatically



I - red icon warns there was an infection detected during the scan and it could not be removed!

Each icon can either be solid or cut in half - the solid icons stands for a scan that was completed and finished properly; the cut-in-half icon means the scan was canceled or interrupted.

Note: For detailed information on each scan please see the <u>Scan</u> <u>Results</u> dialog accessible via the **View details** button (in the bottom part of this dialog).

- Start time date and time when the scan was launched
- End time date and time when the scan ended
- Tested objects number of objects that were checked during scanning
- Infections number of virus infections detected / removed
- Spyware number of spyware detected / removed
- **Scan log information** information relating to the scanning course and result (typically on its finalization or interruption)

Control buttons

The control buttons for the **Scan results overview** dialog are:

- View details this button is only active if a specific scan is selected in the above overview; press it to switch to the <u>Scan results</u> dialog to view detailed data on the selected scan
- Delete result this button is only active if a specific scan is selected in the above overview; press it to remove the selected item from the scan results overview
- Back switches back to the default dialog of the AVG scanning interface



13.7.Scan Results Details

If in the <u>Scan Results Overview</u> dialog a specific scan is selected, you can then click the **View details** button to switch to the **Scan Results** dialog providing detailed data on the course and result of the selected scan.

The dialog is further divided into several tabs:

- <u>Results Overview</u> this tab is displayed at all times and provides statistical data describing the scan progress
- <u>Infections</u> this tab is displayed only if a <u>virus infection</u> was detected during scanning
- <u>Spyware</u> this tab is displayed only if <u>spyware</u> was detected during scanning
- <u>Warnings</u> this tab is displayed only if some objects unable to be scanned were detected during scanning
- *<u>Rootkits</u>* this tab is displayed only if <u>rootkits</u> were detected during scanning
- <u>Information</u> this tab is displayed only if some potential threats were detected but these cannot be classified as any of the above categories; then the tab provides a warning message on the finding



13.7.1.Results Overview Tab

🚔 AVG Internet Security Netwo	rk Edition	_ 0 🛛
File Components History Tools He	elp	
AVG Internet Security	You are protected. All security features are working correctly and are up to date.	
0verview	Scan results Results overview Warnings	
Q Computer scanner	Scan "Scheduled scan" was finished.	
🕼 Update no w	🧭 No infection was found during this scan	
Statistics Last scan 6.11.08, 11:46 Last update: 6.11.08, 12:04 Virus DB: 270.9.0/1770 AVG version: 8.0.209 License expires: Not activated	Folders selected for scanning: Scan whole computer Scan started: 4. listopadu 2008, 23:00:02 Scan finished: 5. listopadu 2008, 1:07:35 (2 hour(s) 7 minute(s) 33 second(s Total object scanned: 777652 User who launched the scan: SYSTEM Export overview to file	s))
Show notification	The scan is complete. Bac	:k

On the *Scan results* tab you can find detailed statistics with information on:

- detected virus infections / spyware
- removed virus infections / spyware
- the number of virus infections / spyware that cannot be removed or healed

In addition you will find information on the date and exact time of the scan launch, on the total number of scanned objects, on the scanning duration and the number of errors that have occurred during scanning.

Control buttons

There is only one control button available in this dialog. The *Close results* button returns to the *Scan results overview* dialog.



13.7.2.Infections Tab

AVG Enterprise Edition		
File Components History Tools H	Your computer is safe. All security features are working correctly and are up to date.	
Dverview	Scan results	
Q Computer scapper	File	Infection
Update now	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\virus\eicar_com.zip:\eicar.com	Virus identified EICAR_ Virus identified EICAR_
Statistics Last scan: 11.1.08, 12.48 Last update: 11.1.08, 958 Virus DB: 25917.13/1216 AVG version: 8.0.46	View details Remove selected infections Remove all u	nhealed infections
License expires: 31.1.2008	u i ne scan nas been iinishêd.	Back

The **Infections** tab is only displayed in the **Scan results** dialog if a <u>virus infection</u> was detected during scanning. The tab is divided into three sections providing the following information:

- File full path to the original location of the infected object
- **Infections** name of the detected <u>virus</u> (for details on specific viruses please consult the <u>Virus Encyclopedia</u> online)
- **Result** defines the current status of the infected object that was detected during scanning:
 - *Infected* the infected object was detected and left in its original location (*for instance if you have <u>switched off the automatic healing</u> <u>option</u> in a specific scan settings)*
 - *Healed* the infected object was healed automatically and left in its original location
 - *Moved to Virus Vault* the infected object was moved to the <u>Virus</u>
 <u>Vault</u> quarantine



- $_{\odot}$ Deleted the infected object was deleted
- Added to PUP exceptions the finding was evaluated as an exception and added to the list of PUP exceptions (configured in the <u>PUP</u> <u>Exceptions</u> dialog of the advanced settings)
- $_{\odot}$ **Locked file not tested** the respective object is locked and AVG is therefore unable to scan it
- Potentially dangerous object the object was detected as potentially dangerous but not infected (*it can contain macros, for instance*); the information should be taken as a warning only
- *Reboot is required to finish the action* the infected object cannot be removed, to remove it completely you have to restart your computer

Control buttons

There are three control buttons available in this dialog:

• View details - the button opens a new dialog window named **Detailed scan** result information:

🚽 Detailed scan	result information 🛛 🔀
Property name	Property value
Object name Detection name	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adware\adwa Adware Generic.ZG
4	
Previous	Next Close

In this dialog you can find information on the location of the detected infectious object (*Property name*). Using the *Previous / Next* buttons you can view information on specific findings. Use the *Close* button to close this dialog.



- Remove selected infections use the button to move the selected finding to the <u>Virus Vault</u>
 - Remove all unhealed infections this button deletes all findings that cannot be healed or moved to the <u>Virus Vault</u>
 - Close results terminates the detailed information overview and returns to the <u>Scan results overview</u> dialog

13.7.3.Spyware Tab

🚽 AVG Enterprise Edition				
File Components History Tools He	lp			
🛃 AVG	Your computer is safe. All security features are working correctly	and are up to date.		
Overview	Scan results Results overview Infections Spyware			
Computer scanner	File	Infection	Result	~
•	S:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.NG	Moved to Virus Vault	
📝 Update now	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.AAI	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.A	Moved to Virus Vault	
	C:\kLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.AKM	Moved to Virus Vault	
	S:\klara\dokumentace\test_virus_adware\adw	Adware Generic.DFB	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.DFB	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.BB	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.XQ	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.FP	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.GU	Moved to Virus Vault	
	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.GZ	Moved to Virus Vault	
Statistics	👰 C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adw	Adware Generic.ZG	Moved to Virus Vault	~
Last scan: 11.1.08, 13:19 Last update: 11.1.08, 9:58	View details Remove selected infec	tions Remove	all unhealed infections	
Virus DB: 269.17.13/1216 AVG version: 8.0.46 License expires: 31.1.2008	🚺 The scan has been finished.		Back	

The **Spyware** tab is only displayed in the **Scan results** dialog in if <u>spyware</u> was detected during scanning. The tab is divided into three sections providing the following information:

- File full path to the original location of the infected object
- Infections name of the detected <u>spyware</u> (for details on specific viruses please consult the <u>Virus Encyclopedia</u> online)
- **Result** defines the current status of the object that was detected during scanning:
 - Infected the infected object was detected and left in its original location (for instance if you have <u>switched off the automatic healing</u>)



option in a specific scan settings)

- Healed the infected object was healed automatically and left in its original location
- *Moved to Virus Vault* the infected object was moved to the <u>Virus</u> <u>Vault</u> quarantine
- Deleted the infected object was deleted
- Added to PUP exceptions the finding was evaluated as an exception and added to the list of PUP exceptions (configured in the <u>PUP</u> <u>Exceptions</u> dialog of the advanced settings)
- Locked file not tested the respective object is locked and AVG is therefore unable to scan it
- Potentially dangerous object the object was detected as potentially dangerous but not infected (it can contain macros, for instance); the information is a warning only
- *Reboot is required to finish the action* the infected object cannot be removed, to remove it completely you have to restart your computer

Control buttons

There are three control buttons available in this dialog:

• *View details* - the button opens a new dialog window named *Detailed scan result information*:



📕 Detailed scan	result information 🛛 🛛 🔀
Duranturan	Description
Propercy name	Property value
Object name	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\adware\adwa
Detection name	Adware Generic.ZG
s	
Previous	Next Close

In this dialog you can find information on the location of the detected infectious object (*Property name*). Using the *Previous / Next* buttons you can view information on specific findings. Use the *Close* button to leave this dialog.

- Remove selected infections use the button to move the selected finding to the <u>Virus Vault</u>
- Remove all unhealed infections this button deletes all findings that cannot be healed or moved to the <u>Virus Vault</u>
- Close results terminates the detailed information overview and returns to the <u>Scan results overview</u> dialog

13.7.4.Warnings Tab

The **Warnings** tab displays information on "suspected" objects (*typically files*) detected during scanning. When detected by the <u>Resident Shield</u>, these files are blocked from being accessed. Typical examples of this kind of findings are: hidden files, cookies, suspicious registry keys, password protected documents or archives, etc.

13.7.5.Rootkits Tab

The **Rootkits** tab displays information on rootkits detected during scanning. Its structure is basically the same as the **Infections tab** or the **Spyware tab**.



13.7.6.Information Tab

The **Information** tab contains data on such "findings" that cannot be categorized as infections, spyware, etc. They can neither be positively labeled as dangerous but they are still worth your attention. All data on this tab is merely informative.

13.8.Virus Vault

🕌 History					
Event History					
Virus Vault	Infection type	Virus name	Path to file	Original object name	Date of storage
	😻 Warning	Found Tracking cookie.Adren	C:\Docume		1.11.2008, 23:07:51
	🂐 Warning	Found Tracking cookie.Adrev	C:\Docume		30.10.2008, 23:08:36
	雛 Warning	Found Tracking cookie.Doubl	C:\Docume		30.10.2008, 23:08:30
	雛 Warning	Found Tracking cookie.Adver	C:\Docume		30.10.2008, 23:08:25
	雛 Warning	Found Tracking cookie.Statc	C:\Docume		30.10.2008, 12:09:13
	🈻 Warning	Found Tracking cookie.Doubl	C:\Docume		30.10.2008, 12:09:00
	🏽 🇱 Warning	Found Tracking cookie.207	C:\Docume		30.10.2008, 12:08:53
	<				
	Bestore	Restore As Delete	Send to an	alueie Emptu Vault	
	Trestore	TIESCOLE AS DEIECE			
					Chur
U					Close

Virus Vault is a safe environment for the management of suspect/infected objects detected during AVG tests. Once an infected object is detected during scanning, and AVG is not able to heal it automatically, you are asked to decide what is to be done with the suspect object. The recommended solution is to move the object to the **Virus Vault** for further treatment.

The **Virus vault** interface opens in a separate window and offers an overview of information on quarantined infected objects:

- **Infection type** distinguishes finding types based on their infective level (*all listed objects can be positively or potentially infected*)
- *Virus Name* specifies the name of the detected infection according to the <u>Virus encyclopedia</u> (online)



- Path to file full path to the original location of the detected infectious file
 - **Original object name** all detected objects listed in the chart have been labeled with the standard name given by AVG during the scanning process. In case the object had a specific original name that is known (*e.g. a name of an e-mail attachment that does not respond to the actual content of the attachment*), it will be provided in this column.
 - Date of storage date and time the suspected file was detected and removed to the Virus Vault

Control buttons

The following control buttons are accessible from the *Virus Vault* interface:

- **Restore** removes the infected file back to its original location on your disk
- **Restore As** in case you decide to move the detected infectious object from the **Virus Vault** to a selected folder, use this button The suspicious and detected object will be saved with its original name. If the original name is not known, the standard name will be used.
- Delete removes the infected file from the Virus Vault completely
- Send to analysis sends the suspected file for deep analysis to the AVG virus labs
- Empty Vault removes all Virus Vault content completely



14. AVG Updates

14.1.Update Levels

AVG offers two update levels to select from:

- **Definitions update** contains changes necessary for reliable anti-virus, anti-spam and anti-malware protection. Typically, it does not include any changes to the code and updates only the definition database. This update should be applied as soon as it is available.
- **Program update** contains various program changes, fixes and improvements.

When <u>scheduling an update</u>, it is possible to select which priority level should be downloaded and applied.

14.2.Update Types

You can distinguish between two types of update:

- **On demand update** is an immediate AVG update that can be performed any time the need arises.
- **Scheduled update** within AVG it is also possible to <u>pre-set an update plan</u>. The planned update is then performed periodically according to the setup configuration. Whenever new update files are present on the specified location, they are downloaded either directly from the Internet, or from the network directory. When no newer updates are available, nothing happens.

14.3.Update Process

The update process can be launched immediately as the need arises by the **Update now** <u>quick link</u>. This link is available at all times from any <u>AVG user interface</u> dialog. However, it is still highly recommended to perform updates regularly as stated in the update schedule editable within the <u>Update manager</u> component.

Once you start the update, AVG will first verify whether there are new update files available. If so, AVG starts their downloading and launches the update process itself. During the update process you will get redirected to the **Update** interface where you can view the process progressing in its graphical representation as well as in an overview of relevant statistic parameters (*update file size, received data, download speed, elapsed time, ...*).



Note: Before the AVG program update launch a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS in its original configuration from this point. This option is accessible via Start / All Programs / Accessories / System tools / System Restore. Recommended to experienced users only!



15. Event History

불 History					
Event History					
Virus Vault	Event date and time	User	Source	Event description	<u>^</u>
	☑─3.11.2008, 11:50:58	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	☑↗3.11.2008, 11:50:04	NT AUTHORITY\SYSTEM	Update	Update was started.	≡
	27 3.11.2008, 8:34:27	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	☑↗3.11.2008, 8:34:01	NT AUTHORITY\SYSTEM	Update	Update was started.	
	223.11.2008, 7:51:35	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	27 3.11.2008, 7:51:02	NT AUTHORITY\SYSTEM	Update	Update was started.	
	2 √3.11.2008, 3:50:24	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	⊿≫3.11.2008, 3:50:01	NT AUTHORITY\SYSTEM	Update	Update was started.	
	🔍 3.11.2008, 1:08:36	NT AUTHORITY\SYSTEM	Scan	Scheduled scan was finis	1
	2.11.2008, 23:53:06	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	2.11.2008, 23:51:26	NT AUTHORITY\SYSTEM	Update	Update was started.	
	🔍 2.11.2008, 23:00:00	NT AUTHORITY\SYSTEM	Scan	Scheduled scan was star	
	2.11.2008, 19:50:23	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	₩2.11.2008, 19:50:01	NT AUTHORITY\SYSTEM	Update	Update was started.	
	₽ 2.11.2008, 15:53:01	NT AUTHORITY\SYSTEM	Update	Update was finished.	
	2.11.2008, 15:51:02	NT AUTHORITY\SYSTEM	Update	Update was started.	~
	<			>	
	Empty list			Refresh list	
0				Close	

The **Event History** dialog is accessible from the <u>system menu</u> via the **History/Event History Log** item. Within this dialog you can find a summary of important events that occurred during **AVG 8.5 Internet Security** operation. **Event History** records the following types of events:

- Information about updates of the AVG application
- Scanning start, end or stop (including automatically performed tests)
- Events connected with virus detection (by the <u>Resident Shield</u> or <u>scanning</u>) including occurrence location
- Other important events

Control buttons

- Empty list deletes all entries in the list of events
- Refresh list updates all entries in the list of events



16. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the *FAQ* section of the AVG website at <u>www.avg.com</u>.

If you do not succeed in finding help this way, contact the technical support department by email. Please use the contact form accessible from the system menu via *Help / Get help online*.